ProTem
Eric Hehner

ProTem is a programming system that serves as both programming language and operating system, and includes a theorem prover to check each step of program composition. This document is an informal specification of ProTem. Formal specifications of the data types and program semantics can be found in the book *a Practical Theory of Programming* (with minor syntactic differences).

Programming languages and operating system languages have a lot of functionality in common, but differ greatly in syntax and terminology. These differences are historical, accidental, and unnecessary. They complicate a programmer's life with no benefit. For example, a file is just a variable; file update and storage are just assignment. By unifying the programming language and the operating system commands, both gain in functionality. Communication channels and file piping are as useful in programming as they are in operating systems. Directories and permissions are useful in large-scale multi-programmer programs. Conditional execution (*if*) and indexed loops (*for*) are useful operating system commands.

ProTem is also designed for easy proof of correctness, including functionality, time requirements, and space requirements. To that end, loops can be constructed by labeling any block of code with a specification, and then using the label within the block of code. For example,

\[
\begin{align*}
\langle n \geq 0 \Rightarrow n' = 0 \rangle & \text{ do if } n > 0 \text{ then } n := n - 1. \\
\langle n \geq 0 \Rightarrow n' = 0 \rangle & \text{ fi od }
\end{align*}
\]

The proof methods are the subject of the book *a Practical Theory of Programming*; they do not require preconditions, postconditions, or invariants. If proof is not wanted, then an ordinary identifier can be used as label. For example,

\[
\text{loop do if } n > 0 \text{ then } n := n - 1. \text{ loop fi od}
\]

A primary design criterion is to make ProTem a small, easy-to-learn, easy-to-use language. The size of a language can be measured by the number of symbols and by the complexity of grammar structure, which can be measured by the number of nonterminals. ProTem has 11 keywords. (C has 28, Python has 33, Pascal has 36, Haskell has 37, Ada has 62, MS Basic has 205.) ProTem is presented by a Presentation Grammar, which has just the structure that a programmer needs to know, not all the structure that a parser needs for parsing. There is also an LL(1) grammar and an LR(0) grammar; they are at the end of this document. But we begin the document with the Presentation Grammar. It has 2 nonterminals (program and data) plus some informally defined kinds of names. (The LL(1) grammar has 24 nonterminals; the LR(0) grammar has 12 nonterminals. For comparison, the Haskell grammar has 68 nonterminals, and the Python grammar has 87 nonterminals.) The design ethos demands an extremely good reason for adding a new feature to ProTem that requires a new keyword or syntax. That same design ethos will not tolerate any addition to the 2 nonterminals in the Presentation Grammar.

To judge ease of use, one needs to use the language, but one may get a sense of the ease of use from reading example programs. (One may also get a sense of the beauty of the language from example programs, if that's of interest.) For that purpose, there are example programs near the end of this document.

The language design is complete except for the following. We need to describe and compose graphical elements. We need to define touchpad and touchscreen gestures. We need a sound (noise) data type. We need to define regions of documents and regions of the screen to be clickable links.
Symbols

ProTem uses letters, digits, and a blank space. In addition, there are 11 keywords, plus 4 kinds of lexeme, and 62 other symbols; altogether they are:

```plaintext
if  then  else  fi  new  old  for  do  od  result  unit
number  text   name   comment
"  "  «  »  _  `  :  ::  :=  =
<  >
≤
≥
!  ?  ,  '  ;  .  ;..  ,..  |  ||  (  )  { }  \\
〈
〉
%
+  –
×
/
↑
↓
→
↔
∧
∨
@
†
*
~
¢
$
#
∈
∪
∩
☐
∆
∇
"
```

Some of the ProTem symbols are not found on ASCII keyboards. Here are some substitutes.

- for “ and ” use “
- for ≤ use ≤
- for ≥ use ≥
- for ‘ use ‘
- for ⌣ use ⌣
- for ↑ use ↑
- for ↓ use ↓
- for → use →
- for ↔ use ↔
- for ∧ use ∧
- for ∨ use ∨
- for ∈ use ∈
- for ∪ use ∪
- for ∩ use ∩
- for nand use nand

Predefined functions can be used in place of some symbols.

```plaintext
for  ∈  use  element  for  ∪  use  union  for  ∩  use  intersect  for  ⌣  use  nand
for  ∨  use  nor
```

A number is formed as one or more decimal digits, optionally followed by a decimal point and one or more decimal digits. Here are four examples.

- 0
- 275
- 27.5
- 0.21

A decimal point must have at least one digit on each side of it.

A text begins with a left-double-quote, continues with any number of any characters (but a double-quote (left or right) within a text must be underlined), and concludes with a right-double-quote. Characters within a text are not limited to any alphabet. Here are five examples.

```plaintext
“”
“abc”
“don’t”
“Just say “no”."
“♠♣♥♦”
```

A name is either simple or compound. A simple name is either plain or fancy. A plain simple name begins with a letter (from some alphabet), and continues with any number of letters and digits, except that keywords cannot be names. A fancy simple name begins with «, and continues with any number of any characters (not limited to any alphabet) except « and »; within a fancy simple name, blank spaces are not significant. A compound name is composed of two or more simple names joined with underscore characters. For examples:

- plain simple names: `x` `A1` `george` `refStack`
- fancy simple names: «William & Mary» «x' ≥ x»
- compound names: ProTem_grammars_LL1 DCS_«grad recruiting»_«2016-9-8»

A comment begins with a ` and ends at the end of a line. Characters within a comment are not limited to any alphabet. For example: `I❤ProTem`

Presentation Grammar

At each point in a program, a name is one of

- newname: a simple name that is not defined in the current scope,
- oldname: a simple name that is defined in the current scope,
At each point in a program, an oldname is a name defined as one of: variablename, constantname, dataname, programname, channelname, unitname, or dictionaryname.

There are 29 ways of forming a program. Some examples, explanations, and pronunciations are shown on the right side.

```
new newname : data := data  # create variable : type := initial value
new newname := data         # create constant name and evaluate data
new newname = data           # create data name but don't evaluate data
new newname do program od    # create program name but don't execute program
new newname ? ! data         # create channel name with type
new newname unit             # create measuring unit name
new newname _                # create dictionary name
old oldname                  # forward definition
variablename := data         # remove or hide
channelname ! data           # assign variable to value
to channel send output
channelname ? data           # from channel receive input of this type
input, edit, and echo
channelname ? ! channelname  # create program name and execute program
newname do program od         # execute (call) named program
programname                  # procedure, parameter is constant
⟨ simplename : data → program ⟩
⟨ simplename :: data → program ⟩
⟨ simplename ! data → program ⟩
⟨ simplename ? data → program ⟩
program data                  # procedure, parameter is variable
program variablename         # procedure, parameter is output channel
program channelname          # procedure, parameter is input channel
program dictionaryname       # procedure, data argument
program . program            # procedure, variable argument
program || program           # procedure, channel argument
program . program sequential composition
if data then program fi      # procedure, dictionary argument
if data then program else program fi
for simplename := data do program od  # sequential composition
for simplename := data do program od
for simplename := data do program od
for simplename := data do program od
for simplename := data do program od
for simplename := data do program od
for simplename := data do program od
```

There are 57 ways of expressing data.

```
number
0 1.2
data %
percentage, divide by 100
+ data
plus, identity
– data
minus, negation, not
data + data
plus, addition
data – data
minus, subtraction
data × data
times, multiplication
data / data
by, division
data ↑ data
to the power, exponentiation
data ∧ data
minimum, conjunction, and
data ∨ data
maximum, disjunction, or
data Δ data
negation of minimum, nand
```
data ∨ data
data = data
data ≠ data
data < data
data > data
data ≤ data
data ≥ data
data , data
data ... data
data : data
∉ data
{ data }
¬ data
data ∈ data
data ∪ data
data ∩ data
≠ data
$ data
text
data ; data
data ;.. data
data ↓ data
data < data > data
↔ data
data * data
* data
[ data ]
# data
data † data
data data
data @ data
⟨ simplename : data → data ⟩
data → data
data data
data l data
data ! data
variablename
constantname
dataname
channelname
? channelname
unitname
if data then data else data fi
result simplename : data := data do program od
( data )
Here is the precedence (order of execution) of the forms of program.

0.   if then fi  if then else fi  for do od   do od   ⟨ ⟩   programname
1.   :=  !  ?
2.   ||
3.   .

Program parentheses do od can always be used to group programs differently.

Here is the precedence (order of evaluation) of the forms of data.

0.   number text name ( ) [ ] { } ⟨ ⟩  if then else fi  result do od
1.   juxtaposition % @ left-to-right
2.   + – $ ← # ← $ ? □ * → ↑ ↓ prefix + – $ ← # ← $ ? □ * → ↑ ↓ right-to-left
3.   × / ∩ ∧ ∨ ∆ ∇ infix / left-to-right
4.   + – ↑ ∪ infix – left-to-right
5.   ; ;.. ; infix
6.   , ,.. ; | infix
7.   = ≠ < > ≤ ≥ : ∈ infix continuing

On level 7, the operators are “continuing”. This means, for example, that \( a=b=c \) neither associates to the left \((a=b)=c\) nor associates to the right \(a=(b=c)\), but means \((a=b)\land(b=c)\). Similarly \(a<b=c\) means \((a<b)\land(b=c)\), and so on.

Whenever “data” appears in an alternative for “program”, the most general form of data is allowed, with these exceptions: in a parameter definition, the type must be on precedence level 0; when a function or procedure is argumented, the argument must be on precedence level 0. Any data expression becomes precedence level 0 by putting it in parentheses \((\ )\). Only one alternative for “data” contains “program”, and there the most general form of program is allowed.

Data

ProTem's basic data are numbers, characters, and binary values. ProTem's data structures are bunches, sets, strings, and lists. In addition, there are functions and programmed data.

Numbers

Numbers are not divided into disjoint types. A natural number is an integer number; an integer number is a rational number; a rational number is real number; a real number is a complex number.

In addition to the number symbols, there are predefined names of numbers such as \( pi \) (the ratio of a circle's circumference to its diameter), \( e \) (the base of the natural logarithms), and \( i \) (the imaginary unit, a square root of \(-1\) ). Predefined names can be redefined. The postfix operator \( % \) means division by 100; for examples, 99% , \( x\% \) and \( (x+y)\% \). There are 1-operand prefix operators + and – . There are 2-operand infix operators \(+ x / \uparrow\). There are predefined function names such as \( abs, \ exp, \ log, \ ln, \ sin, \ cos, \ tan, \ ceil, \ floor, \ round, \ re, \ im, \ sqrt, \ div, \) and \( mod \) (see Predefined Names). Division of integers, such as \( 1/2 \), may produce a noninteger. Exponentiation is 2-operand infix \( \uparrow\); for example, \( 1.2 \times 10\uparrow3 \) (one point two times ten to the power three). The operator \( \land \) is minimum (arms down, does not hold water). The operator \( \lor \) is maximum (arms up, holds water). The operator \( \Delta \) is the negation of minimum. The operator \( \nabla \) is the negation of maximum.
Characters

A character is a text of length 1. We leave it to each implementation to list the characters, and to state their order. In addition to the character symbols such as “a” (small a) and “ ” (space), there are six predefined character names: *delete*, *tab*, *newline*, *click*, *doubleclick*, and *end* (the end-of-file character). Predefined functions *suc* and *pre* give the successor and predecessor respectively.

Binary Values

There are two predefined binary constants: *true* and *false*. Negation is –, conjunction is ∧, disjunction is ∨, nand is ∆, nor is ∨.

The infix 2-operand operators = and ± apply to all data in ProTem with a binary result; the two operands may even be of different types. The order operators < > ≤ ≥ apply to real numbers (including rationals, integers, and naturals), to characters, to binary values, to sets (subset, superset), to strings of ordered items, and to lists of ordered items, with a binary result. In the binary order, *false* is below *true*, so ≤ is implication.

Bunches

There are several predefined bunch names:

- *null* empty
- *nat* all natural numbers. Examples: 0, 1, 2
- *int* all integer numbers. Examples: –2, –1, 0, 1, 2
- *rat* all rational numbers. Example: 1/2
- *real* all real numbers. Example: 2↑(1/2)
- *com* all complex numbers. Example: (–1)↑(1/2)
- *char* all characters. Example: “a”
- *bin* both binary values: *true, false*
- *text* all texts (character strings). Example: “abc”
- *pic* all pictures
- *all* all ProTem items

Any number, character, binary value, set, string of elements, and list of elements is an elementary bunch, or synonymously, an element. For example, the number 2 is an elementary bunch, or element. Every expression is a bunch expression, though not all are elementary.

