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,

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

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

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

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 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 design of ProTem 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 spaces. In addition, there are 11 keywords, plus 4 kinds of lexeme, and 61 other symbols; altogether they are:

```
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 the 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 ↔ use <>  for ∧ use /
for v use \/  for_handling use //  for $ use /$  for □ use []
for < use <l  for > use >r  for “_ and ” use ""

Predefined constants and functions can be used in place of some symbols.

for T use true  for ⊥ use false  for ∧ use nand  for ∨ use nor

A number is formed as one or more decimal digits, with an optional decimal point between digits. A decimal point must have at least one digit on each side of it. Here are four examples.

0  275  27.5  0.21

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.

```
“”  “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 », and ends with » ; 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  AI  george  refStack
fancy simple names:  «William & Mary»  «x’ ≥ x»
compound names:  ProTem_grammars_LL1  DCS_«grad recruiting»_«2016-9-8»

A comment begins with `  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,
- or a compound name that is not defined in its dictionary
- oldname: a simple name that is defined in the current scope,
- or a compound name that is defined in its dictionary
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 28 ways of forming a program. Some examples, explanations, and pronunciations are shown on the right side.

new newname : data := data  
new newname := data  
new newname = data  
new newname do program od  
new newname ? ! data  
new newname unit  
new newname _  
old oldname  
variablename := data  
channelname ! data  
channelname ? data  
channelname ? ! channelname  
newname do program od  
programname  
\{ simplename : data -> program \}  
\{ simplename :: data -> program \}  
\{ simplename ! data -> program \}  
\{ simplename ? data -> program \}  
program data  
program variablename  
program channelname  
program . program  
program || program  
if data then program fi  
if data then program else program fi  
for simplename := data do program od  
do program od

There are 56 ways of expressing data.

number  
data %  
+ data  
– data  
data + data  
data – data  
data \times data  
data / data  
data ↑ data  
\top  
\bot  
data ∧ data  
data ∨ data

0       1.2
percentage, divide by 100
plus, identity
minus, negation, not
plus, addition
minus, subtraction
times, multiplication
divided by, division
to the power, exponentiation
top, true
bottom, false
minimum, conjunction, and, intersection
maximum, disjunction, or, union
data Δ data  

negation of minimum, nand

data ∨ data  

negation of maximum, nor

data = data  

equals, equation

data + data  

not equals, differs from, exclusive or

data < data  

less than, strict implication, strict subset

data > data  

greater than, strict reverse implication, strict superset

data ≤ data  

less than or equal to, implication, subset

data ≥ data  

greater than or equal to, reverse implication, superset

data , data  

bunch union

data ... data  

bunch from (including) to (excluding)
data ‘ data  

bunch intersection

data : data  

bunch inclusion

≠ data  

bunch size

{ data }  

set

~ data  

contents of a set or list

\text{"abc"}  

power

\$ data  

set size

\text{string join}
data ; data  

string from (including) to (excluding)
data ↓ data  

string indexing

data = data > data  

string modification

↔ data  

string length

data * data  

definite repetition

* data  

indefinite repetition

[ data ]  

list

# data  

list length

data ;; data  

list join

data @ data  

list index, function application, composition

data → data  

pointer indexing

\{ \text{ simplenname : data } \rightarrow \text{ data} \}  

function, create constant parameter

data → data  

function, function space

□ data  

domain of a function
data l data  

selective union

variablename  

variable name

constantname  

constant name

dataname  

data name and evaluate data

channelname  
	the most recent data read on the channel

? channelname  

test for presence of unread input on the channel

unitname  

unit name, positive real number constant

if data then data else data fi  

conditional data

result simplenname : data := data do program od  

programmed data, create local variable

( data )  

data parentheses
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. ||.
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. × / △ ∇ left-to-right
4. + – ;; ; ; .. ; infix – left-to-right
5. , .. | ← infix ← left-to-right
6. = ≠ ≤ ≥ : infix continuing
On level 6, 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”, all forms of data are 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 all forms of program are 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 + – \( \times / \uparrow \). There are predefined function names such as \( \text{abs}, \text{exp, log, ln, sin, cos, tan, ceil, floor, round, re, im, sqrt, div, and mod} \) (see Predefined Names). Division of integers, such as \( 1/2 \), may produce a noninteger. Exponentiation is 2-operand infix \( \uparrow \); for example, \( 1.2\times10^{1.3} \) (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 \( \lor \) 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 in the character order.

