MODULE *ABL_with_partial_repayments*

This specification is encodes the specification given in prose in the file ABL-spec-*prose.rst* and some of the one-letter names for the constants and variables are as the same as in the prose specification. Only the behavor after the start of the contract is specified here. For example, "Bob has received P" is implied.

It is natural to model the asset amounts as Natural numbers because in the on-chain contract they are represented in satoshis

EXTENDS *Naturals*, *Sequences*, *TLC*

$Min(x, y) \triangleq$ IF $x < y$ THEN x ELSE y
$Max(x, y) \triangleq$ IF $x > y$ THEN x ELSE y

Rate 1.51% with *RATE_PRECISION* = 10000 will be represented as 151
RATE_PRECISION $\triangleq$ 10000

Note that C (the collateral amount) is not defined because
in this contract the amount of collateral does not change

The amount of the Principal asset
CONSTANT P
ASSUME $P > 0$
The number of installments the full repayment is split into
CONSTANT N
ASSUME $N > 0$
The number consecutive missed payments that result
in collateral forfeiture.
CONSTANT M
ASSUME $M > 0$
The rate for regular repayments due
CONSTANT *RateDue*
ASSUME *RateDue* $\leq$ *RATE_PRECISION*
The rate for surcharge on early repayments
CONSTANT *RateEarly*
ASSUME *RateEarly* $\leq$ *RATE_PRECISION*
The rates for surcharge on late repayment
CONSTANT *RatesLate*

$\textsc{assume}\ \textsc{domain}\ \mathit{RatesLate} = 1 \mathrel{..} M - 1$

$\textsc{assume}\ \forall\, x \in \textsc{domain}\ \mathit{RatesLate} : \mathit{RatesLate}[x] \leq \mathit{RATE\_PRECISION}$

The minumum number of steps in the contract

$\textsc{constant}\ \mathit{S\_min}$

$\textsc{assume}\ \mathit{S\_min} \in \mathit{Min}(N,\, M) \mathrel{..} (N + M)$

The maximum number of steps in the contract

$\textsc{constant}\ \mathit{S\_max}$

$\textsc{assume}\ \mathit{S\_max} \in \mathit{Max}(N,\, M) \mathrel{..} (N + M)$

The duration of each time period in blocks. $\mathit{S\_max}$ periods is the
max duration of the contract (assuming *TimelyEnforcement*)

$\textsc{constant}\ \mathit{BLOCKS\_IN\_PERIOD}$

Included to make the algorithm closer to the real world,
where the contract starts at arbitray block. Can be arbitrary *Nat* value.

$\textsc{constant}\ \mathit{START\_BLOCK}$

$\textsc{variables}\ \mathit{block},\ \mathit{state}$

$\mathit{fullState} \triangleq \langle \mathit{block},\ \mathit{state} \rangle$

$\mathit{ApplyRate}(v,\, r) \triangleq (v * r) \div \mathit{RATE\_PRECISION}$

$\mathit{ApplyLateRate}(v,\, rn) \triangleq \textsc{if}\ rn = 0\ \textsc{then}\ 0\ \textsc{else}\ \mathit{ApplyRate}(v,\, \mathit{RatesLate}[rn])$

$\mathit{P\_remainder} \triangleq P \% N$

The Principal amount is assumed to be much larger than number of periods

$\textsc{assume}\ \mathit{P\_remainder} < P \div 100$

Include the remainder in the last payment

$\mathit{LimitByBalance}(v) \triangleq \textsc{if}\ v + \mathit{P\_remainder} \geq \mathit{state}.B\ \textsc{then}\ \mathit{state}.B\ \textsc{else}\ v$