Bunch union is denoted by a comma:

A, B A union B

For example,

2, 3, 5, 7

is a bunch of four integers. There is also the notation

x..y x to y

where x and y are integers or characters that satisfy x≤y. Note that x is included and y is excluded. For example, 0..10 is a bunch consisting of the first ten natural numbers, and 5..5 is the null bunch.

If A and B are bunches, then

A: B A is included in B

is binary. The size of a bunch is ∅. For examples, ∅(0, 1) = 2 and ∅null = 0 and ∅(a..b) = b–a.
Bunches are equal if and only if they consist of the same elements, ignoring order and multiplicity.

In ProTem, all operators whose precedence is before that of bunch union, except $\not\cup$, distribute over bunch union. For examples,

$$-(3,5) = -3,-5$$
$$\ (2,3)+(4,5) = 6,7,8$$

This makes it easy to express the plural naturals ($\text{nat}+2$), the even naturals ($\text{nat}\times2$), the square naturals ($\text{nat}\uparrow2$), the natural powers of two ($2\uparrow\text{nat}$), and many other things.

Nonempty bunches serve as a type structure in ProTem.

Sets

A set is formed by enclosing a bunch in set braces. For examples, \{0, 2, 5\}, \{0,..100\}, \{null\}, \{nat\}. The inverse of set formation is $\sim$. For example, $\sim\{0, 1\} = 0,1$. The size of a set is $\$$. For examples, $\$\{0, 1\} = 2$ and $\$\{null\} = 0$. The element $\in$, union $\cup$, and intersection $\cap$ operators are as usual. Subset is $\leq$, and the other comparisons $<>\geq$ also apply. The power operator $\not\cup$ takes a bunch as operand and produces all sets that contain only elements of the bunch. For example, $\not\cup(0, 1) = \{null\}, \{0\}, \{1\}, \{0, 1\}$.

Strings

There is a predefined string name:

nil the empty string

Any number, character, binary value, list, and function is a one-item string, or synonymously, an item. For example, the number 2 is a one-item string, or item.

String catenation is denoted by a semi-colon:

\[ S \; ; \; T \]

For example,

\[ 2; 3; 5; 7 \]

is a string of four integers. There is also the notation

\[ x..y \]

x to y (same pronunciation as \(x..y\))

where \(x\) and \(y\) are integers or characters that satisfy \(x\leq y\). Again, \(x\) is included and \(y\) is excluded. For examples, \(0..10\) is a string consisting of the first ten natural numbers, and \(5..5 = \text{nil}\).

The length of a string is obtained by the \(\leftrightarrow\) operator. For example, \(\leftrightarrow(2;3;5;7) = 4\).

A string is indexed by the \(\downarrow\) operator. Indexing is from \(0\). For example, \((2;3;5;7)\downarrow2 = 5\). A string can be indexed by a string. For example, \((3;5;7;9)\downarrow(2;1;2) = 7;5;7\).

If \(S\) is a string and \(n\) is an index of \(S\) and \(i\) is any item, then \(S\langle n\rangle\langle i\) is a string like \(S\) except that item \(n\) is \(i\). For example, \((3;5;9)\langle2\rangle\langle8\) = 3; 5; 8.

A text is a more convenient notation for a string of characters.

“abc” = “a”; “b”; “c”

“He said “Hi”.” = “H”; “e”; “” “s”; “ a”; “i”; “d”; “ ” “” “H”; “i”; “” “.”

“abcdefgahj”\(\downarrow(3;6) = \text{def}’’

Strings are equal if and only if they have the same length, and corresponding items are equal.

We allow a bunch of items to be an item in a string. Since string catenation precedes bunch union on the precedence table, we have

\[(3, 4); (5, 6) = 3;5, 3;6, 4;5, 4;6\]

A string is an element (elementary bunch) if and only if all its items are elements.

If \(S\) is a string and \(n\) is a natural number, then

\[n * S \]

is a string, and

\[* S \]

is a bunch of strings. For examples,

\[3*5 = 5;5;5\]
\[3*(4, 5) = 4;4;4, 4;4;5, 4;5;4, 4;5;5, 5;4;4, 5;4;5, 5;5;4, 5;5;5\]
\[*5 = nil, 5, 5;5, 5;5;5, 5;5;5;5, \]

and so on

The * operator distributes over bunch union, but in its left operand only.

\[null*5 = null\]
\[(2,3)*5 = (2*5),(3*5) = 5;5, 5;5;5\]

Using this semi-distributivity, we have

\[*a = nat*a\]

**Lists**

A list is a packaged string. It can be written as a string enclosed in square brackets. For example,

\[ [0; 1; 2] \]

The list operators are length, content, indexing, pointer indexing, catenation, composition, selective union, and comparisons. Let \(L\) and \(M\) be lists, let \(n\) be a natural number, and let \(p\) be a string of natural numbers.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#L \n ~L \n \L \ n \n \L \ @ \ p \n \L \ † \ M \n \L \ † \ M \n i \rightarrow x \mid L</td>
<td>length of (L) \n content of (L) \n (L) at (n), (L) at index (n) \n (L) at (p), (L) at pointer (p) \n (L) concatenate (M), (L) join (M) \n (L) composed with (M) \n (L) otherwise (M), the selective union of (L) and (M) \n index (i) is item (x) and otherwise (L)</td>
</tr>
</tbody>
</table>

plus the comparisons \(L=M\), \(L\neq M\), \(L<M\), \(L>M\), \(L\leq M\), \(L\geq M\).

Here are some examples.

\[#\{0; 1; 2\} = 3\] \nthe number of items in a list
\[\sim\{0; 1; 2\} = 0;1;2\] \nthe content of a list
\[[0...10] 5 = 5\] \nindexing starts at zero
\[[[2; 3]; 4; [5; [6; 7]]] \ @ (2; 1; 0) = 6\]
\[[0...10] \ † \ [10...20] = [0...20]\]
\[[10...20] [3; 6; 5] = [13; 16; 15]\] \nin general, \((L M)n = L(M n)\)

If a list is indexed with a structure, the result has the same structure as the index. For example,

\[ [10; 20] [2; (3, 4); [5; [6; 7]]] = [12; (13, 14); [15; [16; 17]]] \]

By using the \(\@\) operator, a string acts as a pointer to select an item from within an irregular structure. If the list \(L \ † \ M\) is indexed with \(n\), the result is either \(L n\) or \(M n\) depending on whether \(n\) is in the domain \((0,\#L)\) of \(L\). If it is, the result is \(L n\), otherwise the result is \(M n\).
[10; 11] | [0;..10] = [10; 11; 2;..10]
1→21 | [10; 11; 12] = [10; 21; 12]

The index can be a string, as in
(0;1) → 6 | [[0; 1; 2];
[3; 4; 5]] = [[0; 6; 2];
[3; 4; 5]]

When a string or list is indexed by a structure, the result has that same structure as the index. For example, let \( S = 10; 11; 12 \). Then
\[ S\downarrow (0, \{1, [2; 1]; 0\}) = S\downarrow 0, \{S\downarrow 1, [S\downarrow 2; S\downarrow 1]; S\downarrow 0\} = 10, \{11, [12; 11]; 10\}\]

For another example, let \( L = [10; 11; 12] \). Then
\[ L(0, \{1, [2; 1]; 0\}) = L0, \{L1, [L2; L1]; L0\} = 10, \{11, [12; 11]; 10\}\]

Lists are equal if and only if they are the same length and corresponding items are equal. They are ordered lexicographically.
\[ [3; 5; 2] < [3; 6] \]

The list brackets \([\ ]\) distribute over bunch union. For example,
\[ [0, 1] = [0], [1] \]

Thus \([10*nat]\) is all lists of length 10 whose items are natural, and \([4*[6*real]]\) is all 4 by 6 arrays of reals.

Conditional Data

The 3-operand \( \text{if } x \text{ then } y \text{ else } z \text{ fi} \) has binary operand \( x \), but \( y \) and \( z \) are of arbitrary type. For example,
\[ \text{if } reply=\text{“yes”} \text{ then } 0 \text{ else } \text{“nan”} \text{ fi} \]
If \( reply=\text{“yes”} \) has value \( true \), then this data expression has number value 0. If \( reply=\text{“yes”} \) has value \( false \), then this data expression has text value “nan”.

Functions

A function defines a parameter; that is its only job. Let \( p \) (parameter) be any simple name, let \( D \) (domain) be any expression, and let \( B \) (body) be any expression (possibly using \( p \) as a constant name for an element of \( D \)). Then \( \langle p: D \rightarrow B \rangle \) is a function with parameter \( p \), domain \( D \), and body \( B \). For example,
\[ \langle n: nat \rightarrow n+1 \rangle \text{ map } n \text{ in } nat \text{ to } n+1 \]
is the successor function on the natural numbers. The parameter name begins its scope at \( \langle \) and ends its scope at \( \rangle \).

A function with two parameters is just a function of one parameter whose body is a function of one parameter. For example, the maximum function is
\[ \langle a: real \rightarrow \langle b: real \rightarrow \text{if } a>b \text{ then } a \text{ else } b \text{ fi} \rangle \]
Similarly for functions with more than two parameters.

The \( □ \) operator gives the domain of a function. For example, \( □\langle n: nat \rightarrow n+1 \rangle = nat \).
The notation for applying a function to an argument is the same as that for indexing a list: juxtaposition. Also, composition and selective union can have function operands, and even a mixture of list and function operands.

When the body of a function does not use its parameter, there is a syntax that omits the angle brackets $\langle \rangle$ and unused name. For example,

$$2 \rightarrow 3$$

abbreviates $\langle n: 2 \rightarrow 3 \rangle$ or choose any other parameter name.

Allowing the body of a function to be a bunch generalizes the function to a relation. For example, $nat \rightarrow bin$ can be viewed in either of the following two ways: it is a function (with unused and therefore omitted parameter) that maps each natural to $bin$; it is all functions with domain at least $nat$ and range at most $bin$. As an example of the latter view, we have

$$\langle n: nat \rightarrow mod n 2 = 0 \rangle: nat \rightarrow bin$$

Argumentation comes before bunch union in precedence, and so it distributes over bunch union.

$$(f, g) (x, y) = fx, fy, gx, gy$$

Programmed Data

Programmed data allows us to use a program to compute data.

<table>
<thead>
<tr>
<th><code>result</code> simppname : data := data do program od</th>
</tr>
</thead>
</table>

First, a local variable is defined with a type and initial value; its scope (see Scope, next) is from `do` to `od`. Then the program is executed. The result is the final value of the newly defined local variable. We have not yet presented programs, but the following example, which approximates the base of the natural logarithms $e$, should give the idea.

| `result` sum : rat := 1 |
| `do` new term : rat := 1. |
| `for` i := 1;..15 `do` term := term / i. `sum := sum + term` `od` `od` |

There are no side effects. Nonlocal variables become constants within the `result` expression; their values may be used, but assigning them is not permitted. Input and output are not permitted.

All the ways of expressing data can be combined arbitrarily, without restriction. Here is a function whose body is programmed data. It expresses the number of times 2 is a factor of $n$.

$$\langle n: (nat+1) \rightarrow \text{result } f: 0..n := 0 \rangle \text{ do new } m: 1..n+1 := n. \text{ loop do if mod m 2 = 0 then } f := f + 1. \text{ m := m/2. loop fi od od} \rangle$$

A `result` variable begins its scope after the corresponding `do` and ends its scope at the corresponding `od`. Consequently, the `result` variable can be any simple name, even one that has already been defined in the scope that encloses the programmed data.

Scope

A simple name is defined in these ways: by the keyword `new`, as a named program, as a parameter just after $\langle$, as a `for`-index, or as a `result` variable. We shall come to each of these shortly. The scope of a simple name is the part of a program in which the name is defined. We shall also come to the ways of composing larger programs from smaller programs using program brackets `do od`, and conditional programs `if then fi` and `if then else fi`. And we can parameterize data and programs using angle brackets $\langle \rangle$. Scopes are limited by `do od`, `then fi`, `then else`, `else fi`, and $\langle \rangle$. Each
of these five pairs is a scope opener and a scope closer.