Binary Values

The two binary constants are ⊤ and ⊥. Negation is _, conjunction is ∧, disjunction is ∨, nand is Δ, 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, ⊥ is below ⊤, 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: ⊤, ⊥`
- `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 ϕ. For examples, ϕ(0, 1) = 2 and ϕ(null) = 0 and ϕ(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 $\nabla$, 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 ($\text{nat} \times 2$), the square naturals ($\text{nat} \uparrow 2$), 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\}, \{\text{null}\}, \{\text{nat}\}. The inverse of set formation is the content operator $\sim$. For example, $\sim\{0, 1\} = 0, 1$. The size of a set is $\mid \cdot \mid$. For examples, $\mid\{0, 1\}\mid = 2$ and $\mid\{\text{null}\}\mid = 0$. The element relation, traditionally written $x \in S$, is written $x \sim S$ in ProTem. The union operator, traditionally $\cup$, is $\lor$ in ProTem. The intersection operator, traditionally $\cap$, is $\land$. Subset, traditionally $\subseteq$, is $\leq$; strict subset is $<$; superset is $\supseteq$; strict superset is $>$. The power operator $\mathcal{S}$ takes a bunch as operand and produces all sets that contain only elements of the bunch. For example, $\mathcal{S}(0, 1) = \{\text{null}\}, \{0\}, \{1\}, \{0, 1\}$.

Strings

There is a predefined string name:

\[\text{nil} \quad \text{the empty string}\]

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 join is denoted by a semi-colon:

\[S : T \quad \text{\textit{S join T}}\]

For example,

\[2; 3; 5; 7\]

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

\[x..y \quad \text{\textit{x to y (same pronunciation as x..y) }}\]

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 examples, $\leftrightarrow(2; 3; 5; 7) = 4$, and $\leftrightarrow(x..y) = y-x$.

A string is indexed by the $\downarrow$ operator. Indexing is from 0. For example, $(2; 3; 5; 7) \downarrow 2 = 5$. 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 $S \preceq n \succ i$ is a string like $S$ except that item $n$ is $i$. For example, $(3; 5; 9) \preceq 2 \succ 8 = 3; 5; 8$.

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

\[\text{“abc” = “a”; “b”; “c”}\]

\[\text{“He said “Hi”” = “H”; “e”; “”; “s”; “a”; “i”; “d”; “”; “”; “H”; “i”; “”;}\]
“abcdefghij”↓(3;..6) = “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 join 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

$n * S$ ` $n$ copies of $S$ or $n$ S's

is a string, and

$* S$ ` strings of $S$ or any number of $S$'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, join, 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.

$# L$ ` length of $L$

$~ L$ ` content of $L$

$L n$ ` $L$ at $n$ , $L$ at index $n$

$L @ p$ ` $L$ at $p$ , $L$ at pointer $p$

$L ;; M$ ` $L$ join $M$

$L \backslash; M$ ` $L$ composed with $M$

$L | M$ ` $L$ otherwise $M$ , the selective union of $L$ and $M$

$i \rightarrow x \backslash L$ ` index $i$ is item $x$ and otherwise $L$

plus the comparisons $L=M$ , $L+M$ , $L<M$ , $L>M$ , $L\leq M$ , $L\geq M$

Here are some examples.

