L specification (draft)

Evgenii Balai

June 28, 2015

Contents

1 Syntax

1.1 Symbols

L symbols are non-empty strings of ascii characters divided into the following disjoint categories:

- integer numerals
- identifiers
- special characters

An integer numeral is a string of one or more decimal digits (0-9) possibly preceding by a minus sign

An ***identifier*** is a string of one or more letters, digits and underscore characters beginning with a letter.

A ***special character*** is one of the following characters:

`'>','=','<','+','-','*','-','{','}','(',')',',','.','|'`

A ***symbol*** is an integer numeral, an identifier or a special character.

1.2 Basic Terms

Basic terms are divided into the following categories:

- constants
- variables
- typed variables
- arithmetic terms
- functional terms

A ***constant*** is either an identifier starting with a lowercase letter or an integer numeral.

A ***variable*** is an identifier starting with an uppercase letter.

A ***typed variable*** is a string of the form *id var*, where *id* is an identifier also referred to as *type name* and *var* is a variable.

An ***arithmetic term*** is a string of one of the following forms:

- $-(t)$
- $(t \diamond u)$

where each of t and u is either an integer numeral, a variable, a numeric constant or an arithmetic terms; and $\diamond$ is a special symbol in the set {`'+', '-', '*', '/', '%'`}; (`'%'` stands for modulo operation). Parentheses can optionally be omitted in which case standard operator precedences apply.

A ***functional term*** is a string of the form $f(t_1, \ldots t_n)$ where $t_1, \ldots, t_n$ are basic terms, f is an identifier also referred to as an ***functional symbol*** and $n > 0$.

We will say that a basic term t' is a ***subterm*** of t iff at least one of the following condition holds:

- $t = t'$
- t is of the form $-(t')$
- t is of the form $(t' \diamond t_1)$
- t is of the form $(t_1 \diamond t')$
- t is of the form $f(t_1, \ldots t_n)$ and $t' \in \{t_1, \ldots, t_n\}$
- there exists a term t'' such that t' is a subterm of t'' and t'' is a subterm of t

A term t is called ***ground*** iff

- t is an identifier of an integer numeral; or
- all of the subterms of t other than t itself are ground

1.3 Constant Declarations

A ***constant declaration*** is of the form

$$c = v. \tag{1}$$

where c is an identifier also referred to as ***constant name*** and v is a ground arithmetic term, an integer numeral or an identifier. We will say that the constant c is *defined* by a program if it contains a declaration of the form (1).

1.4 Set Expressions

A ***set expression*** is of one of the following forms:

- $\{t_1, t_2, \ldots, t_n\}$

  where $t_1, \ldots, t_n$ are ground terms.

  A shorthand $\{l..r\}$, where each of l and r is either a constant name, integer numeral or an arithmetic term may be used to represent the set of all integers in the range $n..m$.
- An identifier.
- t `where` V_1 *in* $type_1, \ldots, V_n$ *in* $type_n$

  where t is a term, $\{V_1, \ldots, V_n\}$ is a set of all variables occurring in t and $type_1, \ldots type_n$ are identifiers.
- $(S_1 \diamond S_2)$, where S_1 and S_2 are set expressions and $\diamond$ is a set theoretic operation, one of the special characters in the set $\{+, *, /\}$. Parentheses can be omitted in which case $*$ and $/$ have higher precedence than $+$ and all operations are left-associative.

1.5 Type Declarations

A ***type declaration*** is of the form

$$t = set\_expr. \tag{2}$$

where t is an identifier and set_expr is a set expression defined in section 1.4. We will say that the type t is *defined* by a program if it contains a declaration of the form (2).

1.6 Quantified Terms

A ***quantified term*** is of one of the forms:

- $quantifier\ p$
- `some` t_Var

Where $quantifier$ is an identifier in the set {`every`, `some`}, p is an identifier also referred to as *type*, and t_Var is a typed variable.

We will refer to a quantified term starting with a quantifier `some`(`every`) as an ***existentially quantified***(***universally quantified***).