A simple name defined using the keyword \texttt{new} must be new, not already defined, since the most recent scope opener. Its scope extends from its definition, through all following sequentially composed programs, to the corresponding scope closer. But it may be covered by a redefinition in an inner scope. Using \texttt{new x = 2} and \texttt{new x = 3} as example definitions, and the program brackets \texttt{do od} as example scope limiters, and letting \texttt{A, B, C, D,} and \texttt{E} stand for arbitrary program forms (but not \texttt{new} or \texttt{old}), in

\begin{verbatim}
  do A. new x = 2. B. do C. new x = 3. D od. E od
\end{verbatim}

the definition of \texttt{x} as the number 2 is not yet in effect in \texttt{A,} but it is in effect in \texttt{B, C,} and \texttt{E}. The definition that makes \texttt{x} the number 3 is in effect in \texttt{D}. None of \texttt{A, B, C, D,} or \texttt{E} can contain a redefinition of \texttt{x} unless it is within further scope limiters \texttt{do od, then fi, then else, else fi,} or \texttt{〈〉}.

A name defined by \texttt{new} can become undefined by the keyword \texttt{old}, ending its scope early. So in

\begin{verbatim}
  new x = 2. A. old x. B
\end{verbatim}

the definition of \texttt{x} is in effect in \texttt{A} but not in \texttt{B}. Within \texttt{B,} the name \texttt{x} has the same meaning (if any) that it had before the definition \texttt{new x = 2}. After \texttt{old x,} the name \texttt{x} is again new and available for definition. However,

\begin{verbatim}
  new x = 2. do old x. A od
\end{verbatim}

is not allowed; a scope cannot be ended by \texttt{old} within a subscope.

A scope can be nested inside another scope, which can be nested inside another, and so on. If a name is defined by \texttt{new} outside all scope limiters, its scope ends only with \texttt{old}. Its scope does not end with the end of a computing session, not even by switching off the power. Variables defined outside all scope limiters serve as “files”.

Outside the outermost scope that you can use, there is a superscope where the predefined names are defined. They are usable in all your scopes unless you cover them by redefining the names. You cannot end the scope of a predefined name.

\section*{Programs}

Some program constructs are concerned with names: creating a name (\texttt{new}), deleting a name (\texttt{old}). Other program constructs are variable assignment, input, output, and a variety of ways of combining programs to form larger programs. All programs, including those that create and delete names, are executed in their turn, just like variable assignments and input and output.

\section*{Variable Definition}

Here is an example variable definition.

\begin{verbatim}
  new x: nat: = 5
\end{verbatim}

This defines \texttt{x} to be a variable assignable to any element in \texttt{nat,} and initially assigned to \texttt{5.} There is no such thing as an “uninitialized variable” nor the “undefined value” in ProTem. In a variable definition, the data after \texttt{:} is called the “type” of the variable, and the data after \texttt{:=} is called the “initial value”. The type can be anything except the empty bunch. The initial value can be any element of the type. The type and initial value can depend on previously defined names, including variables. For example,

\begin{verbatim}
  new y: 0..2×x:= x
\end{verbatim}

defines \texttt{y} as a variable whose value can be any natural number from (including) \texttt{0} up to
(excluding) twice the value of \( x \) at the time this definition is executed, with initial value equal to the current value of \( x \). But the type and initial value cannot make use of the name being defined.

Here are three more examples.

\[
\begin{align*}
\text{new } s & : [10*\text{int} ] := [10*0] \\
\text{new } t & : \text{text} := "" \\
\text{new } u & : (0..20)*\text{char} := "abc"
\end{align*}
\]

In the first example, \( s \) is defined as a variable that can be assigned to any list of ten integers, and is initially assigned to the list of ten zeroes. In the middle example, \( text \) is a predefined bunch equal to \( *\text{char} \), so \( t \) can be assigned to any text, and is initially assigned to the empty text. In the last example, \( u \) is defined as a variable that can be assigned to any text of length less than 20, and is initially assigned to the text “abc”.

**Assignment**

A variable can be reassigned by the assignment notation. Here are two examples using the definitions of the previous subsection.

\[
\begin{align*}
& x := x + 1 \\
& s := 3 \rightarrow 5 \mid s
\end{align*}
\]

The data on the right of \( := \) must be an element in the type of the variable on the left of \( := \). As in the examples, the data on the right of \( := \) can make use of the variable on the left of \( := \).

**Constant Definition**

Here are three constant definitions.

\[
\begin{align*}
\text{new } size & := 10 \\
\text{new } piBy2 & := \pi / 2 \\
\text{new } range & := 0..size
\end{align*}
\]

where \( \pi \) is a predefined constant name.

A constant may use variables to express its value. For example

\[
\text{new } xplus1 := x + 1
\]

The current value of variable \( x \) is used to evaluate \( x + 1 \), and \( xplus1 \) expresses that value. Variable \( x \) may later be reassigned to another value, but that does not affect the value of \( xplus1 \). Constant name \( xplus1 \) cannot be reassigned.

The data on the right of \( := \) cannot make use of the name on the left of \( := \).

**Data Definition**

The data definition

\[
\text{new } xplus2 = x + 2
\]

makes the value of \( xplus2 \) depend on the value of variable \( x \). As \( x \) changes value, \( xplus2 \) changes value so that \( xplus2 = x + 2 \) is always true. In the constant definition of \( xplus1 \) earlier, \( x + 1 \) is evaluated once, at definition time. By contrast, in the data definition of \( xplus2 \), \( x + 2 \) is not evaluated at definition time; it is evaluated every time \( xplus2 \) is used.

A data definition can depend indirectly on a variable. For example,

\[
\text{new } twoxplus4 = 2 \times xplus2
\]

makes \( twoxplus4 \) depend indirectly on the value of variable \( x \).
Data Recursion

In a variable definition, the type and initial value cannot depend on the variable being defined. For example,

\[
\text{new } no: 0..2 \times no := no \text{ \ ` illegal}
\]

is not allowed due to the two occurrences of \( no \) to the right of the colon. Likewise a constant definition cannot be recursive.

Data definition does allow recursion. The next two examples define \textit{fact} and \textit{div} to be the factorial function and integer divisor function for natural numbers.

\[
\text{new } \textit{fact} = 0 \rightarrow 1 \mid \langle n: \text{nat}+1 \rightarrow n \times \textit{fact} (n-1) \rangle
\]

\[
\text{new } \textit{div} = \langle a: \text{nat} \rightarrow \langle d: \text{nat}+1 \rightarrow \\
\quad \text{if } a < d \text{ then } 0 \text{ else if } \text{even } a \text{ then } 2 \times \\
\quad \text{div} (a/2) d \text{ else } 1 + \text{div} (a-d) d \text{ fi fi} \rangle
\]

Here is a bunch of texts (a grammar). This bunch includes the text \( \text{“a+b+a–a”} \), and many more.

\[
\text{new } \textit{exp} = \langle \text{“a”}, \text{“b”}, \text{exp} ; \text{“+”}, \text{exp} ; \text{“-”}, \text{exp} \rangle
\]

This recursive definition is equivalent to the nonrecursive definition

\[
\text{new } \textit{exp} = \langle \text{“a”}, \text{“b”}, \ast((\text{“+”}, \text{“-”}); (\text{“a”}, \text{“b”})) \rangle
\]

Here is a function that eats arguments until it is fed argument 0.

\[
\text{new } \textit{eat} = \langle a: \text{nat} \rightarrow \text{if } a=0 \text{ then } 0 \text{ else } \textit{eat} \rangle
\]

So \( \textit{eat} 5 \ 2 \ 0 = 0 \) and \( \textit{eat} 4 \ 7 \ 3 \ 8 \ 0 = 0 \).

The next example is a pure, baseless recursion.

\[
\text{new } \textit{rec} = \textit{rec}
\]

Whenever \( \textit{rec} \) is used, the computation will be nonterminating.

A final example defines all binary trees with integer nodes.

\[
\text{new } \textit{tree} = \langle \textit{nil}, \textit{tree} ; \text{int} ; \textit{tree} \rangle
\]

Constant Definition versus Data Definition

As already stated, a constant definition evaluates its data once, at definition time, whereas a data definition evaluates its data at each use. If the data is fully evaluated, there is no difference. For example, there is no difference between

\[
\text{new } \textit{five} := 5
\]

\[
\text{new } \textit{five} = 5
\]

When there are no variables used to express the value (neither directly nor indirectly), there is no semantic difference between data definition and constant definition, but there may be an efficiency difference. Here is a trivial example.

\[
\text{new } \textit{csix} := 5+1
\]

\[
\text{new } \textit{dsix} = 5+1
\]

If the definition is never used, \( \textit{dsix} \) is more efficient. If the definition is used once, they are equally efficient. If the definition is used two or more times, \( \textit{csix} \) is more efficient. Here is a more interesting example.

\[
\text{new } \textit{cdouble} := \langle n: (0..10) \rightarrow 2 \times n \rangle
\]

\[
\text{new } \textit{ddouble} = \langle n: (0..10) \rightarrow 2 \times n \rangle
\]

The constant definition \( \textit{cdouble} \) causes the function to be evaluated. That means that the function is applied to all its arguments, and all the results are stored. In effect, the function is evaluated to the
When \texttt{cdouble} is used by applying it to an argument, that argument indexes the list. The data definition \texttt{ddouble} does not evaluate the function. Each time \texttt{ddouble} is used by applying it to an argument, the body of the function is evaluated. Which one is more efficient depends on the size of the domain, the complexity of the result, and the number of times the definition is used.

\textbf{Program Definition}

Program definition gives a program a name, but does not execute the program. For example,

\begin{verbatim}
new switchends do s:= 0 → s 919 → s 0 1 s od
\end{verbatim}

Execution of this definition creates the program name \texttt{switchends}, but does not execute program \texttt{do s:= 0 → s 919 → s 0 1 s od}. After execution of this definition, the name \texttt{switchends} can be used to cause execution of the program it names. Program definitions can be recursive.

Predefined program names include \texttt{asm}, \texttt{await}, \texttt{exec}, \texttt{ok}, \texttt{stop}, \texttt{wait}.

\textbf{Measuring Unit Definition}

There are three predefined units of measurement. They are \texttt{g}, representing mass in grams, \texttt{m}, representing distance in meters, and \texttt{s}, representing time in seconds. A unit of measurement has all the properties of an unknown positive real number constant. So, for example, we write 10×\texttt{m/s} for the speed 10 meters per second. And we can define

\begin{verbatim}
new km:= 1000×m
to make km be a kilometer, and
new h:= 3600×s
to make h be an hour. So 1×\texttt{m/s} = 3.6×\texttt{km/h} evaluates to \texttt{true}. To assign a variable to a quantity with units attached, the variable's type must have compatible units attached. For example,
new speed: real×\texttt{m/s}:= 3.6×\texttt{km/h}
\end{verbatim}

assigns \texttt{speed} to 1×\texttt{m/s}.

You can create a new unit of measurement, unrelated to the existing units. For example,

\begin{verbatim}
new sheet unit
\end{verbatim}

creates a new unit of measurement called the \texttt{sheet}. Now you can define the related units

\begin{verbatim}
new quire:= 25×sheet
new ream:= 20×quire
\end{verbatim}

Now you can define a variable using the new units.

\begin{verbatim}
new order: nat×\texttt{sheet}:= 3×ream
\end{verbatim}

This assigns \texttt{order} to 1500×\texttt{sheet}.

When the value 5×\texttt{m/s} is converted to text by \texttt{numtext}, the result is “5 \texttt{m/s}” without the \texttt{×} sign and without evaluating the unknown real value \texttt{m/s}. Similarly for all units of measurement.

\textbf{Forward Definition}

A forward definition, for example

\begin{verbatim}
new abc
\end{verbatim}

is a notice that a definition will follow later. It is used, for example, when definitions are mutually recursive. In a data definition or program definition, the scope of the name being defined starts immediately. This allows the definitions to be recursive. A forward definition allows mutual
recursion by starting the scope of a data name or program name even before its definition. For example, using \( \cdots \) to stand for uninteresting things, in

\[
\text{new } f := 3. \text{ do new } f. \text{ new } g = \cdots f \cdots g \cdots . \text{ new } f = \cdots f \cdots .
\]

B od

the inner \( f \) and \( g \) are each defined in terms of both of them. Without the forward definition of \( f \) (following \text{ do } ), \( g \) would be defined in terms of the earlier constant definition \text{ new } f := 3 .