$#[0; 1; 2] = 3$ ` the number of items in a list

$~[0; 1; 2] = 0;1;2$ ` the content of a list

$[0;..10] 5 = 5$ ` indexing starts at zero

$[ [ 2; 3 ]; 4; [ 5; [ 6; 7 ] ] ] @ (2; 1; 0) = 6$

$[0;..10];[10;..20] = [0;..20]$

$[10;..20] [3; 6; 5] = [13; 16; 15]$ ` in 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 \( L \mid M \) 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 \( M \ n \).

\[
\begin{align*}
[10; 11] \mid [0..10] &= [10; 11; 2;..10] \\
1 \rightarrow 21 \mid [10; 11; 12] &= [10; 21; 12]
\end{align*}
\]

The index can be a string, as in

\[
(0;1) \rightarrow 6 \mid [[0; 1; 2]; [3; 4; 5]] = [[0; 6; 2]; [3; 4; 5]]
\]

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

\[
S \downarrow 0, \{1, [2; 1]; 0\}
\]

\[
= 10, \{11, [12; 11]; 10\}
\]

For another example, let \( L = [10; 11; 12] \). Then

\[
L \ 0, \{1, [2; 1]; 0\}
\]

\[
= 10, \{11, [12; 11]; 10\}
\]

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 \( \top \), then this data expression has number value \( 0 \). If \( reply=\text{"yes"} \) has value \( \bot \), then this data expression has text value \( \text{"nan"} \).

**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,

\( \langle n: \text{nat} \rightarrow n+1 \rangle \)

`map n in nat 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 of \( n+1 \) parameters is a function of 1 parameter whose body is a function of \( n \) parameters. For example, the maximum function

\( \langle a: \text{real} \rightarrow \langle b: \text{real} \rightarrow \text{if } a>b \text{ then } a \text{ else } b \text{ fi} \rangle \)

has two parameters.
The □ operator gives the domain of a function. For example, □(n: nat → n+1) = nat.

The notation for applying a function to an argument is the same as that for indexing a list: juxtaposition. If f is a function of two parameters, then f x y applies f to x and y. 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 ⟨⟩ and unused name. For example,

2 → 3

abbreviates ⟨n: 2 → 3⟩ 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 → 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

⟨n: nat → mod n 2 = 0⟩: nat → 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.

result simplename : data := data do program od

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 program; 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.

⟨n: (nat+1) → result f: 0..n:= 0
do new m: 1..n+1:= n.
loop do if mod m 2 = 0 then f:= f+1. m:= m/2. loop fi od od⟩

A result-variable begins its scope after 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 ⟨, 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 `< >`. Scopes are limited by `do od`, `then fi`, `then else`, `else fi`, and `< >`. Each of these five pairs is a scope opener and a scope closer.

A simple name defined using the keyword `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 `new x = 2` and `new x = 3` as example definitions, and the program brackets `do od` as example scope limiters, and letting `A`, `B`, `C`, `D`, and `E` stand for arbitrary program forms (but not `new` or `old`), in

```
do A. new x = 2. B. do C. new x = 3. D od. E od
```

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

A name defined by `new` can become undefined by the keyword `old`, ending its scope early. So in

```
new x = 2. A. old x. B
```

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

```
new x = 2. do old x. A od
```

is not allowed; a scope cannot be ended by `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 `new` outside all scope limiters, its scope ends only with `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.

**Programs**

Some program constructs are concerned with names: creating a name (`new`), deleting a name (`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.