1.7 Terms

A ***term*** is either a basic term or a quantified term.

1.8 Atoms

Atoms are divided into two categories:

- predicate atoms
- built-in atoms

A ***predicate atom*** is a string of the form $p(t_1, \ldots t_n)$ where p is an identifier also referred to as a ***predicate name*** and $t_1, \ldots, t_n$ are terms.

A ***built-in atom*** is a string of the form $t_1 \preceq t_2$ where t_1 and t_2 are terms and $\preceq \in$ {`'<'`,`'>'`, `'>='`,`'<='`,`'='`,`'<>'`} is a string of special characters.

An atom is called *ground* if all the terms occurring in the atom are ground.

1.9 Sentences

A ***sentence*** is either an atom or an expression of the form (not A), (A or B), (A and B), where A and B are atoms. A sentence of the form A and B can also be written as A, B. Parentheses can be omitted in which case *not* has highest precedence and *or* has the lowest precedence.

1.10 Maybe Literals

A ***maybe literal*** is of the form

$$\texttt{maybe}\ p(t_1, \ldots t_n).$$

where $t_1, \ldots, t_n$ are basic terms.

1.11 Cardinality Constraints

A ***cardinality constraint*** is of the form

$$v_1 <= |\{p(t_1, \ldots t_n)\}| <= v_2.$$

where

1. each of v_1 and v_2 is a ground arithmetic term, integer numeral or a constant name,
2. $t_1, \ldots, t_n$ are basic terms.

1.12 Rules

A ***rule*** can be of the two forms:

$$\textit{head}. \tag{3}$$

or

$$\textit{head} \texttt{ if } \textit{sentence}. \tag{4}$$

Where *head* is either a predicate atom not containing quantified terms, or a maybe literal, or a cardinality constraint.

1.13 Program

A ***program*** is a collection of statements, each of which is either a constant declarations, a type declaration, or a rule.

Constant declarations of a program must satisfy the following conditions:

1. Each constant name must not occur in the left hand side of a constant declaration at most once.
2. Each identifier which is a subterm of the right hand side of a constant declaration must occur in the left hand side of a preceding constant declaration.

Type declarations of a program must satisfy the following conditions:

1. Each type name must occur in the left hand side of a type declaration at most once.
2. Each identifier occurring as a subexpression of an expression on the right hand side of a type declaration must be a type name defined by a preceding type declaration.

Rules of a program must satisfy the following conditions:

1. The leftmost occurrence of any variable V in a rule is preceeded by a type name (also referred to as *the type* of the variable), which can also be preceed by a quantifier. All other occurrences of V are subterms of a basic term.

2. For every typed variable $t\ Var$ the identifier t is a type defined by the program.

3. Every identifier occurring in the rule as a subterm of an arithmetic term is a constant name defined by the program.

4. Every variable occurring in a rule which does not occur in a quantified term also occurs in the head of the rule.

5. Every predicate atom $p(t_1, \ldots, t_n)$ occurring in r does not contain two different variables X and Y such that X occurs in a universally quantified term $everyX$ in r and Y occurs in an existentially quantified term $someY$ in r.

1.14 Language Grammar

1.14.1 Terms

$term$ ::= $basic\_term$ | $quantified\_term$
$basic\_term$ ::= $numeric\_constant$ | $variable$ | $identifier$ | $identifier\ variable$
| $arithmetic\_term$ | $functional\_term$
$arithmetic\_term$ ::= `-(`$T0$`)` | `(`$T0\ infix_1\ T1$`)` | `(`$T1\ infix_2\ T2$`)` |
| $T0\ infix_1\ T1$ | $T1\ infix_2\ T2$
$infix_1$ ::= `+` | `-`
$infix_2$ ::= `*` | `/` | `%`
$infix$ ::= $infix_1$ | $infix_2$
$T0$ ::= $T1$ | $T0\ infix_1\ T1$
$T1$ ::= $T2$ | $T1\ infix_2\ T2$
$T2$ ::= $(T0)$ | $variable$ | $numeric\_constant$ | $identifier$ | $identifier\ variable$
$functional\_term$ ::= $identifier$ `(` $terms$ `)`
$quantified\_term$ ::= $quantifier\ identifier\ variable$ | $quantifier\ identifier$
$quantifier$ ::= `every` | `some`
$basic\_terms$ ::= $basic\_term$ | $basic\_term$ `,` $basic\_terms$
$terms$ ::= $term$ | $term$ `,` $terms$