Name Removal

Names defined with the keyword \text{ new } can be undefined with the keyword \text{ old } . Ironically, by saying \text{ old } x , the name \( x \) becomes available for reuse as a new name. Even though a name may be undefined, its definition will remain as long as there is an indirect way to refer to it. For example,

\[
\text{new } s: *\text{ all} := \text{ nil.}
\]

\[
\text{new push do } (x: \text{ all} \rightarrow s:= s;x) \text{ od.}
\]

\[
\text{new pop do } s:= s\downarrow(0; \leftrightarrow s – 1) \text{ od.}
\]

\[
\text{new top } = s\downarrow(\leftrightarrow s – 1).
\]

\[
\text{new empty } = s = \text{ nil.
}\]

\text{old } s

The names \( \text{ push } , \text{ pop } , \text{ top } , \) and \( \text{ empty } \) are now defined and ready for use. The name \( s \) was defined for the purpose of defining the other names, and then removed, leaving the other names dependent upon an anonymous variable.

The predefined names include \( \text{ randNat } , \text{ randNatInit } , \) and \( \text{ randNatNext } . \) They might have been defined as:

\[
\text{new big} := 2^{131}.
\]

\[
\text{new rv} := 0; \cdots \text{ big} := 123456789.
\]

\[
\text{new randNat} = (\text{from} : \text{ nat} \rightarrow (\text{to} : \text{ nat} \rightarrow \text{ floor} (\text{from} + (\text{to} – \text{from}) \times \text{rv} / \text{big}))).
\]

\[
\text{new randNatInit do } (\text{seed} : (0; \cdots \text{ big}) \rightarrow \text{rv} := \text{ seed}) \text{ od.}
\]

\[
\text{new randNatNext do } \text{rv} := \text{ mod} (\text{rv} \times 5^{13}) \text{ big} \text{ od.}
\]

\text{old } \text{ big. old } \text{ rv}

Constant \( \text{ big } \) and variable \( \text{ rv } \) are now hidden; their names are removed, but \( \text{ randNat } , \text{ randNatInit } , \) and \( \text{ randNatNext } \) still use them. We can use these definitions as follows:

\( \text{randNatInit} 555555555. \)

\( \text{randNatNext}. \)

\( \text{screen! numtext (randNat 0 10)} \)

The following sequence swaps the data names \( i \) and \( j \).

\[
\text{new } t = i. \text{ old } i. \text{ new } i = j. \text{ old } j. \text{ new } j = t. \text{ old } t
\]

Sequential Composition

Sequential composition is denoted by a period (point, dot). According to the grammar, it is an infix connective; in other words, the period comes between and joins two programs. At the outermost scope, each program is executed in sequence, as soon as it is keyed in. The end of the sequence of keystrokes comprising a program to be executed is recognized by the period that will join it to the sequentially next program, after execution of the just completed program. So, at the outermost (operating system) scope, the period feels more like a program terminator than a program joiner.
Parallel Composition

The parallel composition of programs $P$, $Q$, and $R$ is $P || Q || R$. A variable defined before the parallel composition remains a variable in at most one of the programs in the parallel composition; in all the other programs, it becomes a constant. For example,

```plaintext
new c = a+b.
C
```

In the second parallel composition, variable $a$ can be reassigned in one of the parallel programs, but not in both; it is reassigned in the left program. Likewise variable $b$ can be reassigned in one of the parallel programs, but not in both; it is reassigned in the right program. At the start of $A$, variable $a$ has value 4, constant $b$ has value 2, and data $c$ has value 6. At the start of $B$, constant $a$ has value 1, variable $b$ has value 8, and data $c$ has value 9. At the start of $C$, variable $a$ has value 4, variable $b$ has value 8, and data $c$ has value 12. Parallel programs cannot affect each other through assignments of variables. For co-operation, programs can communicate with each other on channels defined for the purpose (see Channel Definition).

Here is a program to find the maximum value in nonempty list $L$ in $\log (#L)$ time. ( $L$ is a variable, and its initial value is destroyed in the process.) We define $\text{findmax } i \ j$ to find the maximum in the segment of $L$ from index $i$ to index $j$, reporting the result as $L \ i$.

```plaintext
new findmax do \langle i: (0,..#L) \rightarrow \langle j: (1,..#L+1) \rightarrow
      if \ j-i\geq2 \ then \ findmax \ i \ (div \ (i+j) \ 2) \ || \ findmax \ (div \ (i+j) \ 2 \ j).
      L:= i \rightarrow (L \ i \ \lor \ (L \ (div \ (i+j) \ 2) \ \lor \ L \ fi)) \ od
```

After execution of $\text{findmax } 0 \ (#L)$, the maximum value in the initial list is $L \ 0$.

Output and Input

Each channel is defined to transmit a specific type of value. The output channels $\text{screen}$ and $\text{printer}$, and the input channel $\text{keys}$, are predefined to transmit text.

Channel $\text{screen}$ accepts text, which is displayed on the screen. The program

```plaintext
\text{screen! \ "Hi there."}
```

sends the text “Hi there.” to the screen. Output is buffered so it will be available when $\text{screen}$ is ready to receive it. A string of outputs can be sent together

```plaintext
\text{screen! \ "Answer = "; \ \text{numtext } x; \ \text{newline}
```

where $\text{numtext}$ is a predefined function that converts from a number to a text.

The keyboard is a program that runs in parallel with other programs; you don't need to initiate it; it is already running. It monitors what key combinations are pressed, and for what duration, and creates a string of characters. The shift-A combination is a single character “A”. Likewise the control-Q combination is a single character. The click button is just a key like any other; $\text{click}$ is a character, and $\text{doubleclick}$ is a character. And $\text{delete}$, $\text{tab}$ and $\text{newline}$ are characters.

Text from the keyboard (including the click button) can be received from channel $\text{keys}$. Five characters of input are received from channel $\text{keys}$ by saying

```plaintext
\text{keys? 5*char}
```

If input is not yet available, it is awaited. The $\text{delete}$ and $\text{newline}$ characters may be part of the input; no corrections are made. The input is not echoed on the screen. The program

```plaintext
\text{keys? text; newline}
```
reads text up to and including the first newline character. To receive a text that can be interpreted as a signed number, possibly preceded or followed by spaces, ending in a newline character, define

\[ \text{new digit} := \text{"0"}, \text{"1"}, \text{"2"}, \text{"3"}, \text{"4"}, \text{"5"}, \text{"6"}, \text{"7"}, \text{"8"}, \text{"9"} \]

and then input

\[ \text{keys}?: \text{""}; (\text{"+"}, \text{"-"}, \text{"."}); \text{digit}; * \text{digit}; (\text{\"."}; \text{digit}; * \text{digit}; \text{""}); * \text{""}; \text{newline} \]

This grammar is predefined, and named formnum. The least input that fits the pattern is read.

When input is received, it is referred to by the channel name. After the previous example input, we might have the assignment

\[ x := \text{textnum \ keys} \]

where textnum is a predefined function that converts from a text to a number. We may choose to echo the previous input to the screen by saying

\[ \text{screen! \ keys} \]

There is a second form of input that reads from a text channel and simultaneously writes (echoes) what is read on another text channel. For example,

\[ \text{keys?!screen} \]

reads text from channel keys, edited according to delete characters and cut and paste, up to and including the first newline character, and echoes each input character and edit on screen. The newline character is consumed and echoed, but not included in the value of keys.

If c is the name of an input channel, then the input test ?c is a binary expression saying whether there is currently any unread input on channel c.

Channel Definition

The definition

\[ \text{new \ c?!nat} \]

defines c to be a new local channel that transmits naturals. It can be used for output and input. For example,

\[ \text{new \ c?!nat. \ c! 7 \ || \ do \ c? 0 .. 100. \ x := \text{od. old} \ c} \]

assigns x to 7.

The type of the channel cannot use the name of the channel being defined. Only one of the programs that are in parallel with each other can use a channel for output. More than one of the parallel programs can use the same channel for input only if the parallel composition is not sequentially followed by a program that uses that channel for input. When parallel programs read from the same channel, they read the same inputs independently.

Conditional Program

The conditional program if a then b fi is executed as follows: binary expression a is evaluated; if its value is true, then b is executed; if its value is false, then the conditional program has no effect. The conditional program if a then b else c fi is executed as follows: binary expression a is evaluated; if its value is true, then b is executed; if its value is false, then c is executed.

Named Programs

A named program has the syntax

\[ \text{name \ do \ program \ od} \]
The name of a named program must be new, just as if it were defined with the keyword \texttt{new}. But its scope is just within the \texttt{do od} pair that it names. After that, it is again new and can be reused. The name is attached to the program (like a program definition), and the program is executed (unlike a program definition). One purpose of this naming is to make loops. Here is a two-dimensional search for $x$ in an $n \times m$ array $A$ of integers (that is, $A: [n*[m*int]]$).

\begin{verbatim}
new i: nat:= 0.
tryThisI do if i=n then screen! numtext x; " does not occur."
else new j: nat:= 0.
tryThisJ do if j=m then i:= i+1. tryThisI
else if A i j = x then screen! numtext i; " occurs at ";
umtext i; "; numtext j
else j:= j+1. tryThisJ fi fi od fi od
\end{verbatim}

The next example is a fast remainder program, assigning natural variable $r$ to the remainder when natural $a$ is divided by positive natural $d$, using only addition and subtraction.

$r$:= $a$.

\begin{verbatim}
outerloop do if $r \geq d$ then new dd: nat:= d.
innerloop do $r$:= $r$–dd. dd:= dd+dd.
if $r$<$dd$ then outerloop else innerloop fi od fi
\end{verbatim}

The use of a program name is semantically a call; it means the same as replacing it with the program it names (including the \texttt{do od} brackets). The fast remainder example means the same as

$r$:= $a$.

\begin{verbatim}
outerloop
do if $r$\geq$d$
then new dd: nat:= d.
innerloop
do $r$:= $r$–dd. dd:= dd+dd.
if $r$<$dd$ then outerloop else innerloop fi od
\end{verbatim}

The calls \texttt{outerloop} and \texttt{innerloop} were replaced by the programs they name. They reappear, and again they mean the programs they name. Although semantically they are calls, in this example they are tail recursions, so they are implemented as branches (jumps, go to's).

The next example illustrates that named programs provide general recursion, not just tail recursion. It computes $x$:=$f_n$ and $y$:=$f_{n+1}$, where $f_0$, $f_1$, $f_2$, and so on, are the Fibonacci numbers, in $\log n$ time.

\begin{verbatim}
Fib do if $n$=0 then $x$:= 0. $y$:= 1
else if odd $n$ then $n$:= ($n$–1)/2. Fib. $n$:= $x$. $x$:= $x$↑2 + $y$↑2. $y$:= 2$x$*$y$ + $y$↑2
else $n$:= $n$/2 – 1. Fib. $n$:= $x$. $x$:= 2$x$*$y$ + $y$↑2. $y$:= $n$↑2 + $y$↑2 + $x$ fi fi od
\end{verbatim}

A fancy name can be used as a specification. For example,

\begin{verbatim}
« \texttt{$x'$} $x$ » do $x$:= $x$+1 od
\end{verbatim}

The specification on the left \texttt{« $x'$ $x$ »} is implemented (refined, implied) by the program on the right $x$:=$x$+1. If the specification is written within the language that the prover understands, the prover
attempts to prove that the specification is implemented (refined, implied) by the program. If the program makes use of a specification, the inner specification is used in the outer proof. For example, 

« \( x' = 0 \) »  do if \( x \neq 0 \) then \( x := x - 1 \). « \( x' = 0 \) » fi od

In the then-part, the specification « \( x' = 0 \) » means exactly what it says, rather than the program that it names. Thus the use of specifications makes complicated fixed-point semantics unnecessary. If the prover fails to understand the specification, or fails to prove the refinement, it informs the programmer, and treats the specification as just a name.

Suppose a name is defined within a loop. For example, the name \( a \) in

\[
\text{infinitleoop do new } a := \text{“a”}. \\text{screen } a. \text{infinitleoop od}
\]

Executing this loop prints an infinite sequence of the letter “a”. Replacing the call with the called program, it is equivalent to

\[
\text{infinitleoop do new } a := \text{“a”}. \\text{do new } a := \text{“a”}. \\text{screen } a. \text{infinitleoop od od}
\]

In a general recursion, each call opens a new scope, and each new definition hides but does not destroy the previous definition. But when the recursive call is the last action performed in the named program (a tail recursion), the old scope and its definitions cannot be used again, so the new scope replaces the old one; the scopes and variables do not pile up.

