There follows a Z specification of a program that derives randomness from some kind of seed. The Z specification was written by Rob Arthan after a request by Dave Topham.

**Z specification**
Let the outcome of an experiment be denoted by the set \( \text{OUTCOME} \) where the ultimate objective is that any outcome is equally likely. For example consider the flip of a coin.

We model the outcomes by the free type:

\[
\text{OUTCOME} ::= \text{Head} \mid \text{Tail}
\]

In order to model probability aspects of this specification consider the set \( \text{SEED} \) where a seed is drawn from some non-empty finite set of integers whose size is a multiple of the number of possible outcomes. For example a seed might be a 64 bit number representing a time.

\[
\begin{align*}
\text{SEED} & : F_1 Z \\
\text{\#SEED} & \mod \text{\#OUTCOME} = 0
\end{align*}
\]

The following states that \( \text{pick} \) makes a fair choice of an outcome given an input seed: the predicate says that \( \text{pick} \) divides the input sample space evenly amongst the possible outcomes.

\[
\begin{align*}
\text{pick} : \text{SEED} \rightarrow \text{OUTCOME} \\
\forall f : \text{OUTCOME} \cdot \text{\#}(\text{pick}^{-1}\{f\}) & = \text{\#SEED} \ \text{div} \ \text{\#OUTCOME}
\end{align*}
\]

The schema \( \text{Flip} \) models the experiment:

\[
\begin{array}{c}
\text{Flip} \\
\text{seed? : SEED} \\
\text{outcome! : OUTCOME} \\
\text{outcome!} = \text{pick}(\text{seed?})
\end{array}
\]