MODULE *CigaretteSmokers*

A specification of the cigarette smokers problem, originally described in 1971 by *Suhas Patil*. https://*en.wikipedia.org*/wiki/*Cigarette_smokers_problem*

EXTENDS *Integers*, *FiniteSets*

CONSTANT *Ingredients*
VARIABLE *smokers*, *dealer*

'Ingredients' is a set of ingredients, originally {*matches*, *paper*, *tobacco*}. 'Offers' is a subset of subsets of ingredients, each missing just one ingriedent

$$Offers \triangleq \{i \in \text{SUBSET } Ingredients : Cardinality(i) = Cardinality(Ingredients) - 1\}$$

'smokers' is a function from the ingredient the smoker has infinite supply of, to a BOOLEAN flag signifying smoker's state (smoking/not smoking) 'dealer' is an element of 'Offers', or an empty set

$$TypeOK \triangleq \begin{array}{l} \land\ smokers \in [Ingredients \to [smoking : \text{BOOLEAN }]] \\ \land\ dealer \quad \in Offers \lor dealer = \{\} \end{array}$$

$$vars \triangleq \langle smokers,\ dealer \rangle$$

$$Init \triangleq \begin{array}{l} \land\ smokers = [r \in Ingredients \mapsto [smoking \mapsto \text{FALSE}]] \\ \land\ dealer \in Offers \end{array}$$

$$startSmoking \triangleq \begin{array}{l} \land\ dealer \neq \{\} \\ \land\ smokers' = [r \in Ingredients \mapsto [smoking \mapsto \{r\} \cup \\ \qquad\qquad\qquad\qquad\qquad\qquad dealer = Ingredients]] \\ \land\ dealer' = \{\} \end{array}$$

$$stopSmoking \triangleq \begin{array}{l} \land\ dealer = \{\} \\ \land\ smokers' = [r \in Ingredients \mapsto [smoking \mapsto \text{FALSE}]] \\ \land\ dealer' \in Offers \end{array}$$

$$Next \triangleq startSmoking \lor stopSmoking$$

$$Spec \triangleq Init \land \Box[Next]_{vars}$$
$$FairSpec \triangleq Spec \land \text{WF}_{vars}(Next)$$

An invariant checking that at most one smoker smokes at any particular moment

$$AtMostOne \triangleq Cardinality(\{r \in Ingredients : smokers[r].smoking\}) \leq 1$$