Let \( name \) be a new name (not defined in the local scope), and let \( program \) be a program, possibly using the name \( name \). Then the following three lines are equivalent to each other.

\[
\text{name do program od}
\]
\[
\text{do new name do program od. name od}
\]
\[
\text{new name do program od. name. old name}
\]

Indexed Program

This example computes the transitive closure of \( A: [n*[n*bin]] \).

\[
\text{for } j := 0;..n
\]
\[
\text{do for } i := 0;..n
\]
\[
\text{do for } k := 0;..n
\]
\[
\text{do if } A \ i \ j \ \&\ A \ j \ k \ \text{then } A := (i;k) \rightarrow \text{true} | A \text{ fi od od od}
\]

The if then fi can be restated as

\[
A := (i;k) \rightarrow (A \ i \ k \ \lor (A \ i \ j \ \&\ A \ j \ k)) \ \lor \ A
\]

if you prefer. The name being defined by for is known only within the loop body, and it is known there as a constant, and so it is not assignable. We call it a for-index. In the example, each index takes values 0, 1, 2, and so on up to and including \( n-1 \), but not including \( n \).

For a second example, here is the sieve of Eratosthenes.

\[
\text{new } n := 1000.
\]
\[
\text{new prime: } [n*[n*bin]] := [2\text{false}; (n-2)*true].
\]
\[
\text{for } i := 2;..\text{ceil (sqrt n)}
\]
\[
\text{do if prime i then for } j := i;..\text{ceil (n/i)} \text{ do prime := (i}j) \rightarrow \text{false} | \text{prime od fi od}
\]

A for-index is “by initial value”, so

\[
\text{for } i := x; x \text{ do } x := i+1 \text{ od}
\]

increases \( x \) by 1, not 2.

After the := we can have any string expression; the index stands for each item in the string, in sequence. We can also have any bunch expression; the index stands for each element of the bunch, in parallel. As an example (note the use of .. rather than ;.. as earlier),
for $i := 0 .. \#A$ do $A := i \rightarrow 0 \mid A$ od

makes the items of $A$ be 0, in parallel. We can also have a bunch of strings, or a string of bunches, and so on, so that sequential and parallel execution can be nested within each other. (Note: we do not apply distribution or factoring laws; the structure of the expression is the structure of execution.)

A for-index begins its scope after the corresponding do and ends its scope at the corresponding od. Consequently, the for-index can be any simple name, even one that has already been defined in the scope that encloses the for-loop.

Procedures

A program can have a parameter, as in this example.

\[ \langle y: \text{real} \rightarrow x := x \times y \rangle \]

A program with one or more parameters is called a “procedure”. A procedure of $n+1$ parameters is a procedure of 1 parameter whose body is a procedure of $n$ parameters. A procedure can be argumented in the same way that lists are indexed and functions are argumented. The argument provides a value for the parameter. For example,

\[ \langle y: \text{real} \rightarrow x := x \times y \rangle 3 \]

is the same as

\[ x := x \times 3 \]

A procedure's parameter is known only within the procedure body.

In the previous paragraph, the parameter is a constant (note the single colon); it is not assignable. It is “by initial value”, so

\[ \langle i: \text{int} \rightarrow x := i, y := i \rangle (x+1) \]

gives both $x$ and $y$ a final value one greater than $x$’s initial value.

A program can also have a variable parameter, as in this example (note the double colon).

\[ \langle x: \text{int} \rightarrow x := 3 \rangle \]

A procedure with a variable parameter cannot be applied to a variable appearing in the procedure. This example procedure can be applied to any variable, even one named $x$, because the nonlocal name $x$ does not (and cannot) appear in the procedure. The procedure

\[ \langle x: \text{int} \rightarrow x := 3, y := 4 \rangle \]

cannot be applied to variable $y$. The main use for variable parameters is probably to affect many files in the same way; for example, a procedure to sort files.

A program can also have a channel parameter, as in this example.

\[ \langle c! \text{text} \rightarrow c! \text{“abc”} \rangle \]

can be applied to any channel that receives text. A procedure with a channel parameter cannot be applied to a channel appearing in the procedure. This example procedure can be applied to any output channel, even one named $c$, because the nonlocal channel name $c$ does not (and cannot) appear in the procedure. The procedure

\[ \langle c? \text{text} \rightarrow c?. \text{screen!} c \rangle \]

can be applied to any input channel that delivers text. But

\[ \langle c! \text{text} \rightarrow c! \text{“abc”}, d! \text{“def”} \rangle \]

cannot be applied to channel $d$.

The following procedure $pps$ has three channel parameters. On the first, $a$, it reads the coefficients of a rational power series; on the second, $b$, it reads the coefficients of another rational power series; on the last, $c$, it writes the coefficients of the product power series.
new pps do ⟨a? rat → ⟨b? rat → ⟨c! rat →
   a? rat || b? rat. c! a×b.
new a0:= a || new b0:= b || new ?!rat.
   pps a b d
   || do a? rat || b? rat. c! a0×b+a×b0.
   c! a0×b+d+a×b0. loop od od od
⟩⟩⟩ od

Since ⟨ opens a new scope, the parameter can be any simple name, even one that has already been
defined in the enclosing scope. The corresponding ⟩ closes its scope.

Dictionary Definition

Dictionaries are the way you organize your programs and data. You can create as many dictionaries
as you want. To create a new dictionary named abc, write

new abc_

(It does not matter whether there are spaces between the name and the underscore.) Now you can
define names within this dictionary. A name being defined in a dictionary must not already be
defined in that dictionary. Each name in a dictionary is defined, using the keyword new and a
compound name, to be one of the following: a variable name, a constant name, a data name, a
program name, a channel name, a unit name, or a dictionary name. For example,

new abc_x:= 2

defines x in dictionary abc to be the constant 2. (There must not be a space before or after an
underscore in a compound name.) This constant can then be used as abc_x. To define new
dictionary def within dictionary abc write

new abc_def_

(The first underscore is in the compound name abc_def, and it must not have space around it; the
last underscore indicates dictionary definition, and it may and may not have space before it.) When a
name in a dictionary is defined to be a dictionary, this dictionary also contains names, some of which
can be defined as dictionaries, and so on. So a dictionary can be a tree structure. Suppose there is a
dictionary named ProTem within which there is a dictionary named grammars within which there
is a text named LL1. Its name is ProTem_grammars_LL1. You can shorten this name with a new
definition.

new LL1:= ProTem_grammars_LL1

A dictionary that is not within another dictionary obeys the scope rules. In other words, if you define
a dictionary within scope brackets, for example do od, the dictionary becomes undefined at the end
of the scope, just like any other simple name definition. And its scope can be ended early by old.
For example,

old abc

And, like any other simple name, its scope cannot be ended by old within a subscope. When a
dictionary becomes undefined, so do all the names within it. When a name becomes undefined, what
it named remains in existence, anonymously, as long as something refers to it.

Names within a dictionary do not obey the normal scope rules. Instead, they obey the scope rules of
the dictionary they are within. For example, if we define dictionary abc outside a local scope, and
constant x in dictionary abc within the local scope, the definition of x within abc remains in
effect past the end of the local scope because the definition of abc remains in effect. The name
abc_x will no longer be defined when abc is no longer defined. The name abc_x can become
undefined earlier by using old, even within a subscope. For example,
new abc_.  do new abc_x:= 2 od.  screen! abc_x.  do old abc_x od \ abc_x undefined here
The name \(abc_x\) is defined after the first \(\text{do od}\) scope, but not after the second \(\text{do od}\) scope.

In the superscope where the predefined names are defined, there is also a dictionary named \textit{predefined} with all the predefined names in it (except \textit{predefined}). This dictionary has two uses. One use is to uncover a covered predefined name. For example, one of the predefined names is the imaginary number \(i\) (a square root of \(-1\)). You may also want to define a local variable \(i\). If you do, you can still refer to the predefined \(i\) as \textit{predefined}_\(i\) (unless you have also covered the predefined name \textit{predefined} with a redefinition). If predefined name \(i\) is covered by a definition in a scope between the superscope where it is defined and the local scope where you are working, you can retrieve the simple name \(i\) as the imaginary number by the constant definition

\[
\text{new } i:= \text{predefined}_i
\]

To retrieve a covered constant name, use a constant definition (as in the example). To retrieve a covered data name, use a data definition. To retrieve a covered program name, use a program definition. To retrieve a covered measuring unit name, use a constant definition. You cannot retrieve a covered variable name, and you cannot retrieve a covered dictionary name.

Format

Although it is not part of the ProTem language, here are some suggested formatting rules. The choice of alternative depends on the length of component data and programs.

\[
\begin{align*}
A & . B \\
or & \\
A & \ \ |
\end{align*}
\]

\[
\begin{align*}
A & + B \\
or & \\
A & \ |
\end{align*}
\]

\[
\begin{align*}
\text{if } A \text{ then } B \text{ else } C \text{ fi} \\
or & \\
\text{if } A \text{ then } B \text{ else } C \text{ fi} \\
or & \\
\text{if } A \text{ then } B \text{ else } C \text{ fi} \\
or & \\
\text{result } x: A = B \text{ do } C \text{ od} \\
or & \\
\text{result } x: A = B \text{ do } C \text{ od} \\
or & \\
\langle x: A \rightarrow \langle y: B \rightarrow C \rangle \rangle \\
or & \\
\langle x: A \rightarrow y: B \rightarrow C \rangle \\
or & \\
\text{Commands}
\]

There are 7 commands in ProTem. They are not presented in the grammar, and they cannot be part of a stored program. They can be used only by a human at a keyboard. A command may be given at any time; it does not have to respect the grammatical structure of a program; it interrupts execution. Each command is the escape character followed by a word. The commands are:

- \text{esc-edit} enter or exit editor
- \text{esc-abort} abort program
- \text{esc-permit} change dictionary permits
esc-session quit current session and start a new session
esc-undo undo current session
esc-names print the names defined in the current scope or in a dictionary
esc-note attach or modify or retrieve a note to a defined name

Edit

The edit command esc-edit first invokes a dialogue using keys and screen to determine whether you want to create, modify, or delete a definition (variable name, constant name, data name, program name, channel name, or dictionary name), and if you want to modify or delete, which definition. If you want to create or modify, it then invokes an editor. In the editor, esc-edit exits the editor, throws away the old definition that has been modified, and compiles and saves the new definition.

Abort

It is essential to be able to abort the execution of a program, especially if you suspect that its execution will take forever.

Permit

Each dictionary has a read-permit, which determines who can read its contents, and a write-permit, which determines who can add new contents, change the current contents, and delete old contents. A permit is one of:

- no-one but this dictionary's creator
- anyone who knows this dictionary's password
- everyone

The read-permit and the write-permit may be different; the read-password and the write-password may be different. Initially, when a dictionary is created, its read-permit and write-permit are both “no-one but this dictionary's creator”. Only the dictionary's creator can change the permits. A permit is changed by means of the esc-permit command. The command starts a dialogue using keys and screen to ask which dictionary, and set the permits and passwords if necessary.

Permits belong to dictionaries, not to people. Dictionary predefined has read-permit “everyone” and write-permit “no-one but this dictionary's creator”.

Session

Sessions are defined for each user of a multiuser computer for security and error recovery. When the computer is turned on, a session begins. The esc-session command ends a session and starts a new session. When some idle time passes (how much time is a parameter of the system and may be set to infinity), a session ends and a new one begins (just like esc-session). When the computer is turned off, a session ends. In each session, passwords are requested at the first use (reading or writing) of each dictionary that requires a password for that use. A password is not requested twice within the same session for the same use of the same dictionary.

Undo

The command esc-undo undoes a session (except for inputs and outputs and the session text). Implementing it requires capturing the state at the start of a session. On many computers, returning to the prior state may be cheap; nonvolatile memory contains the state as it was at the start of the
current session, and volatile memory contains the current state.

Error recovery can be achieved as follows. The predefined name *session* is a text consisting of all keystrokes since the start of the current session. (This is quite practical: an hour's hard work produces only 10kbytes of keystrokes.) One first performs a session undo; this resets the state except for the keystroke file. One then makes a copy of the keystroke file to capture it at some instant (it is always growing).

```
new copy: text := session
```

One then edits the copy, and then executes the result by writing *exec copy*. This gives us perfectly flexible error recovery for the modest cost of a keystroke file.