1.14.2 Constant Declarations

$const\_decl$ ::= $identifier$=$arithmetic\_term$. | $identifier$=$identifier$.
| $identifier$=$numeric\_constant$.

1.14.3 Type Declarations

$type\_decl$ ::= $identifier$ `=` set_expr.
$limit$ ::= $identifier$ | $numeric\_constant$ | $arithmetic\_term$
set ::= $\{[basic\_terms]\}$ [1]
$range$ ::= $\{limit..limit\}$
set_expr ::= $ST0$
set_constr ::= $basic\_term$ `where` $tvars$
$tvars$ ::= $tvar$ | $tvar$ `,`$tvars$

[1] Square brackets around $basic\_terms$ mean that $basic\_terms$ are optional, that is, {} is a valid expression for non-terminal set

$tvar$ ::= $variable$ `in` $identifier$
$ST0$ ::= $ST1$ | $ST0$ + $ST1$
$ST1$ ::= $ST2$ | $ST1$ * $ST2$ | $ST1 \setminus ST2$
$ST2$ ::= ($ST0$) | set | $range$ | set_constr | $identifier$

1.14.4 Atoms

$atom$::= $identifier$[($terms$)] | $built\_in$
$built\_in$ ::= $basic\_term$ op $basic\_term$
op ::= `>` | `<` | `>=` | `<=` | `=` | `!=`

1.14.5 Sentences

$sentence$ ::= $s3$
$s3$ ::= $s2$ | $s3$ `or` $s2$
$s2$ ::= $s1$ | $s2$ `and` $s1$ | $s2$ `,` $s1$
$s1$ ::= $s0$ | `not` $s0$
$s0$ ::= $atom$ | ($s3$)

1.14.6 Maybe Literals

$maybe\_lit$ ::= `maybe` $identifier$($basic\_terms$)

1.14.7 Cardinality Constraints

$bound$ ::= $arithmetic\_term$ | $numeric\_constant$ | $identifier$
$card\_constr$ ::= $bound$ `<=` |{$identifier$($basic\_terms$)}| `<=` $bound$|
$bound$ `<=` |{$identifier$}| `<=` $bound$

1.14.8 Rules

$rule$ ::= $head$.|$head$ `if` $sentence$.
$basic\_terms$ ::= $basic\_term$ | $basic\_term, basic\_terms$
$disj$ ::= $atom$ `or` $atoms$ | $atom$
$head$ ::= $disj$ | $maybe\_lit$ | $card\_constr$

1.14.9 Program

$program$ ::= $statements$
$statements$ ::= $statement$ | $statement$, $statements$
$statement$ ::= $const\_decl$ | $type\_decl$ | $rule$

1.15 Comments

L programs can have comments starting with `/*` and ending with `*/` . For example:

```
/*
 This is a
 multiline comment
```

```
*/
type t = {1,2,3}. /* this is a type declaration */
p(t X) if /* this is a rule */ q(X).
```

2 Semantics

We define the semantics of an L program Π in terms of *models* of P. A model is a set of atoms which, intuitively, satisfies the rules of the program. The notion of satisfiability is defined in section 2.5 with all necessary background provided in sections 2.1 - 2.4.

The semantics of a program P containing a comment coincide with the semantics of the program obtained from P by removing the comments. In the rest of this section we will consider programs not containing comments.

2.1 Constant Declarations

Let Π be an L program starting with constant declaration of the form

$$cn = gar\_term.$$

Where cn is referred to as a constant name and gar_term is a ground arithmetic term. By condition 2 for constant declarations defined in section 1.13, gar_term cannot contain identifiers as subterms, therefore its value v can be obtained as defined in section 2.2.