"Fraction of P" is the installment size

$\mathit{FracP} \triangleq (P \div N)$

D is the portion of the balance currently due

$D \triangleq \mathit{LimitByBalance}(\mathit{FracP} * (\mathit{state}.m + 1))$

L is the amount the repayment is late on

$L \triangleq \mathit{LimitByBalance}(\mathit{FracP} * \mathit{state}.m)$

When *TimelyEnforcement* is in effect, the value returned by *PeriodOf*
corresponds to 's' in the prose spec

$$\mathit{PeriodOf}(b) \triangleq (b - \mathit{START\_BLOCK}) \div \mathit{BLOCKS\_IN\_PERIOD}$$

$$\mathit{StepsTaken} \triangleq \mathit{Len}(\mathit{state.path})$$

$$\mathit{InDefault}(m,\ \mathit{period}) \triangleq m \geq M \lor \mathit{period} \geq \mathit{S\_max}$$

$$\mathit{RegularRepaymentAmount} \triangleq D + \mathit{ApplyRate}(D,\ \mathit{RateDue}) + \mathit{ApplyLateRate}(L,\ \mathit{state.m})$$

$$\begin{aligned}
&\mathit{RegularRepayment} \triangleq \\
&\quad \mathit{state}' = [\begin{aligned}[t]
&n \mapsto \mathit{state}.n + 1, \\
&m \mapsto 0, \\
&B \mapsto \mathit{state}.B - D, \\
&\mathit{total\_repaid} \mapsto \mathit{state.total\_repaid} + \mathit{RegularRepaymentAmount}, \\
&\mathit{path} \mapsto \mathit{state.path} \circ \text{“>”}, \\
&\mathit{at\_block} \mapsto \mathit{block}, \\
&\mathit{custody} \mapsto \textsc{if}\ \mathit{state}.B = D\ \textsc{then}\ \text{“Debtor>”}\ \textsc{else}\ \ \mathit{state.custody}]
\end{aligned}
\end{aligned}$$

$$\begin{aligned}
&\mathit{EarlyRepaymentAmount} \triangleq \\
&\quad \mathit{state}.B + \mathit{ApplyRate}(D,\ \mathit{RateDue}) \\
&\qquad\quad + \mathit{ApplyRate}((\mathit{state}.B - D),\ \mathit{RateEarly}) \\
&\qquad\quad + \mathit{ApplyLateRate}(\mathit{LimitByBalance}(\mathit{FracP} * \mathit{state.m}), \\
&\qquad\qquad\qquad\qquad\qquad \mathit{state.m})
\end{aligned}$$

$$\begin{aligned}
&\mathit{EarlyRepayment} \triangleq \\
&\quad \mathit{state}' = [\mathit{state}\ \textsc{except}\ \begin{aligned}[t]
&!.B = 0, \\
&!.\mathit{total\_repaid} = \mathit{state.total\_repaid} \\
&\qquad\qquad\qquad\qquad + \mathit{EarlyRepaymentAmount}, \\
&!.\mathit{path} = \mathit{state.path} \circ \text{“!”}, \\
&!.\mathit{custody} = \text{“Debtor!”}]
\end{aligned}
\end{aligned}$$

$$\begin{aligned}
&\mathit{Repayment} \triangleq \\
&\quad \land \neg \mathit{InDefault}(\mathit{state.m},\ \mathit{PeriodOf}(\mathit{block})) \\
&\quad \land\ \lor \mathit{RegularRepayment} \\
&\qquad\ \lor\ \land \mathit{EarlyRepaymentAmount} > \mathit{RegularRepaymentAmount} \\
&\qquad\qquad \land \mathit{EarlyRepayment}
\end{aligned}$$

$$\begin{aligned}
&\mathit{RepaymentMissed} \triangleq \\
&\quad \textsc{if}\ \mathit{InDefault}(\mathit{state.m} + 1,\ \mathit{PeriodOf}(\mathit{block})) \\
&\quad\ \textsc{then}\ \mathit{state}' = [\mathit{state}\ \textsc{except}\ \begin{aligned}[t]
&!.m = \mathit{state.m} + 1, \\
&!.\mathit{path} = \mathit{state.path} \circ \text{“X”}, \\
&!.\mathit{custody} = \text{“Creditor”}]
\end{aligned}
\end{aligned}$$

```
    ELSE  $state' = [state$ EXCEPT $!.m = state.m + 1,$
                                   $!.at\_block = block,$
                                   $!.path = state.path \circ$ "v"$]$

$Enforcement \triangleq$
  IF $PeriodOf(block) \neq PeriodOf(state.at\_block)$
   THEN $RepaymentMissed$
   ELSE  UNCHANGED $state$
```