Sessions do not define the lifetime of definitions. A definition that is outside all *do od, then fi, then else, else fi,* and *〈 〉* pairs lasts from the execution of the definition (*new*) to the execution of the corresponding name removal (*old*). This may be less than a session, or more than a session.

Turning off the computer should not cut the power instantly, but should first cause any variables whose values are stored in volatile memory (that requires power), and whose values outlast a session, to be saved in nonvolatile memory.

**Names**

The command *esc-names* begins a dialogue using *keys* and *screen* to determine whether you want the names defined in the current scope, or the names defined in a dictionary, and if the latter, which dictionary. It then prints those names on *screen*. It does not print the names in subdictionaries of the selected dictionary.

**Note**

Each definition can optionally have a note attached to it. The note might explain the purpose or use of the definition. It is there to be read by a human, not for execution. A note is very similar to a comment that you would make at the point of definition, but differs in that you can retrieve it anytime.

The command *esc-note* starts a dialogue using *keys* and *screen* to determine which name (simple or compound), and whether you want to attach a new note, modify an existing note, or retrieve an existing note. For example, you may say that you want to attach the note

```
This variable accumulates the sum of the products.
```
to name *x*. Or you may ask for the note attached to predefined name *e*, which prints

```
The base of the natural logarithms.
```

**Miscellaneous**

As a character within a text, the left- and right-double-quote characters must be underlined. For example, “Just say “no”.”. As a character within a text, an underlined left- and right-double-quote character must be underlined again. And so on. Thus every character can occur within a text. But we cannot write a self-reproducing expression with this convention. For that purpose, we need another convention, such as repeating the left- and right-double-quote characters within a text. For example, “Just say ""no""."”. Using this convention, here is a self-reproducing expression (perform the indexing to see what you get).

```
""""↓(0;0;(0;..32);31;31;(1;..31))""""↓(0;0;(0;..32);31;31;(1;..31))
```
The ProTem equivalent of enumerated type is shown here.

```protem
new color:= "red", "green", "blue".
new brush: color:= "red"
```

The ProTem equivalent of the record type (structure type) is as follows.

```protem
new person:= "name" → text | "age" → nat.
```

The fields of `p` can be selected in the usual way, for example

```protem
screen! p "name"
```

prints the text “Josh”. The value of `p` can be changed in the usual ways, such as

```protem
p:= "age" → 17 | p.
p:= "name" → "Amanda" | "age" → 2
```

We can even have a whole file (string) of records

```protem
new file: *person:= nil
```

and catenate new records onto its end.

```protem
file:= file; p
```

The efficiency of pointers is obtained through the use of the predefined function `index`. When applied to a list argument, it yields the deep domain of the list. For example,

```protem
index [10; [11; 12]; 13] = 0 , 1;(0, 1) , 2 = 0 , 1;0 , 1;1 , 2
```

The use of `index` is a signal to the implementation that its strings of natural numbers will be used only as indexes into the list (and the implementation will check that this is so). For example, we can define a linked list `G` as follows.

```protem
new G: [*("name" → text | "next" → index G)]:= ["name" → end | "next" → 0].
new first: index G:= 0.
```

We can use `first` in an arithmetic context, for example

```protem
first:= first+1
```

and similarly for the “next” field of each record of `G`. But we can ultimately use them only as indexes into `G`, for example

```protem
first:= G@first "next"
G:= first → ("name" → "Aaron" | "next" → first) | G
```

With this limited use, the implementation of these indexes can be memory addresses. This way we obtain all the performance benefits of pointers without destroying the logic of our language.

The previous example, with linked list `G`, does not show the full generality of `index`. Here is a tree-structured example.

```protem
new tree = [nil], [tree; all; tree].  
new t: tree:= [nil].  
new p: index t:= nil
```

To move `p` down to the left in the tree we reassign it this way:

```protem
p:= p; 0
```

To move it down to the right, reassign it this way:

```protem
p:= p; 2
```

Thus `p` is a string of indexes indicating a subtree `t@p` of `t`. We can replace this subtree with tree `s` using the assignment

```protem
t:= p → s | t
```

We can express the information at the node indicated by `p` as

```protem
   t@p 1  or  t@(p; 1)
```

and we can replace the information at this node with the integer 6 using the assignment

```protem
   t:= (p;1) → 6 | t
```
To move up in the tree, we just remove the final item of \( p \), and to make that easy, the predefined
\[
\text{new back} = \langle p: (*\text{nat}) \to p\downarrow(0:\ldots\leftrightarrow p-1) \rangle
\]
allows us to move \( p \) up to its parent by writing
\[
p := \text{back} \ p
\]
The \textit{index} function is also useful in \textit{for}-loops. For example,
\[
\text{for } i := \text{index} \ L \text{ do } L := i \to L \ i + 1 \mid L \ od
\]
adds 1 to each item of list variable \( L \), in parallel.

The procedure of some other programming languages is a combination of naming and parameterization. For example,
\[
\text{new transform do } \langle \text{magnification: real } \to \langle \text{translation: real } \to \text{x := magnification} \times \text{x + translation} \rangle \rangle \ od
\]
Here is a procedure with one parameter
\[
\text{new translate do transform} \ 1 \ od
\]
formed by providing one argument to a two-parameter procedure. To provide an argument for just the second parameter is a little more awkward, but not too bad.
\[
\text{new magnify do } \langle \text{magnification: real } \to \text{transform magnification} \ 0 \rangle \ od
\]
We can now obtain a three-times magnification of \( x \) in either of these ways.
\[
magnify \ 3
\]
\[
\text{transform} \ 3 \ 0
\]

In some other programming languages, the “function” is a combination of naming, parameterizing, and programmed data. For example,
\[
\text{new factorial } = \langle n: \text{nat } \to \text{result} f: \text{nat } := 1 \text{ do for } i := 0;..n \text{ do } f := f \times (i + 1) \od \ od\rangle
\]

Exception handling is provided by bunch union and by \( \mid \) or \( \text{if} \). For example,
\[
\text{new divide } = \langle \text{dividend: com } \to \langle \text{divisor: com } \to \text{if divisor } = 0 \text{ then } \text{“zero divide” else dividend} \ / \ \text{divisor} \ fi \ od \rangle
\]
We can state the type of result returned by this function as \( \text{com}, \text{“zero divide”} \)
The implementation will provide the tag to discriminate between the two.

The selective union operator applies its left side to an argument if that argument is in the stated domain of its left side; otherwise it applies its right side. Let us define
\[
\text{new weekday } = \langle d: (0,..7) \to 1 \leq d \leq 5 \rangle
\]
Then in the expression
\[
(\text{weekday} \mid \text{all} \rightarrow \text{“domain error”}) \ i
\]
if \( i \) fails to be an integer in the range \( 0,..7 \), the left side “catches” the exception and “throws” it to the right side, where it is “handled”.

The effect of an input choice connective can be obtained as follows.
\[
\text{inputchoice do if } ?c \text{ then } c? \text{ formnum. } P
\]
\[
\text{else if } ?d \text{ then } d? \text{ formnum. } Q
\]
\[
\text{else inputchoice fi fi od}
\]

At its outermost scope, ProTem functions as an operating system, where programs are executed as soon as they are entered. Unix directories are dictionaries. Unix files are variables. The commands \( \text{esc-names} \) and \( \text{esc-note} \) are the Unix \texttt{ls} and man commands. ProTem’s \texttt{old} is Unix’s rm. The effect of Unix pipes is obtained by channel parameters. For example, suppose \( \text{trim} \) is a procedure to trim
off leading and following blanks and tabs and newlines from text, and \texttt{sort} is a procedure to sort texts. (Please excuse the informal body since it's not the point of the example.)

\begin{verbatim}
new trim do \langle in? text \rightarrow \langle out! text \rightarrow \rangle \rangle repeatedly read from \textit{in}, trim off leading and trailing space, output to \textit{out}, until \textit{end} is read.

The final \textit{end} is output } \textbf{od}.

new sort do \langle in? text \rightarrow \langle out! text \rightarrow \rangle \rangle repeatedly read from \textit{in} until \textit{end} is read and output the sorted texts to \textit{out}. The final \textit{end} is output } \textbf{od}
\end{verbatim}

We can feed the output from \texttt{trim} to the input of \texttt{sort} by defining a channel for the purpose. If the original input comes from \texttt{keys}, and the final output goes to \texttt{screen}, then

\begin{verbatim}
new pipe?!text. trim keys pipe \parallel sort pipe screen. old pipe
\end{verbatim}

Even better:

\begin{verbatim}
new pipe?!text. trim keys pipe \parallel sort pipe screen. old pipe
\end{verbatim}

If \texttt{sort} needs input before it is available from \texttt{trim}, \texttt{sort} waits.

There is no direct counterpart to the import construct or frame construct. It is recommended to place a comment at the head of each major program component saying which nonlocal names are used, and in what way they are used. It is possible for an implementation to recognize them and check these comments. It is also possible for an implementation to generate such comments on request. Here is the format.

`input: on these channels  `output: on these channels  `use: the values of these variables and constants and datanames and units and function names  `assign: these variables  `call: these program names and procedure names  `refer: to these dictionaries

They are transitive through “use” and “call” without requiring the implementation to do a transitive closure (it just checks the comments at the head of the used data names and called program names). Fancy names are a syntax for checkable specifications, but additionally we can include comments

`pre: precondition  `post: postcondition  `inv: invariant

The predefined procedure \texttt{asm} has one text parameter. If the argument represents an assembly-language program, the execution is that of the represented assembly-language program. An implementation may provide procedures for a variety of languages; for example, it may provide a procedure named \texttt{Python}, with one text parameter, whose execution is that of the Python fragment represented by the argument.

ProTem considers object orientation to be a programming style, rather than a programming-language style, or collection of language features. Object-oriented programming (as a style of programming) can be done in ProTem. Data structures, and the functions and procedures that access and update them, can be defined together in one dictionary. If many objects of the same type are wanted, the type can be defined once and used many times.

The predefined name \texttt{pic} is all picture values. It can be used to create a picture-valued variable.

\begin{verbatim}
new p: pic := [x*[y*0]]
\end{verbatim}

The name \texttt{pic} is defined as \texttt{[x*[y*(0..z)]]} where \texttt{x} is the number of pixels in the horizontal direction, \texttt{y} is the number of pixels in the vertical direction, and \texttt{z} is the number of pixel values. A picture can therefore be expressed in the same way as any other two-dimensional array, and one can refer to the pixel in column 3 and row 4 of picture \texttt{p} as \texttt{p 3 4}.
Another predefined name is *movie*, defined as *pic*. The operations on movies are just those of strings, such as catenation. To help in the creation of movies, one of the pixel values should be “transparent”, and one of the operations on pictures should be overlaying one picture on another.

To execute a program stored on someone else’s computer, just invoke that remote program using its full address (computername_programname). For efficiency, it might be best to compile that remote program for your own computer and run it locally. Any nonlocal names (variables, channels, and so on) refer to entities on the computer where the program is compiled.

**Intentionally Omitted Features**

Each of the following suggestions is a syntactic convenience, and it’s no trouble to add to the language. But they make the language larger, and that’s a cost. And they move away from the form needed for verification. So they are not included in ProTem.

- **assertion**
  
  ```
  assert x ≤ y
  ```

- **string item assignment**
  
  ```
  S ↓ 3 := 5
  ```

- **list item assignment**
  
  ```
  L 3 := 5
  L 3 4 := 5
  ```

- **name grouping**
  
  ```
  new x, y: int := 0
  old x, y
  ⟨a, b: nat → a+b⟩
  ⟨a, b: nat → x:= a+b⟩
  ```

- **looping constructs**
  
  ```
  while n > 0 loop n := n – 1 pool
  loop n := n – 1 until n = 0 pool
  loop n := n – 1. exit when n = 0. m := m + 1 pool
  ```

**Implementation Philosophy**

Ideally, an implementation checks whether the text presented to it represents a program, and issues an error message if it does not. That check should include determining whether every variable assignment is to a value that is included in the type of the variable. That determination is most helpful if it can be made before execution; but if not, it is still helpful if it can be made during an execution attempt.