The models Π coincide with the models of program Π' obtained from Π by:

1. Removing the declaration $cn = gar\_term$.

2. Replacing every subterm of a term Π equal to cn with numeric constant v.

By condition 2 for constant declarations defined in section 1.13, if the program Π' starts another constant declaration, its right hand side cannot contain numeric constants, therefore its semantics can be defined in the same manner as for Π.

Therefore, it is sufficient to define the semantics for programs not containing constant declarations (and, therefore, not containing constant names in arithmetic terms too).

2.2 Arithmetic Terms

A program may contain ground arithmetic terms constructed from integer numerals and operations '+' (plus), '-' (minus), '*' (multiplication), '/' (integer division), '%' (modulo)[2] Each arithmetic term has *a value*. The meaning and precedence of operations '+', '-', '*' is as usual. The operation '/' has the same precedence as '*' and is defined as

$$a/b := sgn(a * b) * (|a|\ div\ |b|)$$

[2]Current implementation allows only numerals in the range -2,147,483,648 to 2,147,483,647. Moreover, correct evaluation for an arithmetic term is guaranteed only if all its subterms have values within the range.

where

1. $sgn(a * b) = \begin{cases} 1 & \text{if } a * b \geq 0 \\ -1 & \text{otherwise .} \end{cases}$

2. for $a \geq 0$ and $b \geq 0$ a *div* b is a floor division, i.e, a *div* b is the largest integer such that $b * (a \ div \ b) \leq a$.

The operation '/' has the same precedence as '*' and is defined as

$$a\%b := a - n * (a/n)$$

All operations are associated from left to right.

The semantics of programs containing undefined arithmetic operations (division by zero or modulo with its second operand equal to zero) is undefined.

2.3 Type Declarations

Type declarations of a program Π define a mapping $\mathscr{D}_\Pi$ from identifiers (also called type names) and set expressions of Π to sets of ground terms. If q is a type name or a sort expression, $\mathscr{D}_\Pi(q)$ denotes the set of ground terms it is mapped to.

The mapping is defined as follows:

1. For every sort expression of the form

$$\{t_1, \ldots, t_n\}$$

   $\mathscr{D}_\Pi(\{t_1, \ldots, t_n\})$ is $\{t_1, \ldots, t_n\}$

2. For every sort expression of the form

$$t \ \texttt{where} \ V_1 \ in \ type_1, \ldots, V_n \ in \ type_n$$

   $\mathscr{D}_\Pi(t \ \texttt{where} \ V_1 \ in \ type_1, \ldots, V_n \ in \ type_n)$ is $\{t | V_1 \in \mathscr{D}_\Pi(type_1), \ldots, V_n \in \mathscr{D}_\Pi(type_n)\}$

3. For every sort expression of the form

$$S_1 \diamond S_2$$

   $\mathscr{D}_\Pi(S_1 \diamond S_2)$ is $\mathscr{D}_\Pi(S_1) \odot \mathscr{D}_\Pi(S_2)$, where $\odot$ is a set operation: union, intersection, or difference when $\diamond$ is $+$, $*$ or $/$ correspondingly.

4. For every type declaration of the form

$$tn = set\_expr$$

   $\mathscr{D}_\Pi(tn)$ is $\mathscr{D}_\Pi(set\_expr)$

In the remainder of the section we will mostly use $\mathscr{D}_\Pi$ to obtain the values which correspond to the type names of Π.

2.4 Programs with Free Variables and Ground Programs

Let Π be an L program and r be a rule of P. A variable V occurring in r is called a *free* variable if at least one of the following conditions is satisfied:

1. V occurs in the head of r, and the head of r is either a sentence or a maybe literal.
2. V occurs in the head of r and in the body of r.

Other variables occurring in r are *quantified* variables.

