

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.

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*

$$\text{Min}(x, y) \triangleq \text{IF } x < y \text{ THEN } x \text{ ELSE } y$$

$$\text{Max}(x, y) \triangleq \text{IF } x > y \text{ THEN } x \text{ ELSE } y$$

Rate 1.51% with $\text{RATE_PRECISION} = 10000$ will be represented as 151
 $\text{RATE_PRECISION} \triangleq 10000$

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 $\text{RateDue} \leq \text{RATE_PRECISION}$

The rate for surcharge on early repayments

CONSTANT RateEarly
 ASSUME $\text{RateEarly} \leq \text{RATE_PRECISION}$

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 S
 ASSUME $S \in Max(N, M) + 1 \dots (N + M)$
 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
 $D \triangleq LimitByBalance(FracP * (state.m + 1))$
 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
 $PeriodOf(b) \triangleq (b - START_BLOCK) \div BLOCKS_IN_PERIOD$
 $StepsTaken \triangleq Len(state.path)$

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

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

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

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

$$\begin{aligned} \text{EarlyRepayment} &\triangleq \\ \text{state}' &= [\text{state} \text{ EXCEPT } !.B = 0, \\ &\quad !.total_repaid = \text{state}.total_repaid \\ &\quad \quad + \text{EarlyRepaymentAmount}, \\ &\quad !.path = \text{state}.path \circ "!", \\ &\quad !.custody = \text{"Debtor!"}] \end{aligned}$$

$$\begin{aligned} \text{Repayment} &\triangleq \\ &\quad \wedge \neg \text{InDefault}(\text{state}.m, \text{PeriodOf}(\text{block})) \\ &\quad \wedge \vee \text{RegularRepayment} \\ &\quad \quad \vee \wedge \text{EarlyRepaymentAmount} > \text{RegularRepaymentAmount} \\ &\quad \wedge \text{EarlyRepayment} \end{aligned}$$

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

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 overall 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

```

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

```

ConsistentProgress \triangleq

```

IF state.custody = "Contract"
  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 state.custody  $\in$  { "Debtor>", "Debtor!" }
  THEN  $\wedge$  state.B = 0
     $\wedge$  state.total_repaid  $\geq$  P
     $\wedge$   $\neg$ InDefault(state.m, PeriodOf(block))
  ELSE TRUE

```

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

$ConsistentRemainder \triangleq$
 $(state.B \geq FracP \vee state.B = 0)$ 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
 $\wedge PeriodOf(block) \leq StepsTaken + 1$
 Can progress over S time periods, period index in $0 \dots S - 1$
 $\wedge PeriodOf(block) \leq S$
 ELSE TRUE

Init & Next

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

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

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