While not an error, there are also expressions that cannot or should not be evaluated further. That presents an implementation problem, but not a semantic problem. For example,

```
screen! numtext (–3)
```

prints –3

We do not evaluate the application of the minus operator to its operand 3, so the implementation prints the operator and operand. Similarly
No general-purpose programming language has ever been, or will ever be, implemented entirely. Every such language is infinite; every implementation is finite. There is always a program too big for the implementation. There is a multitude of size limitations: the parse stack might overflow, the dictionary (symbol table) might be too small, the forward branch fixup list might be exceeded, and so on. It would be ugly to define a programming language by listing all the size limitations of programs. And it would be counter-productive because it would exclude implementations that can accommodate larger programs.

Whenever a program exceeds a size limitation, the implementation should not say “Error: limitation exceeded.”, because the program is not in error. The implementation should say “Sorry: this implementation is too limited to accommodate your program.”. An “error” message tells a programmer to correct the error; there is no other option. A “sorry” message gives the programmer 3 options: change the program to live within the limitation; change the implementation options to increase the limit that was exceeded; take the program to a different implementation.

Natural numbers and integers are usually limited to those that are representable in a specific number of bits, for example, 32 bits. This is a size limitation, just the same as other size limitations. It is uglier to define arithmetic within finite limitations than to define the naturals and the integers. And it is counter-productive to do so, because it excludes an implementation with 64-bit arithmetic. As with other implementation limitations, numeric overflow should not get an “error” message; it should get a “sorry” message.

Floating-point numbers and arithmetic should never be offered as a language feature. The programmer wants rational or real numbers and arithmetic, but may be willing to accept the floating-point approximation for the sake of efficiency. Floating-point, with a specific number of bits, is an implementation limitation. Any alternative to floating-point that increases the accuracy without taking too much time or space should be welcome.

ProTem is a rich programming system, offering many kinds of data and operators on data, and many ways to structure a computation. Some features may be difficult to implement. And some features may be of little use to most programmers. It may be a wise decision not to implement some features. For example, an implementer might decide that in a variable definition, the type must be one of

```
  nat int rat bin text [n*type]
```

where \( n \) is a natural number and \( \text{type} \) is any of these types just listed. An implementer may decide not to implement parallel execution. No-one can complain that the complete language is not implemented, since it is impossible to completely implement any language. But ProTem is defined to allow all type expressions that make sense, so the next implementation can implement programs that previous implementations could not accommodate.
Predefined Names

Here are the predefined names. Each name is one of:

- variable indicated by \texttt{var} (evaluated; assignable)
- constant indicated by \texttt{con} (evaluated; not assignable)
- data indicated by \texttt{dat} (unevaluated; evaluation upon use; not assignable)
- program indicated by \texttt{pro} (unexecuted; execution upon use)
- channel indicated by \texttt{cha}
- unit indicated by \texttt{uni}
- dictionary indicated by \texttt{dic}

Some definitions use \$ or \∃, which are defined in \textit{A Practical Theory of Programming}.

\texttt{abs: com\rightarrow real dat} Absolute value. \texttt{abs x} = \texttt{sqrt (re x ↑ 2 + im x ↑ 2)}.
\texttt{all dat} All ProTem items.
\texttt{arc: com} \rightarrow \$\langle r: real \rightarrow 0 \leq r < 2×\pi \rangle dat The angle or arc of a complex number.
\texttt{arccos: \$\langle r: real \rightarrow -1 \leq r \leq +1 \rangle \rightarrow \$\langle r: real \rightarrow 0 < r < \pi/2 \rangle dat} A trigonometric function.
\texttt{arcsin: \$\langle r: real \rightarrow -1 \leq r \leq +1 \rangle \rightarrow \$\langle r: real \rightarrow 0 < r < \pi/2 \rangle dat} A trigonometric function.
\texttt{arctan: real \rightarrow \$\langle r: real \rightarrow 0 < r < \pi/2 \rangle dat} A trigonometric function.
\texttt{asm pro} A machine-dependent program with one text input parameter. If the input represents an assembly-language program, the execution is that of the represented assembly-language program.
\texttt{await pro} A program with one constant parameter of type \texttt{real\times s}. If the argument represents the present or a past time, its execution does nothing but takes time until the instant given by the argument. If the argument represents the present or a past time, its execution does nothing and takes no time. See \texttt{time} and \texttt{wait} and \texttt{s}.
\texttt{back: *nat \rightarrow *nat dat} \texttt{back (s; i) = s}.
\texttt{bin} = \texttt{true, false con}
\texttt{bintext: bin\rightarrow text con} \texttt{bintext true} = “\texttt{true}” and \texttt{bintext false} = “\texttt{false}”.
\texttt{ceil: real\rightarrow int dat} \texttt{r ≤ ceiling r < r+1}
\texttt{char dat} The characters.
\texttt{charnat: char\rightarrow nat dat} A one-to-one function with inverse \texttt{natchar}.
\texttt{click: char con}
\texttt{com dat} The complex numbers.
\texttt{cos: real \rightarrow \$\langle r: real \rightarrow -1 \leq r \leq +1 \rangle dat} A trigonometric function.
\texttt{cosh: com\rightarrow com dat} A hyperbolic function.
\texttt{cursor: nat; nat dat} A data name whose value is the current cursor position.
\texttt{delete: char con}
\texttt{div: real \rightarrow \$\langle r: real \rightarrow r>0 \rangle \rightarrow int dat} \texttt{div a d} is the integer quotient when \texttt{a} is divided by \texttt{d}.
\texttt{(0 ≤ mod a d < d) \wedge (a = div a d \times d + mod a d)}
\texttt{doubleclick: char con}
\texttt{e = 2.718281828459045} (approximately) \texttt{con} The base of the natural logarithms.
\texttt{element: all\rightarrow all\rightarrow bin dat} An alternative for \$.
\texttt{encode: text\rightarrow text dat} A not easily invertible function.
\texttt{end: char con} The end-of-file character. It is greater than all letters, digits, punctuation marks, \texttt{space}, \texttt{tab}, and \texttt{newline}.
\texttt{eval: text\rightarrow *all dat} If the argument represents a ProTem data expression, the evaluation is that of the represented data. It “unquotes” its argument. In \texttt{eval “x”}, the “x” refers to whatever \texttt{x} refers to at the location where \texttt{eval “x”} occurs.
\texttt{even: int\rightarrow bin dat} A function that says whether its argument is even or odd.
\texttt{exec pro} A program with one text parameter. If the input represents a ProTem program, the
The natural numbers.

The maximum representable integer (machine dependent).

The minimum representable integer (machine dependent).

The imaginary part of a complex number.

The natural logarithm (base $e$).

The common logarithm (base $10$).

A unit representing distance in meters.

To the program that monitors key presses, it is an input channel; to all other programs, it is an output channel.

To the program that handles incoming mail, it is an output channel; to all other programs, it is an input channel.

To the program that handles outgoing mail, it is an input channel; to all other programs, it is an output channel.

If pattern occurs within subject, then match pattern subject is the index of its first occurrence. If not, then match pattern subject = $\leftrightarrow$subject.

The maximum representable integer (machine dependent).

The maximum representable natural (machine dependent).

The minimum representable integer (machine dependent).

The remainder when $a$ is divided by $d$.

An alternative for $\Delta$.

The natural numbers.
nachar: charnat char → char dat A one-to-one function with inverse charnat.
nl: char con The return or newline character.
nil: The empty bunch.
nor: (bin, real)→(bin, real)→(bin, real) dat An alternative for v.
null: The empty bunch.
numtext: com→text dat A text representation of a number. See also form.
odd: int→bin dat
ok: pro A program whose execution does nothing and takes no time.
ord = char, bin, [*ord] dat The ordered type, for which < > ≤ ≥ are defined.
pi = 3.141592653589793 (approximately) con. The ratio of a circle's circumference to its diameter.

\[ \pi = \sqrt{-1} \]

The return or newline character.

Predefined dic A dictionary containing all predefined names except predefined.
printer??text cha To the printer, it is an input channel; to all other programs, it is an output channel.
rndNat: nat→nat dat A reasonably uniform function, dependent on a hidden variable, over
the interval from (including) the first argument to (excluding) the second argument.
rndNatInit: pro A program with one constant natural parameter. Its execution assigns a hidden
variable to the natural value.
rndNatNext: pro A program. Its execution assigns a hidden variable to the next value in a random
sequence.
rndReal: real→real→real dat A reasonably uniform function, dependent on a hidden variable,
over the interval between the arguments.
rndRealInit: pro A program with one constant real parameter. Its execution assigns a hidden
variable to the real value.
rndRealNext: pro A program. Its execution assigns a hidden variable to the next value in a random
sequence.
rat: dat The rational numbers.
re: com→real dat The real part of a complex number.
real: dat The real numbers.
round: real→int dat \( r-0.5 \leq \text{round} \ r < r+0.5 \)
s: real A unit representing time in seconds.
screen??text cha To the screen, it is an input channel; to all other programs, it is an output channel.
session: text dat A text data name whose value is all keystrokes on channel keys since the start of
a session.
sign: real → (−1, 0, 1) dat
sin: real → \$, (r: real → −1 ≤ r ≤ +1) dat A trigonometric function.
sinh: com→com dat A hyperbolic function.
sort: *ord→*ord dat Sorts in nondecreasing order.
sqrt: com→com dat The principle square root.
stop: pro A program whose execution does nothing and takes forever so that no computation can
follow.
subst: all→all→*all→*all dat subst x y s is a string formed from s by replacing all occurrences
of y with x. Substitute x for y in s.
suc: char→char con The character successor function.
tab: char con
tan: (\$, (r: real → −∞ ≤ r ≤ ∞)) → real dat A trigonometric function.
tanh: com→com dat A hyperbolic function.
text = *char dat
textnum: text→com dat If the argument represents a number, possibly preceded by space, tab,
and newline characters, possibly followed by space, tab, and newline characters, the result is the represented number.

texttime: text→(real×s) ∈ A If the argument represents a time, possibly preceded by space, tab, and newline characters, possibly followed by space, tab, and newline characters, the result is the represented time in seconds since 2000 January 1 at 0:00 UTC (the midnight that begins 2000 January 1 at longitude 0). Times before then are negative. For example, texttime “1947 September 16 at 14:24:32.5 UTC–5” = –68675727.5×s.

time?!real×s ∈ A To the time provider, it is an output channel. To all other programs, it is an input channel that gives the current time in seconds since 2000 January 1 at 0:00 UTC (the midnight that begins 2000 January 1 at longitude 0).

timetext: (real×s)→int→text ∈ A Given the time in seconds since 2000 January 1 at 0:00 UTC (the midnight that begins 2000 January 1 at longitude 0), and a time zone, the result is a readable text. Times before then are negative. For example, timetext (–68675727.5×s) (–5) = “1947 September 16 at 14:24:32.5 UTC–5”

trim: text→text ∈ A A text formed from the argument by removing all leading and trailing space, tab, and newline characters.

type: bin ∈ A A binary value.

union: all→all→all ∈ A An alternative for ∪.

wait pro ∈ A A program with one constant parameter of type real×s. If the argument is nonnegative, its execution does nothing but takes the time in seconds given by the argument. If the argument is nonpositive, its execution does nothing and takes no time. See await and time and s.
Example Program

new simport ` a program to simulate portation
do `input: keys time
  `output: screen
  `use: ceil index nat real rat sqrt newline numtext textnum m s nil
  `call: stop await
  ` Distance between control boxes is always 1 m.
  ` Merges do not overlap, so at most 1 corresponding box on the merging portway.
  ` Each divergence has a left branch and a right branch; there’s no “straight”.
  ` Leading to a divergence, boxes record only one square speed.

