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 $RatesLate$

ASSUME DOMAIN $RatesLate = 1 \,..\, M - 1$
ASSUME $\forall\, x \in$ DOMAIN $RatesLate : RatesLate[x] \leq RATE\_PRECISION$
The maximum number of steps in the contract
CONSTANT S
ASSUME $S \in Max(N,\, M) + 1 \,..\, (N + M)$
The duration of each time period in blocks. S periods is the
max duration of the contract (assuming *TimelyEnforcement*)
CONSTANT $BLOCKS\_IN\_PERIOD$
Included to make the algorithm closer to the real world,
where the contract starts at arbitray block. Can be arbitrary *Nat* value.
CONSTANT $START\_BLOCK$

VARIABLES $block,\, state$

$fullState \triangleq \langle block,\, state \rangle$

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

$ApplyLateRate(v,\, rn) \triangleq$ IF $rn = 0$ THEN 0 ELSE $ApplyRate(v,\, RatesLate[rn])$

$P\_remainder \triangleq P\%N$

The Principal amount is assumed to be much larger than number of periods
ASSUME $P\_remainder < P \div 100$

Include the remainder in the last payment
$LimitByBalance(v) \triangleq$ IF $v + P\_remainder \geq state.B$ THEN $state.B$ ELSE v

"Fraction of P" is the installment size
$FracP \triangleq (P \div N)$

D is the portion of the balance currently due
$D \triangleq LimitByBalance(FracP * (state.m + 1))$

L is the amount the repayment is late on
$L \triangleq LimitByBalance(FracP * state.m)$

When *TimelyEnforcement* is in effect, the value returned by *PeriodOf*
corresponds to 's' in the prose spec
$PeriodOf(b) \triangleq (b - START\_BLOCK) \div BLOCKS\_IN\_PERIOD$

$StepsTaken \triangleq Len(state.path)$

$$InDefault(m,\ period) \triangleq m \geq M \lor period \geq S - 1$$

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

$$\begin{array}{l}
RegularRepayment \triangleq \\
\quad state' = [n \mapsto state.n + 1, \\
\qquad\quad m \mapsto 0, \\
\qquad\quad B \mapsto state.B - D, \\
\qquad\quad total_repaid \mapsto state.total_repaid + RegularRepaymentAmount, \\
\qquad\quad path \mapsto state.path \circ \text{“>”}, \\
\qquad\quad at_block \mapsto block, \\
\qquad\quad custody \mapsto \text{IF } state.B = D \text{ THEN “Debtor>” ELSE } state.custody]
\end{array}$$

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

$$\begin{array}{l}
EarlyRepayment \triangleq \\
\quad state' = [state \text{ EXCEPT } !.B = 0, \\
\qquad\qquad\qquad\quad !.total_repaid = state.total_repaid \\
\qquad\qquad\qquad\qquad\qquad\qquad + EarlyRepaymentAmount, \\
\qquad\qquad\qquad\quad !.path = state.path \circ \text{“!”}, \\
\qquad\qquad\qquad\quad !.custody = \text{“Debtor!”}]
\end{array}$$

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

$$\begin{array}{l}
RepaymentMissed \triangleq \\
\quad \text{IF } InDefault(state.m + 1,\ PeriodOf(block)) \\
\quad\ \text{THEN } state' = [state \text{ EXCEPT } !.m = state.m + 1, \\
\qquad\qquad\qquad\qquad\qquad\quad !.path = state.path \circ \text{“X”}, \\
\qquad\qquad\qquad\qquad\qquad\quad !.custody = \text{“Creditor”}] \\
\quad\ \text{ELSE } state' = [state \text{ EXCEPT } !.m = state.m + 1, \\
\qquad\qquad\qquad\qquad\qquad\quad !.at_block = block, \\
\qquad\qquad\qquad\qquad\qquad\quad !.path = state.path \circ \text{“v”}]
\end{array}$$

$Enforcement \triangleq$
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 $\land\ state.B = 0$
$\land\ state.total\_repaid \geq P$
$\land \neg InDefault(state.m,\ PeriodOf(block))$
ELSE TRUE

$ConsistentEnforcement \triangleq$
IF $state.custody =$ "Creditor"
THEN $InDefault(state.m,\ PeriodOf(block))$
ELSE TRUE

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

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

Init & Next

$Init \triangleq$
$\land\ block = START\_BLOCK$
$\land\ state = [n \mapsto 0,\ m \mapsto 0,\ B \mapsto P,\ at\_block \mapsto block,$
$total\_repaid \mapsto 0,\ path \mapsto$ "",
$custody \mapsto$ "Contract"$]$

$Next \triangleq$
$\land\ state.custody =$ "Contract"
$\land\ TimelyEnforcement$
$\land\ \lor\ Repayment \quad \land$ UNCHANGED $block$
$\lor\ Enforcement \quad \land$ UNCHANGED $block$
$\lor\ block' = block + 1 \quad \land$ UNCHANGED $state$

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