

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* ≤ *RATE_PRECISION*
 The rates for surcharge on late repayment
 CONSTANT *RatesLate*
 ASSUME DOMAIN *RatesLate* = 1 .. *M* − 1
 ASSUME $\forall x \in \text{DOMAIN } \textit{RatesLate} : \textit{RatesLate}[x] \leq \textit{RATE_PRECISION}$
 The maximum number of steps in the contract
 CONSTANT *RateCollateralPenalty*
 ASSUME *RateCollateralPenalty* ≤ *RATE_PRECISION*
 CONSTANT *S*
 ASSUME *S* ∈ *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 $\triangleq \langle \textit{block}, \textit{state} \rangle$

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

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

P_remainder $\triangleq P \% N$

 The Principal amount is assumed to be much larger than number of periods
 ASSUME *P_remainder* < *P* ÷ 100

 Include the remainder in the last payment
LimitByBalance(*v*) $\triangleq \text{IF } v + \textit{P_remainder} \geq \textit{state.B} \text{ THEN } \textit{state.B} \text{ ELSE } v$

 “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
 $\text{PeriodOf}(b) \triangleq (b - \text{START_BLOCK}) \div \text{BLOCKS_IN_PERIOD}$

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

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

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

$\text{CollateralPenalty} \triangleq \text{ApplyRate}(\text{RegularRepaymentAmount}, \text{RateCollateralPenalty})$

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

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

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

$Repayment \triangleq$
 $\vee RegularRepayment$
 $\vee \wedge EarlyRepaymentAmount > RegularRepaymentAmount$
 $\wedge EarlyRepayment$

$RepaymentMissed \triangleq$
 IF $InDefault(state.m + 1, PeriodOf(block))$
 THEN LET $AmountOwed \triangleq Max(\{state.B,$
 $RegularRepaymentAmount + CollateralPenalty\})$
 $C_forfeited \triangleq Max(\{1, Min(\{C, (C * AmountOwed) \div P\})\})$
 IN $state' = [state$
 $EXCEPT !.m = state.m + 1,$
 $!.path = state.path \circ "X",$
 $!.custody = [Creditor \mapsto C_forfeited,$
 $Debtor_D \mapsto C - C_forfeited]]$
 ELSE $state' = [state$
 $EXCEPT !.m = state.m + 1,$
 $!.at_block = block,$
 $!.path = state.path \circ "v"]$

$Enforcement \triangleq$
 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 $state$

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

Invariants

$TypeOK \triangleq$

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

$ConsistentProgress \triangleq$

$\text{IF "Contract"} \in \text{DOMAIN } state.custody$
 THEN
 $\quad \text{Early repayment available only before } N - 1 \text{ steps are taken}$
 $\quad \wedge \text{IF } StepsTaken < N - 1$
 $\quad \quad \text{THEN } EarlyRepaymentAmount > RegularRepaymentAmount$
 $\quad \quad \text{ELSE } EarlyRepaymentAmount = RegularRepaymentAmount$
 ELSE TRUE

$ConsistentRepayment \triangleq$

$\text{IF } \text{DOMAIN } state.custody \cap \{ \text{"Debtor_R"}, \text{"Debtor_E"} \} \neq \{ \}$
 $\text{THEN } state.B = 0 \wedge state.total_repaid \geq P$
 ELSE TRUE

$ConsistentEnforcement \triangleq$

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

■ $ConsistentRemainder \triangleq$
 $(state.B \geq FracP \vee state.B = 0) \text{ last payment includes } P_remainder$

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

Init & Next

$Init \triangleq$
 $\wedge block = START_BLOCK$
 $\wedge state = [n \mapsto 0, m \mapsto 0, B \mapsto P, at_block \mapsto block,$
 $total_repaid \mapsto 0, path \mapsto "", custody \mapsto [Contract \mapsto C]]$

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

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