  ` start of definitions
new km := 1000 × m. new h := 60 × 60 × s. ` kilometer and hour
new maxaccel := 1.5 × m/s². ` maximum deceleration = – maxaccel
new speedlimit := 60 × km/h. ` speed limit is 60 km/h everywhere
new cushion := 1 × s. ` reaction time for all porters
new impatience := 10/s. ` acceleration factor
new maxdistance := ceil (speedlimit↑² / (2 × maxaccel)). ` max search distance ahead
new numpoters := 120.
new numboxes := 7480.
new visualdelaytime := 0.5 × s. ` for human viewing

new porter. ` so porter can be indexed before it is defined

new box: [numboxes * ((“ahead left”, “ahead right”, “behind left”, “behind right”) → index box
  | “beside” → index box
  | “above” → index porter, numpoters
  | (“x”, “y”) → nat )] ` box position on screen
  := [numboxes * ((“ahead left”, “ahead right”, “behind left”, “behind right”) → 0
  | “beside” → 0
  | “above” → numpoters ` indicates no porter above
  | (“x”, “y”) → 0 )].

new porter: [numpoters * (“below” → index box ` what’s beneath
  | “arrival time” → reals ` arrival time at this box
  | “speed” → real × m/s )] ` current speed
  := [numpoters * (“below” → 0
  | “arrival time” → 0 × s
  | “speed” → 0 × m/s )].

new draw do ⟨b: nat, c: (“grey”, “blue”, “red”) → UNFINISHED⟩ od. ` end of draw
 ` draws a box at screen position (box b “x”) (box b “y”) of color c.
 ` “grey” means no porter present, “blue” means porter present, “red” means crash
 ` UNFINISHED because graphical output has not yet been designed

  ` end of definitions, start of initialization
new x: 0..numboxes := 0. ` for input of box number
for b:= 0..numboxes
  do  screen! “What box is ahead-left of box ”; numtext b; “?”.
    keys?!screen. x:= textnum keys.
    box:= (b; “ahead left”) → x l (x; “behind left”) → b l box.
    screen! “What box is ahead-right of box ”; numtext b; “?”.
    keys?!screen. x:= textnum keys.
    box:= (b; “ahead right”) → x l (x; “behind right”) → b l box.
    screen! “What box is beside box ”; numtext b; “?”.
    keys?!screen. box:= (b; “beside”) → textnum keys l box.
    screen! “What are the x and y coordinates of box ”; numtext b; “?”.
    keys?!screen. box:= (b; “x”) → textnum keys l box.
    draw x “grey” od. ` default; may be changed below

for p:= 0..numporters
  do  screen! “Porter ”; numtext p; “ is over what box? ”.
    keys?!screen. x:= textnum keys.
    porter:= (p; “below”) → x l porter. box:= (x; “above”) → p l box.
    draw x “blue” od.
old x.

randNatInit 123456789. ` initialize a random number generator

` end of initialization, start of simulation

infiniloo p; index porter:= 0. ` p:= the porter that arrived at its current position first
new t: realsxs:= 10↑38xs. ` t is a time, and 10↑38 is an approximation to ∞
for q:= 0..numporters
  do if porter q “arrival time” < t then t:= porter q “arrival time”. p:= q fi od.
old t.

new b:= porter p “below”. ` the box below porter p
new bb:= box b “beside”. ` the box beside b; if none then bb=b
new boxesToDo: *[index box; nat×m]:= nil.
  ` queue of boxes to be explored; their distances ahead of porter p
  ` queue is sorted by increasing distance ahead
  ` difference between any two distances in the queue is at most 1

` initialize boxesToDo
if bb = b then boxesToDo:= nil
else if box bb “above” = numporters then boxesToDo:= nil
  else if porter (box bb “above”) “speed” < porter p “speed” then boxesToDo:= nil
    else boxesToDo:= [bb; 0×m] fi fi.
boxesToDo:= boxesToDo; [box b “ahead left”; 1×m].
if box b “ahead left” + box b “ahead right”
then boxesToDo:= boxesToDo; [box b “ahead right”; 1×m] fi.
old b. old bb.

new accel: real×m/s² := maxaccel. ` acceleration for porter p

` using boxesToDo calculate accel for porter p

nextbox do new b := (boxesToDo↓0) 0. ` the box we are looking at
new d := (boxesToDo↓0) 1. ` its distance ahead of porter p
boxesToDo := boxesToDo↓(1;..⇔boxesToDo).
if d ≤ maxdistance
then new desiredspeed = `according to porter pa

〈pa: (index porter, numporters) →
if pa = numporters then speedlimit
else ( sqrt ( porter pa “speed”↑2 + 2×maxaccel×d
+ (maxaccel×cushion)↑2 )
− maxaccel×cushion ) ∧ speedlimit fi ).
accel := ( ( ( desiredspeed (box b “above”)
∧ desiredspeed (porter (box b “beside”) “above”)
− porter p “speed”)
× impatience)
∨ −maxaccel ∧ maxaccel.
if box b “above” = numporters = porter (box b “beside”) “above”
then ` add boxes ahead to queue and continue
boxesToDo := boxesToDo; [box b “ahead left”; d+1×m].
if box b “ahead left” ≠ box b “ahead right”
then boxesToDo := boxesToDo; [box b “ahead right”; d+1×m] fi.
nextbox
else if ⇔boxesToDo > 0 then nextbox fi fi od.

old boxesToDo.

` using accel, move porter p ahead one box
new b: index box := porter p “below”.
box := (b; “porter”) → numporters \ box. draw b “grey”.
randNatNext.
b := box b if randNat 0 2 = 0 then “ahead left” else “ahead right” fi.
if box b “porter” < numporters then draw b “red”. stop fi. ` crash
porter := (p; “below”) → b \ porter. box := (b; “above”) → p \ box. draw b “blue”.
old b.
new speed := sqrt (porter p “speed”↑2 + 2×accel×m) ∧ speedlimit.
porter := (p; “arrival time”) → porter p “arrival time” + 2×m/(porter p “speed” + speed)
| (p; “speed”) → speed
| porter.

old speed. old accel. old p. ` these olds aren’t really necessary

await (time+visualdelaytime).
infinitleoop od od ` end of simport
Another Example Program

` program to compare quote notation lengths with numerator/denominator lengths

`output: screen
`use: even odd nat div bin false true numtext

new shl = \langle n: nat \rightarrow (m: nat \rightarrow \` shift \ n \ left \ m \ places; \ n \times 2^m \result \ r: nat:= n \ do \ for \ i:= 0;..m \ do \ r:= r \times 2 \ od \ od \rangle).

new shr = \langle n: nat \rightarrow (m: nat \rightarrow \` shift \ n \ right \ m \ places; \ floor \ (n \times 2^{-m}) \ or \ div \ n \ (2^m) \result \ r: nat:= n \ do \ for \ i:= 0;.. m \ do \ r:= div \ r \ 2 \ od \ od \rangle).

new gcd = \langle a: (nat+1) \rightarrow \langle b: (nat+1) \rightarrow ` greatest \ common \ divisor \ of \ a \ and \ b \if \ a=b \ then \ a \ else \ if \ a<\ b \ then \ gcd \ a \ (b-a) \ else \ gcd \ (a-b) \ b \ fi \ fi \rangle).

new norm do \langle num:: (nat+1) \rightarrow \langle denom:: (nat+1) \rightarrow ` normalize \ num/denom \new g:= gcd num denom. \num:= num/g. \denom:= denom/g \rangle \ od \rangle.

new count: nat:= 0. ` number of examples
new qlen: nat:= 0. ` total length of quote representations
new rlen: nat:= 0. ` total length of numerator/denominator representations

for length:= 1;..15 do for string:= 0;..(shl 1 length) ` each string of that length
  do for quote:= 0;..length ` each quote position (at least one bit to left of quote)
    do if ` the rightmost bit is 1 or it's to the left of quote or point
      then if ` repeat-normalized
        result repeatnorm: bin:= true
        do new len: nat:= div (length–quote) 2. ` the length of the possibly repeating part
          trythislen do if len>0 \ 1 \ l \ len \ (length–quote)/2
            then new extract = \langle i: nat \rightarrow \langle l: nat \rightarrow ` index \ i \ length \ l \shl \ string \ l \ shr \ string \ (i+l) \ l \rangle \rangle.
          new ex:= extract quote len.
          if ` the negative part is a repetition (twice or more) of ex
           result r: bin = true
           do new i: nat:= quote+len. ` i+len \ length
             iloop do new ey:= extract i len.
               if ex=ey then i:= i+len. ` i\leq \ length
                  if i<\length
                    then iloop
                    else r:= false fi
                 else r:= false fi od od
          then repeatnorm:= false
          else len:= len–1. trythislen fi fi od od
    then for point:= 0;..length+1 ` each point position (right end, interior, left end)
      do if ` the rightmost bit is 1 or it's to the left of quote or point
        odd string \ v \ quote=0 \ v \ point=0
then `convert to numerator/denominator

new num: nat:= shl string (length-quote) – string – shl (shr string quote) length.

if num<0 then num:= –num fi.
new denom: nat:= shl (shl 1 (length-quote) – 1) point.
norm num denom.
`update statistics
count:= count+1. qlen:= qlen+length.
rlen:= rlen+1. `for the sign
loop do num:= div num 2. rlen:= rlen+1.
   if num>0 then loop fi od.
loop do denom:= div denom 2. rlen:= rlen+1.
   if denom>0 then loop fi od fi fi od od od.

screen! “In”; numtext count; “ examples, quote average length = ”;
numtext (qlen/count); “, num/denom average length = ”; numtext (rlen/count).

old shl. old shr. old gcd. old norm. old count. old qlen. old rlen
**LL(1) Grammar**

In this grammar, for each nonterminal, every production except possibly the last begins with a different terminal. So director sets are not needed, and that's a special case of LL(1) that deserves its own name; I suggest LL($\frac{1}{2}$). To parse a program, the parse stack begins with only the program nonterminal on it, and ends empty with no more input. However, ProTem functions as an operating system, parsing and executing each sequent in turn. So the parse stack begins with sequent on top, and . below it. When the stack is empty, the sequent is executed, the parse stack is reinitialized, and parsing resumes.

```
program  sequent aftersequent
sequent   phrase afterphrase
aftersequent . program empty

phrase    new name afternewname
          old name
          do program od arguments
          if data then program elsepart fi arguments
          for name := data do program od
          ( name parameterkind primary \rightarrow program ) arguments
          name aftername

elsepart  else program empty

parameterkind :
          ::
          !
          ?

aftername ::= data
          ! data
          ? echoortype
do program od arguments

echoortype ! name
data

afterphrase || sequent empty

afternewname : data := data
              = data
              := data
              ? ! data
do program od
```
unit
-
empty
data comparand aftercomparand
comparand element afterelement
element item afteritem
item term afterterm
term factor afterfactor
factor # factor
– factor
~ factor
+ factor
? factor
☐ factor
$ factor
↔ factor
primary afterprimary
primary number
text
if data then data else data fi arguments
result name : data := data do program od arguments
{ data }
[ data ] arguments
( data ) arguments
〈 name : primary → data 〉 arguments
name arguments
arguments number arguments
text arguments
if data then data else data fi arguments
result name : data := data do program od arguments
{ data } arguments
[ data ] arguments
( data ) arguments
〈 name : primary → data 〉 arguments
name arguments
empty
A name control procedure is responsible for classifying names. For efficiency, the productions (except possibly the last) for each nonterminal should be placed in order of frequency. The following nonterminals have only one production each, so they can be eliminated: program sequent data comparand element item term.
LR(0) Grammar

The following grammar has no reduce-reduce choices and no shift-reduce choices. It has shift-shift choices. Such a grammar is commonly called LR(0), but it shouldn't be, because a shift action pushes an input symbol onto the parse stack, and therefore a shift action depends on the input symbol. It is a special case of LR(1) that deserves its own name, but not LR(0); I suggest LR(1/2).

To parse a program, the parse stack begins empty, and ends with only the program nonterminal on it and no more input. However, ProTem functions as an operating system, parsing and executing each sequent in turn. So the parse stack begins empty, and ends with . on top and sequent below it. The sequent is executed, the parse stack is reinitialized, and parsing resumes.

```
program     sequent
            program . sequent

sequent     phrase
            sequent || phrase

phrase      new name : data := data
            new name := data
            new name = data
            new name do program od
            new name ? ! data
            new name unit
            new name _
            new name
            old name
            name := data
            name ! data
            name ? data
            name ? ! name
            name do program od
            if data then program fi
            if data then program else program fi
            for name := data do program od
            do program od

procedure   ( name : primary → program )
            ( name :: primary → program )
            ( name ! primary → program )
            ( name ? primary → program )
            procedure argument
            name

data        data = comparand
            data + comparand
            data < comparand
            data > comparand
            data ≤ comparand
            data ≥ comparand
```
data : comparand
data ∈ comparand
comparand

comparand
comparand , element
comparand ... element
comparand | element
comparand < data > element
element

element
element ; item
element .. item
element ` item
item

item
item + term
item – term
item † term
item ∪ term
term

term
term × factor
term / factor
term ∧ factor
term ∨ factor
term △ factor
term ∇ factor
term ∩ factor
factor

factor
+ factor
– factor
c factor
$ factor
↔ factor
# factor
~ factor
? factor
□ factor
‡ factor
* factor
primary * factor
primary → factor
primary ↑ factor
primary ↓ factor
primary
A name control procedure is responsible for classifying names.