For a program Π we obtain a corresponding *ground* program Π^g as follows:

1. each rule r containing free variables is replaced with a maximal collection of rules, each of which corresponds to a unique substitution of free variables (together with possibly preceeding type names) with ground terms. A variable v can be replaced with a term f if
   - there in an occurrence of a typed variable $t\ v$ in r, and
   - $f \in \mathscr{D}(t)$
2. each arithmetic term is evaluated as described in section 2.2.

For example, consider the program

```
type1 = {1,2,5}.
type2 = {1,2}.

p(type1 X, type2 Y) if X+Y = 7.
maybe q(type1 X).
1<=|{t(type1 X, type2 Y)}| <= 2 if q(Y).
```

The corresponding ground program is:

```
p(1, 1) if 2 = 7
p(1, 2) if 3 = 7
p(2, 1) if 3 = 7
p(2, 2) if 4 = 7
p(5, 1) if 6 = 7
p(5, 2) if 7 = 7
maybe q(1).
maybe q(2).
maybe q(5).
1<=|{t(type1 X, 1)}| <= 2 if q(1).
1<=|{t(type1 X, 2)}| <= 2 if q(2).
```

Therefore, any program Π can be viewed as a shorthand for the corresponding ground program Π^g. In the following sections we will define the semantics of ground programs.

2.5 Program Models

A model of Π is a set of ground atoms satisfying certain conditions.

To describe the conditions, we first introduce some definitions. We will call a predicate atom $p(t_1, \ldots, t_n)$ *basic* if all the terms $t_1, \ldots t_n$ are basic. Similarly, a sentence is called basic if all the atoms occurring in the sentence are basic.

Definition 1. *(A set ground atoms satisfying a basic predicate atom)*
A set of ground atoms A satisfies a simple predicate atom $p(t_1, \ldots t_n)$ if and only if $p(t_1, \ldots t_n) \in A$.

$\square$

Definition 2. *(A set of ground atoms satisfying a built-in atom)*
A set of ground atoms satisfies a ground built-in atom $t_1 \diamond t_2$ iff one of the following conditions is satisfied:

1. $\diamond$ is $=(\neq)$ and $t_1 = t_2(t_1 \neq t_2)$;
2. $\diamond$ is $< (\leq, \geq, >)$, t_1 and t_2 are integer numerals representing numbers N_1 and N_2 respectively and $N_1 < N_2$ $(N_1 \leq N_2, N_1 \geq N_2, N_1 > N_2)$;
3. $\diamond$ is $< (\leq, \geq, >)$, t_1 and t_2 are identifiers starting with a lowercase letter, and t_1 lexicographically smaller than (smaller than or equal to, greater than or equal to, greater) t_2.

$\square$

The semantics of a program containing a built-in atom $t_1 \diamond t_2$ where $\diamond \in \{<, \leq, \geq, >\}$ is *defined* if and only of both t_1, t_2 are both constants or integer numerals.

Definition 3. *(A set of ground atoms satisfying a basic sentence)*
A set of of ground atoms A satisfies a basic sentence S $(A \vdash S)$ if one of the following conditions is satisfied:

1. S is a basic atom, and $S \in A$
2. S is of the form *not* S', and A does not satisfy S'
3. S is of the form S_1 *or* S_2 (S_1 *and* S_2) and A satisfies one (both) of the sentences S_1 and S_2

$\square$

Let S be a sentence. By S' we denote the sentence obtained from S by replacing each quantified term

$$quantifier\ p$$

with

$$quantifier\ p\ X$$

where X is a variable not occurring in S and unique for each quantified term in S.
Let

- $X_1, \dots X_n$ be the variables occurring in existentially quantified terms of S' of types $Tx_1, \dots, Tx_n$ correspondingly
- $Y_1, \dots Y_m$ be the variables occurring in universally quantified terms of S' of types $Ty_1, \dots, Ty_m$ correspondingly

For a sentence S by $S|_{\{Z_1=z_1,\dots,Z_n=z_n\}}$ we denote the sentence obtained from S by

1. for each variable $Z_i \in \{Z_1, \dots, Z_n\}$ replacing every occurrence of a quantified term
$$quantifier\ p\ Z_i$$
with z_i;
2. replacing all other occurrences of each $Z_i \in \{Z_1, \dots, Z_n\}$ with z_i.