If the enforcement is not done in time, the number of states to check grows
while all that new states will be duplicates. It can be said that
no enforcement within the period just means that period is now $2x$ as long,
but the overal state of the contract does not progress.
No-enforcement only hurts the *Creditor*, and it is the *Creditor* who is
doing the enforcement, so there's natural incentive for them to enforce.

```
$TimelyEnforcement \triangleq PeriodOf(block) \leq PeriodOf(state.at\_block) + 1$
```

Invariants

```
$TypeOK \triangleq$
    $\land$  DOMAIN $state = \{$"n", "m", "B", "at_block", "total_repaid", "custody",
                               "path"$\}$
    $\land$  $state.n \in 0 \,..\, N$
    $\land$  $state.m \in 0 \,..\, M$
    $\land$  $state.custody \in \{$"Contract", "Debtor>", "Debtor!", "Creditor"$\}$
    $\land$  $StepsTaken \leq N * M$

$ConsistentProgress \triangleq$
  IF $state.custody =$ "Contract"
   THEN
```

Early repayment available only before $N - 1$ steps are taken

```
      $\land$ IF $StepsTaken < N - 1$
          THEN $EarlyRepaymentAmount > RegularRepaymentAmount$
          ELSE  $EarlyRepaymentAmount = RegularRepaymentAmount$
   ELSE  TRUE

$ConsistentRepayment \triangleq$
  IF $state.custody \in \{$"Debtor>", "Debtor!"$\}$
   THEN  $\land\ state.B = 0$
```

```
            $\land \mathit{state.total\_repaid} \geq P$
            $\land \neg \mathit{InDefault}(\mathit{state.m},\ \mathit{PeriodOf}(\mathit{block}))$
       ELSE  TRUE

$\mathit{ConsistentEnforcement} \triangleq$
     IF $\mathit{state.custody} = \text{“Creditor”}$
      THEN $\mathit{InDefault}(\mathit{state.m},\ \mathit{PeriodOf}(\mathit{block}))$
      ELSE  TRUE

$\mathit{ConsistentRemainder} \triangleq$
     $(\mathit{state.B} \geq \mathit{FracP} \lor \mathit{state.B} = 0)$  last payment includes $\mathit{P\_remainder}$

$\mathit{ConsistentPeriods} \triangleq$
     IF $\mathit{TimelyEnforcement}$
      THEN
          At least one step in each period has to be taken
          when enforcement is on-time
          $\land \mathit{PeriodOf}(\mathit{block}) \leq \mathit{StepsTaken} + 1$
          Can progress over $\mathit{S\_max} + 1$ time periods, period index in $0 \mathrel{..} \mathit{S\_max}$
          $\land \mathit{PeriodOf}(\mathit{block}) \leq \mathit{S\_max}$
      ELSE  TRUE

Init & Next

$\mathit{Init} \triangleq$
     $\land \mathit{block} = \mathit{START\_BLOCK}$
     $\land \mathit{state} = [n \mapsto 0,\ m \mapsto 0,\ B \mapsto P,\ \mathit{at\_block} \mapsto \mathit{block},$
                 $\mathit{total\_repaid} \mapsto 0,\ \mathit{path} \mapsto \text{“”},\ \mathit{custody} \mapsto \text{“Contract”}]$

$\mathit{Next} \triangleq$
     $\land \mathit{state.custody} = \text{“Contract”}$
     $\land \mathit{TimelyEnforcement}$
     $\land \lor \mathit{Repayment}$              $\land$ UNCHANGED $\mathit{block}$
        $\lor \mathit{Enforcement}$             $\land$ UNCHANGED $\mathit{block}$
        $\lor \mathit{block}' = \mathit{block} + 1$   $\land$ UNCHANGED $\mathit{state}$

$\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\mathit{fullState}}$
```