MODULE *ABL_with_partial_repayments*

This specification encodes the description 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 used in the prose description. Only the behavor after the start of the contract is specified here. For example, "Bob has received P" is implied.

Note that due to limitations of model checker that only supports 32-bit signed integer numbers, the calculations of the amounts might not be exact due to the rounding inherent in integer calculations

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

$Min(set) \triangleq$ CHOOSE $x \in set : \forall\, y \in set : x \leq y$
$Max(set) \triangleq$ CHOOSE $x \in set : \forall\, y \in set : x \geq y$

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 amount of the Collateral asset
CONSTANT C
ASSUME $C > 0$
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 $RateCollateralPenalty$

ASSUME $RateCollateralPenalty \leq RATE\_PRECISION$

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 $START\_BLOCK$

CONSTANT C_UNCOND

ASSUME $C\_UNCOND \leq C$

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 $N < P \div 100$

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 description

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

$$StepsTaken \triangleq Len(state.path)$$

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

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

$$\begin{aligned} &RegularRepayment \triangleq \\ &\quad state' = [n \mapsto state.n + 1, \\ &\qquad m \mapsto 0, \\ &\qquad B \mapsto state.B - D, \\ &\qquad total\_repaid \mapsto state.total\_repaid + RegularRepaymentAmount, \\ &\qquad path \mapsto state.path \circ \text{“>”}, \\ &\qquad at\_block \mapsto block, \\ &\qquad custody \mapsto \text{IF } state.B = D \text{ THEN } [Debtor\_R \mapsto C] \text{ ELSE } state.custody] \end{aligned}$$

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

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

$$
\begin{array}{l}
\mathit{Repayment} \triangleq \\
\quad \lor \mathit{RegularRepayment} \\
\quad \lor \ \land \mathit{EarlyRepaymentAmount} > \mathit{RegularRepaymentAmount} \\
\qquad \land \mathit{EarlyRepayment}
\end{array}
$$

$$
\begin{array}{l}
\mathit{AmountForCollateralForfeiturePenalty} \triangleq \\
\quad \mathit{Max}(\{\mathit{state}.B,\ \mathit{RegularRepaymentAmount}\}) \\
\quad + \mathit{ApplyRate}(\mathit{Max}(\{\mathit{state}.B,\ \mathit{RegularRepaymentAmount}\}), \\
\qquad\qquad \mathit{RateCollateralPenalty})
\end{array}
$$

$$
\begin{array}{l}
\mathit{RepaymentMissed} \triangleq \\
\quad \text{IF } \mathit{InDefault}(\mathit{state}.m + 1,\ \mathit{PeriodOf}(\mathit{block})) \\
\quad \text{THEN LET } \mathit{C\_forfeited} \triangleq \\
\qquad\qquad \mathit{Max}(\{\mathit{C\_UNCOND}, \\
\qquad\qquad\qquad \mathit{Min}(\{C,\ (C * \mathit{AmountForCollateralForfeiturePenalty}) \\
\qquad\qquad\qquad\qquad \div P\})\}) \\
\qquad\quad \text{IN } \ \mathit{state}' = [\mathit{state} \\
\qquad\qquad\qquad\quad \text{EXCEPT } !.m = \mathit{state}.m + 1, \\
\qquad\qquad\qquad\qquad\quad !.\mathit{path} = \mathit{state}.\mathit{path} \circ \text{“X”}, \\
\qquad\qquad\qquad\qquad\quad !.\mathit{custody} = [\mathit{Creditor} \ \mapsto \mathit{C\_forfeited}, \\
\qquad\qquad\qquad\qquad\qquad\qquad \mathit{Debtor\_D} \mapsto C - \mathit{C\_forfeited}]] \\
\quad \text{ELSE } \ \mathit{state}' = [\mathit{state} \\
\qquad\qquad\quad \text{EXCEPT } !.m = \mathit{state}.m + 1, \\
\qquad\qquad\qquad\quad !.\mathit{at\_block} = \mathit{block}, \\
\qquad\qquad\qquad\quad !.\mathit{path} = \mathit{state}.\mathit{path} \circ \text{“v”}]
\end{array}
$$

If it is possible that nothing happens within a period,
the number of states to check grows while all that new states
will be duplicates. It can be said that no action within a period
just means that period is now $2x$ as long, but the overal state
of the contract does not progress.

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

$Enforcement \triangleq$

More than one repayment can happen on a single period,
but extra repayments do cover the subsequent periods,
so we cannot use $state.at\_block$ and need to use
for this check the number of steps taken

IF $PeriodOf(block) > StepsTaken$
THEN $RepaymentMissed$
ELSE UNCHANGED $state$

Invariants

$TypeOK \triangleq$
$\land$ DOMAIN $state = \{$"n", "m", "B", "at_block", "total_repaid", "custody", "path"$\}$
$\land$ $state.n \in 0 \,..\, N$
$\land$ $state.m \in 0 \,..\, M$
$\land$ LET $cdom \triangleq$ DOMAIN $state.custody$
IN IF "Creditor" $\notin cdom$
THEN $\land\ Cardinality(cdom) = 1$
$\land\ cdom \subseteq \{$"Contract", "Debtor_R", "Debtor_E"$\}$
ELSE $cdom = \{$"Creditor", "Debtor_D"$\}$
$\land$ $StepsTaken \leq N * M$

$ConsistentProgress \triangleq$
IF "Contract" $\in$ DOMAIN $state.custody$
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 DOMAIN $state.custody \cap \{$"Debtor_R", "Debtor_E"$\} \neq \{\}$
THEN $state.B = 0 \land state.total\_repaid \geq P$
ELSE TRUE

$ConsistentEnforcement \triangleq$
$NoIdlePeriods \land PeriodOf(block) > 0$
$\Rightarrow (InDefault(state.m,\ PeriodOf(block) - 1)$
$\Rightarrow\ \land$ "Creditor" $\in$ DOMAIN $state.custody$
$\land\ state.custody[$"Creditor"$] + state.custody[$"Debtor_D"$] = C$
$\land\ (state.total\_repaid = 0 \Rightarrow state.custody[$"Creditor"$] = C))$

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

$ConsistentPeriods \triangleq$

$NoIdlePeriods$

$\Rightarrow$ 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 $0 \,..\, S-1$

$\land\ PeriodOf(block) \leq S$

Init & Next

$Init \triangleq$

$\land\ block = START\_BLOCK$

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

$Next \triangleq$

$\land$ DOMAIN $state.custody = \{\text{“Contract”}\}$

$\land\ NoIdlePeriods$

$\land\ \lor\ Repayment \quad \land$ UNCHANGED $block$

$\lor\ Enforcement \quad \land$ UNCHANGED $block$

$\lor\ block' = block + 1 \quad \land$ UNCHANGED $state$

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