Definition 4. *(A set of ground atoms satisfying a sentence)*
A set of ground terms A satisfies S iff

$$\exists(x_1, \dots, x_n) \in \mathscr{D}(Tx_1)\times\dots\times\mathscr{D}(Tx_n) : \forall(y_1, \dots, y_m) \in \mathscr{D}(Ty_1)\times\dots\times\mathscr{D}(Ty_m) :$$
$$(A \vdash S'|_{\{X_1=x_1,\dots,X_n=x_n,Y_1=y_m,\dots Y_m=y_m\}})$$

□

Definition 5. *(A set of ground atoms satisfying a cardinality constraint)*
Let A be a set of ground atoms and

$$v_1 <= |\{p(t_1, \dots t_n)\}| <= v_2.$$

be a cardinality constraint of a program Π. Let $X_1 \dots, X_n$ be all variables occurring in the constraint and $Tx_1, \dots Tx_n$ be the types of the variables $X_1 \dots, X_n$ correspondingly. Let S be a set of ground atoms of Π of the form $p(t'_1, \dots t'_n)$ each of which is obtained from $p(t_1, \dots t_n)$ by replacing all occurrences of variables with elements of their corresponding types.
A satisfies the constraint $v_1 <= |\{p(t_1, \dots t_n)\}| <= v_2$ iff $v_1 \leq |S| \leq v_2$.

□

As described in section 1.12, program rules may be in one of the two forms. We sometimes say that a rule of the form

$$head.$$

has a body which is satisfied by any set of ground atoms and use a canonical form

$$head\ \texttt{if}\ body.$$

even if the body is not present.

Definition 6. *(A set of ground atoms satisfying a rule)*
A set of ground atoms A satisfies a rule head is either a cardinality constraint or a sentence and one of the following conditions holds:

1. A does not satisfy *body*;
2. A satisfies both *body* and *head*.

$\square$

Definition 7. *(A model of a program)*
Let A be a set of ground atoms of a program Π; M be the sets of all literals l such that Π contains a rule

$$\texttt{maybe}\ l\ \texttt{if}\ body.$$

where *body* is satisfied by A. A is a model of Π if and only if it can be written as a union $M' \cup C$, where

1. M' is $M \cap A$;
2. C is the smallest set of ground literals such that $M' \cup C$ satisfies all the rules of Π whose heads are sentences;
3. $M' \cup C$ satisfies all the rules of Π whose heads are cardinality constraints.

$\square$

Alternative Definition for program models(by Dr.Gelfond)

Definition 8. *(Program reduct)*
Let Π be an L program and A be a set of ground atoms. We obtain an L program Π^A (the *reduct* of Π with respect to S) from Π as follows:

1. For every rule r of Π of the form

   $$\texttt{maybe}\ l\ \texttt{if}\ body.$$

   if *body* is satisfied by S, add the rule l `if`*body* and remove r.
2. For every rule r of Π of the form

   $$\texttt{maybe}\ l\ \texttt{if}\ body.$$

   where *body* is not satisfied by S, remove r.

$\square$

Note that the reduct of Π is an L program not containing rules with maybe literals in heads.

Definition 9. *(A model of a program)*
Let A be a set of ground atoms of a program Π; A is a model of Π if and only if the following conditions are satisfied:

1. A is the mimimal set satisfying the rules of Π^A whose heads are sentences.
2. A satisfies all the rules of Π^A whose heads are cardinality constraints.

$\square$

3 Examples

3.1 Simple Examples

The program Π_1:

```
a.
b if a.
```

has exactly one model $\{a, b\}$.

The program Π_2:

```
a if b.
```

has exactly one model $\{\}$, because it does not contain maybe literals or cardinality constraints, and $\{\}$ is the minimal set of atoms satisfying the only rule of the program.

