A Personal Perspective of the Alpern-Schneider Characterization of Safety and Liveness

Martin Rem

0 Introduction

In [1] Alpern and Schneider give a topological characterization of safety and liveness properties. This note is the formal reflection of my own understanding of their theory.

Throughout this note $A$ is a fixed set of at least two symbols. As usual, $A^*$ denotes the set of all finite sequences of symbols from $A$, and $A^\omega$ denotes the set of all infinite sequences of symbols from $A$. Let $P$ be the set of all boolean functions on $A^\omega$. Elements of $P$ are known as properties. They are our object of study.

We give a few examples of properties, formulated as predicates in sequence $t$, $t \in A^\omega$. Let $a \in A$.

$p0$: \hspace{1cm} false;  
$p1$: \hspace{1cm} the first symbol of $t$ is $a$;  
$p2$: \hspace{1cm} the first symbol of $t$ differs from $a$;  
$p3$: \hspace{1cm} the first symbol of $t$ is $a$, and $t$ contains a symbol that differs from $a$;  
$p4$: \hspace{1cm} the number of $a$'s in $t$ is finite;  
$p5$: \hspace{1cm} the number of $a$'s in $t$ is infinite;  
$p6$: \hspace{1cm} true.

1 Safety properties

Let $x \in A^*$ and $y \in A^\omega$. We say that $x$ is a prefix of $y$, notation $x \preceq y$, when
where catenation of sequences is denoted by juxtaposition. With each property \( p \) we associate a set \( \text{pref}_p \), \( \text{pref}_p \subseteq A^* \), as follows:

\[
x \in \text{pref}_p \iff (\exists y : y \in A^* \land x \leq y : p.y)
\]

Set \( \text{pref}_p \) is prefix-closed:

**Property 0** \( wx \in \text{pref}_p \Rightarrow w \in \text{pref}_p \)

**Proof**

\[
wx \in \text{pref}_p \\
= \quad \{\text{definition of } \text{pref}\}
\]

\[
(\exists y : y \in A^* \land wx \leq y : p.y)
\]

\[
\Rightarrow \quad \{wx \leq y \Rightarrow w \leq y\}
\]

\[
(\exists y : y \in A^* \land w \leq y : p.y)
\]

\[
= \quad \{\text{definition of } \text{pref}\}
\]

\[
w \in \text{pref}_p
\]

(*End of proof*)

We can form negations, conjunctions, and disjunctions of properties in the usual way, for example \( (p \lor q).t = p.t \lor q.t \). With respect to the examples in Section 0 we have \( \neg p0 = p6, \neg p1 = p2, \neg p4 = p5, p1 \lor p2 = p6, p4 \land p5 = p0, \) etc.

**Property 1** \( \text{pref}.(p \lor q) = \text{pref}_p \cup \text{pref}_q \)

**Proof**

\[
x \in \text{pref}.(p \lor q)
\]

\[
= \quad \{\text{definition of } \text{pref}\}
\]

\[
(\exists y : x \leq y : (p \lor q).y)
\]

\[
= \quad \{\text{definition of disjunction}\}
\]

\[
(\exists y : x \leq y : p.y \lor q.y)
\]

\[
= \quad \{\text{calculus}\}
\]

\[
(\exists y : x \leq y : p.y) \lor (\exists y : x \leq y : q.y)
\]

\[
= \quad \{\text{definition of } \text{pref}\}
\]

\[
x \in \text{pref}_p \lor x \in \text{pref}_q
\]

(*End of proof*)