──────────── 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*, *Offers*
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 ingriedient

ASSUME $\land$ *Offers* $\subseteq$ (SUBSET *Ingredients*)
$\qquad\land \forall\, n \in$ *Offers* : *Cardinality*$(n) =$ *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 $\triangleq$ $\land$ *smokers* $\in$ [*Ingredients* $\to$ [*smoking* : BOOLEAN]]
$\qquad\qquad\land$ *dealer* $\in$ *Offers* $\lor$ *dealer* $= \{\}$

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

ChooseOne(*S*, *P*(_)) $\triangleq$ CHOOSE $x \in S : P(x) \land \forall\, y \in S : P(y) \Rightarrow y = x$

Init $\triangleq$ $\land$ *smokers* $= [r \in$ *Ingredients* $\mapsto$ [*smoking* $\mapsto$ FALSE]]
$\qquad\quad\land$ *dealer* $\in$ *Offers*

startSmoking $\triangleq$ $\land$ *dealer* $\neq \{\}$
$\qquad\qquad\qquad\quad\land$ *smokers*$' = [r \in$ *Ingredients* $\mapsto$ [*smoking* $\mapsto \{r\} \cup$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ *dealer* $=$ *Ingredients*]]
$\qquad\qquad\qquad\quad\land$ *dealer*$' = \{\}$

stopSmoking $\triangleq$ $\land$ *dealer* $= \{\}$
$\qquad\qquad\qquad\quad\land$ LET $r \triangleq$ *ChooseOne*(*Ingredients*,
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ LAMBDA $x :$ *smokers*[*x*].*smoking*)
$\qquad\qquad\qquad\qquad$ IN $\quad$ *smokers*$' = [$*smokers* EXCEPT ![*r*].*smoking* $=$ FALSE]
$\qquad\qquad\qquad\quad\land$ *dealer*$' \in$ *Offers*

Next $\triangleq$ *startSmoking* $\lor$ *stopSmoking*

Spec $\triangleq$ *Init* $\land \Box$[*Next*]$_{vars}$
FairSpec $\triangleq$ *Spec* $\land$ 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*$\}) \leq 1$

──