The program Π_3:

```
t1 = {5,6,7}.
t2 = {0,1,2}
p(t2 N) if q(N+5).
maybe q(t1 N).
1{q(t1 N)}2.
```

has three models:

```
{q(5),q(6),p(1),p(0)};
{q(6),q(7),p(1),p(2)};
{q(5),q(7),p(0),p(2)}.
```

Note that, for example, {`q(5),q(6),p(1),p(0),p(2)`} is not a model of Π_3, because C = {`p(1),p(0),p(2)`} is not the smallest set of ground atoms such that {`q(5),q(6)`} $\cup\, C$ satisfies the rules

```
p(0) if q(5).
p(1) if q(6).
p(2) if q(7).
```

3.2 Safety Obligations

The safety obligations are met if

1. The system requirements have been certified;
2. The process for insuring validation has been followed, and
3. The system has passed all required inspections.

The 3 conditions for meeting safety obligations can be defined by the following L rule:

```
safetyObligationsMet if
   requirementsCertified and
   validationProcessFollowed and
   passed(every requiredInspection).
```

The system requirements are certified if they are sound and complete. This is expressed by the following L rule:

```
requirementsCertified if
   requirementsSound and
   requirementsComplete.
```

The validation process has been followed if sections $A - E$ of code $825/A/6$ have been satisfied. The code sections are represented by identifiers of the form $825\_A\_6\_X$, where X is a character in the range A-Z. The corresponding L rule is:

```
validationProcessFollowed if
   satisfied(code_825_A_6_A) and
   satisfied(code_825_A_6_B) and
   satisfied(code_825_A_6_C) and
   satisfied(code_825_A_6_D) and
   satisfied(code_825_A_6_E).
```

The set of required inspection is represented by a type consisting of two elements:

```
requiredInspection = {epa_i_652_6B_714_A, epa_i_652_6B_714_B}.
```

The first inspection named EPA i/652/6B/714/A is passed if we have completed all required forms and have no EPA safety hearings pending:

```
passed(epa_i_652_6B_714_A) if
   completed(every requiredFromEPA714) and
   not pending(every epaFine_j_652_6B_710_C).
```

The second inspection named EPA i/652/6B/714/B is passed if we have paid all fines required under previous infractions under EPA code j/652/6B/710/C:

```
passed(epa_i_652_6B_714_B) if
   paid(every epaFine_j_652_6B_710_C).
```

All the forms, hearings and infractions mentioned in the previous two definitions are defined by types:

```
epaSafetyHearing = {}.
requiredFromEPA714 = {} .
epaFine_j_652_6B_710_C = {}.
```

A complete program with type declarations and rules put in the right order is given in appendix A

3.3 K-vertex Connectivity of Graphs

A graph is called *K-vertex-connected* (or simply *K-connected*) if it has more than K vertices and remains connected whenever fewer than K vertices are removed.

We consider the undirected graph shown in Figure 1.

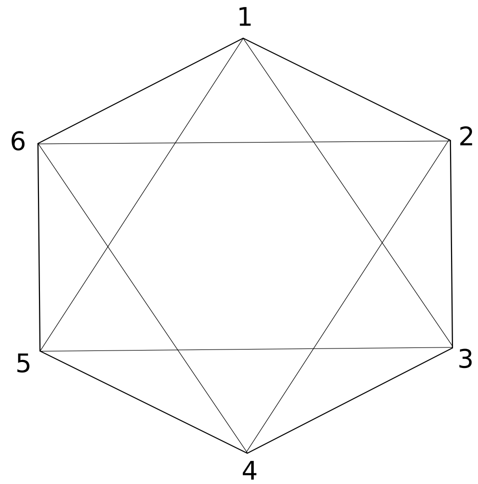

Figure 1: Complete undirected graph with 5 nodes

The number of nodes in the graph is stored in a constant n:

```
n = 5.
```

The number K is also a constant:

```
k = 2.
```

The nodes of the graph are represented with a type *node*.

```
node = {1..n}.
```

The edges of the graph are represented with the facts below. The atom $edge(i, j)$ for integers i and j is true if and only if there is an edge from node i to node j in the graph. The edges are defined as follows[3] :

```
edge(node X, node Y) if X%n = (Y+1)%n.
edge(node X, node Y) if X%n = (Y+2)%n.
```

