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 $OUTCOME$ 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:

$$OUTCOME ::= Head \mid Tail$$

In order to model probability aspects of this specification consider the set $SEED$ where a seed is drawn from some non-empty finite set of integers whose size isa multiple of the number of possible outcomes. For examplea seed might be a 64 bit number representing a time.

$$SEED : \mathbb{F}_1 \mathbb{Z}$$
$$\#SEED \bmod \#OUTCOME = 0$$

The following states that $pick$ makes a fair choice of an outcome given an imput seed: the predicate says that pick divides the imput sample space evenly amongst the possible outcomes.

$$pick : SEED \longrightarrow OUTCOME$$
$$\forall fl : OUTCOME \bullet \#(pick^{\sim}(\!|\{fl\}|\!)) = \#SEED \operatorname{div} \#OUTCOME$$

The schems $Flip$ models the experiment:

Flip

$$seed? : SEED$$
$$outcome! : OUTCOME$$
$$outcome! = pick(seed?)$$