MODULE *DieHarder*

EXTENDS *Integers*, *GCD*

CONSTANTS *Goal*, *Jugs*, *Capacity*

ASSUME $\land$ $Goal \in Nat$
$\land$ $Capacity \in [Jugs \rightarrow Nat \setminus \{0\}]$

$Min(m, n) \triangleq$ IF $m < n$ THEN m ELSE n

****

--algorithm *DieHarder*
{ variable $injug = [j \in Jugs \mapsto 0]$ **;**
{ while (TRUE **)**
{ either with ($j \in Jugs$ **)** fill $Jug[j]$
{ $injug[j] := Capacity[j]$ **}**
or with ($j \in Jugs$ **)** empty $Jug[j]$
{ $injug[j] := 0$ **}**

When pouring from j to k, we first ask if $In[j]+In[k] > In[k]$. If so, we make $In[k]' = Cap[k]$ and $In[j]' = In[j]-(Cap[k]-In[k])$; if not, we make $In[k]' = In[k]+In[j]$ and $In[j]' = 0$. In the former case, the amount poured is $Cap[k] - In[k]$; in the latter case, the amount poured is $In[j]$, which equals $(In[k]+In[j]) - In[k]$. In both cases, the amount poured is $Min(In[k]+In[j], In[k]) - In[k]$.

or with ($j \in Jugs, k \in Jugs \setminus \{j\}$ **)** pour from j to k
{ with ($poured = Min(injug[j] + injug[k], Capacity[k]) - injug[k]$ **)**
{ $injug[j] := injug[j] - poured$
|| $injug[k] := injug[k] + poured$
} } } **} }**

****

BEGIN TRANSLATION

VARIABLE *injug*

$vars \triangleq \langle injug \rangle$

$Init \triangleq$ Global variables
$\land$ $injug = [j \in Jugs \mapsto 0]$

$Next \triangleq$ $\lor$ $\land$ $\exists j \in Jugs :$
$injug' = [injug$ EXCEPT $![j] = Capacity[j]]$
$\lor$ $\land$ $\exists j \in Jugs :$
$injug' = [injug$ EXCEPT $![j] = 0]$
$\lor$ $\land$ $\exists j \in Jugs :$
$\exists k \in Jugs \setminus \{j\} :$
LET $poured \triangleq Min(injug[j] + injug[k], Capacity[k]) - injug[k]$ IN
$injug' = [injug$ EXCEPT $![j] = injug[j] - poured,$
$![k] = injug[k] + poured]$

$Spec \triangleq Init \land \Box[Next]_{vars}$

END TRANSLATION

$$NecessaryCondition \triangleq \forall j \in Jugs : \\ \quad Divides(SetGCD(\{Capacity[k] : k \in Jugs\}), \\ \qquad\qquad injug[j])$$

Proof by induction that existence of a solution implies that the *GCD* of the jug capacities divides the contents of each jug after any amount of pouring.

Every pouring event consists in either filling the destination jug k or in emptying the source jug j into k.

A sequence of pouring events must begin with j full and the k empty because prior to the first pouring, the only possible actions are filling or emptying jugs. Before this event, all jugs are either full or empty, with at least one jug empty. That means $injug[j]$ is either $Capacity[j]$ or 0 for every j. The invariant is maintained because the *GCD* of all jugs' capacities divides every jug capacity individuallyk, and the *GCD* of all jugs' capacities divides 0.

In case the capacity of the destination jug k is greater than or equal to the contents of the source jug j, the entire contents of j is poured into k. In this case, because the amount poured is equal to
$Capacity[j]$, and because the *GCD* of all jugs' capacities divides the
$Capacity[j]$ (the *GCD* of all jugs' capacities divides every individual jug capacity), the invariant is maintained.

In case the capacity of k is less than the contents of j, then k will be filled and $injug[j]$ will be reduced by $Capacity[k]$, that is, $injug[j]$ will become $Capacity[j] - Capacity[k]$. But the *GCD* of all jugs' capacities divides this quantity, so the invariant is maintained.

That establishes the base case.

Now assume an intermediate situation where the jugs have various amounts in them, $injug[j]$ for all j in *Jugs*, where all $injug[j]$ are divisible by the *GCD*, by the induction hypothesis. A pouring event will replqce $injug[j]$ with $injug[j] - amount\_poured$ and $injug[k]$ with $injug[k] + amount\_poured$, where $amount\_poured$ is either $injug[j]$, emptying j, or $Capacity[k] - injug[k]$, either emptying j or leaving some in it. But all quantities are divisible by *GCD* of all jugs' capacities, again using the induction hypothesis.

Thus, an initial state where all jugs contain a divisible amount leads, by any possible pouring event, to a next state where all jugs contain divisible amounts. The induction is thus proved.

* Modification History
* Last modified *Mon Feb* 17 09:13:53 *PST* 2014 by *bbeckman*
* Created *Mon Feb* 17 07:51:51 *PST* 2014 by *bbeckman*