We will check $K-connectedness$ by trying to remove up to $K-1$ nodes from the graph and checking whether the graphs remains connected. For a node N `removed(N)` is true if N is removed from the graph. Any node may be removed from the graph:

[3]for this example we could also define the edges using a single rule `edge(node X, node Y)`, however we use a more sophisticated description for demonstration purpose. Similar rules can be used to define, for example, graphs with double ring topologies.

```
maybe removed(node N).
```

We are only interesting in the models where less than K nodes are removed:

```
0 <= |{removed(node N)}| <= k-1.
```

To defined the connectedness of a graph, we first define a `reachable(X,Y)` relation, which is true if and only if there exists a path from X to Y in the graph not containing removed nodes:

Any node which wasn't removed is reachable from itself:

```
reachable(node X, X) if not removed(X).
```

A node Y is reachable from node X if they are both not removed and there is an edge from X to Y:

```
reachable(node X,node Y) if edge(X,Y)
                            and not removed(X)
                            and not removed(Y).
```

A node Y is reachable from node X if there exists a node Z reachable from X such that Y is reachable from Z and none of the nodes X,Y,Z was removed:

```
reachable(node X,node Y) if reachable(X,some node Z)
                            and reachable(Z,Y)
                            and not removed(X)
                            and not removed(Y)
                            and not removed(Z).
```

The graph is k-connected if any two nodes that were not removed are reachable from each other. We next define the disconnected relation: the graph is disconnected if there exists a pair of nodes which are not reachable from each other.

```
disconnected if    not reachable(some node X, some node Y)
                   and not removed(X)
                   and not removed(Y).
```

If there exists at least one way to remove at most $k-1$ such that the graph is disconnected, the graph is not k-connected. We can check this by, first, putting a constraint requiring the graph to be disconnected:

```
1<=|{disconnected}|<=1.
```

The graph is not K-connected if and only there exists at least one model of the program.

The program has no models for $k <= 4$ but has a model for $k = 5$. That is, the graph on figure 3.3 is $4 - \textit{connected}$ but not $5 - \textit{connected}$ (for example, the nodes {2,3,4,5} can be removed from the graph to make it disconnected).

A L program for checking safety obligations

```
requiredInspection = {epa_i_652_6B_714_A, epa_i_652_6B_714_B}.
epaSafetyHearing = {}.
requiredFromEPA714 = {} .
epaFine_j_652_6B_710_C = {}.


safetyObligationsMet if
   requirementsCertified and
   validationProcessFollowed and
   passed(every requiredInspection).

requirementsCertified if
   requirementsSound and
   requirementsComplete.

validationProcessFollowed if
   satisfied(code_825_A_6_A) and
   satisfied(code_825_A_6_B) and
   satisfied(code_825_A_6_C) and
   satisfied(code_825_A_6_D) and
   satisfied(code_825_A_6_E).


passed(epa_i_652_6B_714_A) if
   completed(every requiredFromEPA714) and
   not pending(every epaFine_j_652_6B_710_C).


passed(epa_i_652_6B_714_B) if
   paid(every epaFine_j_652_6B_710_C).
```

B L program for checking K-connectivity of a graph

```
n = 5.
k = 2.

node = {1..n}.

edge(node X, node Y) if X%n = (Y+1)%n.
edge(node X, node Y) if X%n = (Y+2)%n.

maybe removed(node N).

0 <= |{removed(node N)}| <= k-1.

reachable(node X, X) if not removed(X).
reachable(node X,node Y) if edge(X,Y)
                            and not removed(X)
                            and not removed(Y).
reachable(node X,node Y) if reachable(X,some node Z)
                            and reachable(Z,Y)
                            and not removed(X)
                            and not removed(Y)
                            and not removed(Z).

disconnected if    not reachable(some node X, some node Y)
                   and not removed(X)
                   and not removed(Y).

1<=|{disconnected}|<=1.
```