

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 behavior 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*

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

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 $RatesLate = 1 \dots M - 1$
 ASSUME $\forall x \in \text{DOMAIN } RatesLate : RatesLate[x] \leq RATE_PRECISION$
 The maximum number of steps in the contract
 CONSTANT *RateCollateralPenalty*
 ASSUME $RateCollateralPenalty \leq RATE_PRECISION$
 CONSTANT *S*
 ASSUME $S \in \text{Max}(\{N, M\}) + 1 \dots (N + M)$
 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*

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

 $ApplyRate(v, r) \triangleq (v * r) \div RATE_PRECISION$

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

 $P_remainder \triangleq P \% N$

 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
 $LimitByBalance(v) \triangleq \text{IF } v + P_remainder \geq state.B \text{ THEN } state.B \text{ ELSE } v$

 “Fraction of *P*” is the installment size
 $FracP \triangleq (P \div N)$

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

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

When *TimelyEnforcement* is in effect, the value returned by *PeriodOf* corresponds to 's' in the prose description
 $\text{PeriodOf}(b) \triangleq (b - \text{START_BLOCK}) \div \text{BLOCKS_IN_PERIOD}$

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

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

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

$\text{RegularRepayment} \triangleq$
 $\text{state}' = [n \mapsto \text{state}.n + 1,$
 $m \mapsto 0,$
 $B \mapsto \text{state}.B - D,$
 $\text{total_repaid} \mapsto \text{state}.total_repaid + \text{RegularRepaymentAmount},$
 $path \mapsto \text{state}.path \circ ">",$
 $at_block \mapsto \text{block},$
 $custody \mapsto \text{IF } \text{state}.B = D \text{ THEN } [\text{Debtor_R} \mapsto C] \text{ ELSE } \text{state}.custody]$

$\text{EarlyRepaymentAmount} \triangleq$
 $\text{state}.B + \text{ApplyRate}(D, \text{RateDue})$
 $+ \text{ApplyRate}((\text{state}.B - D), \text{RateEarly})$
 $+ \text{ApplyLateRate}(\text{LimitByBalance}(\text{FracP} * \text{state}.m),$
 $\text{state}.m)$

$\text{EarlyRepayment} \triangleq$
 $\text{state}' = [\text{state} \text{ EXCEPT } !.B = 0,$
 $!.total_repaid = \text{state}.total_repaid$
 $+ \text{EarlyRepaymentAmount},$
 $!.path = \text{state}.path \circ "!",$
 $!.custody = [\text{Debtor_E} \mapsto C]]$

■

$$\begin{aligned}
\text{Repayment} &\triangleq \\
&\vee \text{RegularRepayment} \\
&\vee \wedge \text{EarlyRepaymentAmount} > \text{RegularRepaymentAmount} \\
&\quad \wedge \text{EarlyRepayment} \\
\\
\text{AmountForCollateralForfeiturePenalty} &\triangleq \\
&\text{Max}(\{\text{state}.B, \text{RegularRepaymentAmount}\}) \\
&+ \text{ApplyRate}(\text{Max}(\{\text{state}.B, \text{RegularRepaymentAmount}\}), \\
&\quad \text{RateCollateralPenalty}) \\
\\
\text{RepaymentMissed} &\triangleq \\
&\text{IF } \text{InDefault}(\text{state}.m + 1, \text{PeriodOf}(\text{block})) \\
&\quad \text{THEN LET } C_{\text{forfeited}} \triangleq \\
&\quad \quad \text{Max}(\{1, \text{Min}(\{C, (C * \text{AmountForCollateralForfeiturePenalty}) \\
&\quad \quad \quad \div P\})\}) \\
&\quad \text{IN } \text{state}' = [\text{state} \\
&\quad \quad \text{EXCEPT } \begin{aligned} &!.m = \text{state}.m + 1, \\ &!.path = \text{state}.path \circ \text{"X"}, \\ &!.custody = [\text{Creditor} \mapsto C_{\text{forfeited}}, \\ &\quad \text{Debtor}_D \mapsto C - C_{\text{forfeited}}] \end{aligned} \\
&\quad \text{ELSE } \text{state}' = [\text{state} \\
&\quad \quad \text{EXCEPT } \begin{aligned} &!.m = \text{state}.m + 1, \\ &!.at_block = \text{block}, \\ &!.path = \text{state}.path \circ \text{"V"} \end{aligned}]
\end{aligned}$$

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 overall state
of the contract does not progress.

$$\text{NoIdlePeriods} \triangleq \text{PeriodOf}(\text{block}) \leq \text{PeriodOf}(\text{state}.at_block) + 1$$

■ *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

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

ConsistentProgress \triangleq

IF “Contract” \in DOMAIN *state.custody*
 THEN
 Early repayment available only before $N - 1$ steps are taken
 \wedge 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 \wedge *state.total_repaid* $\geq P$
 ELSE TRUE

$$\begin{aligned}
\text{ConsistentEnforcement} &\triangleq \\
&\text{NoIdlePeriods} \wedge \text{PeriodOf}(\text{block}) > 0 \\
&\Rightarrow (\text{InDefault}(\text{state}.m, \text{PeriodOf}(\text{block}) - 1) \\
&\quad \Rightarrow \wedge \text{"Creditor"} \in \text{DOMAIN } \text{state}.custody \\
&\quad \wedge \text{state}.custody[\text{"Creditor"}] + \text{state}.custody[\text{"Debtor_D"}] = C \\
&\quad \wedge (\text{state}.total_repaid = 0 \Rightarrow \text{state}.custody[\text{"Creditor"}] = C))
\end{aligned}$$

$$\begin{aligned}
\text{ConsistentRemainder} &\triangleq \\
&(\text{state}.B \geq \text{FracP} \vee \text{state}.B = 0) \quad \text{last payment includes } P_remainder
\end{aligned}$$

$$\begin{aligned}
\text{ConsistentPeriods} &\triangleq \\
&\text{NoIdlePeriods} \\
&\Rightarrow \quad \text{At least one step in each period has to be taken} \\
&\quad \text{when enforcement is on-time} \\
&\quad \wedge \text{PeriodOf}(\text{block}) \leq \text{StepsTaken} + 1 \\
&\quad \text{Can progress over } S \text{ time periods, period index in } 0 \dots S - 1 \\
&\quad \wedge \text{PeriodOf}(\text{block}) \leq S
\end{aligned}$$

Init & Next

$$\begin{aligned}
\text{Init} &\triangleq \\
&\wedge \text{block} = \text{START_BLOCK} \\
&\wedge \text{state} = [n \mapsto 0, m \mapsto 0, B \mapsto P, at_block \mapsto \text{block}, \\
&\quad total_repaid \mapsto 0, path \mapsto "", custody \mapsto [\text{Contract} \mapsto C]]
\end{aligned}$$

$$\begin{aligned}
\text{Next} &\triangleq \\
&\wedge \text{DOMAIN } \text{state}.custody = \{\text{"Contract"}\} \\
&\wedge \text{NoIdlePeriods} \\
&\wedge \vee \text{Repayment} \quad \wedge \text{UNCHANGED } \text{block} \\
&\quad \vee \text{Enforcement} \quad \wedge \text{UNCHANGED } \text{block} \\
&\quad \vee \text{block}' = \text{block} + 1 \quad \wedge \text{UNCHANGED } \text{state}
\end{aligned}$$

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