**Variable Definition**

Here is an example variable definition.

```
new x: nat:= 5
```

This defines `x` to be a variable assignable to any element in `nat`, and initially assigned to 5. There is no such thing as an "uninitialized variable" nor the "undefined value" in ProTem. In a variable definition, the data after `:` is called the "type" of the variable, and the data after `:=` 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,

```
new y: 0..2*x:= x
```
defines \( y \) as a variable whose value can be any natural number from (including) 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.

```
new s: [10*int]:= [10*0]
new t: text:= ""
new u: (0..20)*char:= "abc"
```

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 \( *char \), 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.

```
x:= x+1
s:= 3 → 5 \mid s
```
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.

```
new size:= 10
new piBy2:= pi / 2
new range:= 0..size
```

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

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

```
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

```
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 \( \top \). 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,

```
new twoplus4 = 2*xplus2
```

makes `twoplus4` 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,

```
new no: 0..2*no := no  ` 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 `fact` and `div` to be the factorial and integer divisor function for natural numbers.

```
new fact = 0 \rightarrow 1 | n: (nat+1) \rightarrow n \times fact (n–1)
```

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

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

```
new exp = "a", "b", exp; "+"; exp, exp; "–"; exp
```

This recursive definition is equivalent to the nonrecursive definition

```
new exp = "a", "b", *(("+", "–"); ("a", "b"))
```

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

```
new eat = \langle a: nat \rightarrow \text{if } a=0 \text{ then } 0 \text{ else eat fi} \rangle
```

So `eat 5 2 0 = 0` and `eat 4 7 3 8 0 = 0`.

The next example is a pure, baseless recursion.

```
new rec = rec
```

Whenever `rec` is used, the computation will be nonterminating.

A final example defines all binary trees with integer nodes.

```
new tree = [nil], [tree; int; tree]
```

## 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

```
new five := 5
```

```
new 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.

```
new csix := 5+1

new dsix = 5+1
```

If the definition is never used, `dsix` is more efficient. If the definition is used once, they are equally efficient. If the definition is used two or more times, `csix` is more efficient. Here is a more interesting example.
new cdouble:= (n: (0..10) → 2×n)
new ddouble = (n: (0..10) → 2×n)

The constant definition 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 list

[0; 2; 4; 6; 8; 10; 12; 14; 16; 18]

When cdouble is used by applying it to an argument, that argument indexes the list. The data definition ddouble does not evaluate the function. Each time 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.

Program Definition

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

new switchends do s:= 0 → s 9 | 9 → s 0 | s od

Execution of this definition creates the program name switchends, but does not execute program do s:= 0 → s 9 | 9 → s 0 | s od. After execution of this definition, the name switchends can be used to cause execution of the program it names. Program definitions can be recursive.

Predefined program names include asm, await, exec, ok, stop, wait.

Measuring Unit Definition

There are three predefined units of measurement. They are g, representing mass in grams, m, representing distance in meters, and 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×m/s for the speed 10 meters per second. And we can define

new km:= 1000×m
to make km be a kilometer, and
new h:= 3600×s
to make h be an hour. So 1×m/s = 3.6×km/h evaluates to T. To assign a variable to a quantity with units attached, the variable's type must have compatible units attached. For example,

new speed: real×m/s:= 3.6×km/h
assigns speed to 1×m/s.

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

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

new quire:= 25×sheet
new ream:= 20×quire

Now you can define a variable using the new units.

new order: nat×sheet:= 3×ream
This assigns order to 1500×sheet.

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

A forward definition, for example

```
new abc
```

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

```
new f := 3. 
do new f.
new g = \cdots f \cdots. 
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 \( \do \)), \( g \) would be defined in terms of the earlier constant definition \( new f := 3. \)

Name Removal

Names defined with the keyword \( new \) can be undefined with the keyword \( old \). Ironically, by saying \( old x \), 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,

```
new s: *all:= nil.
new push do (x: all \rightarrow s:= s;x) od.
new pop do s:= s↓(0;..↔s–1) od.
new top = s↓(↔s–1).
new empty = s=nil.
old s
```

The names \( push \), \( pop \), \( top \), and \( empty \) 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 \( randNat \), \( randNatInit \), and \( randNatNext \). They might have been defined as:

```
new big:= 2↑31.
new rv: 0;..big:= 123456789.
new randNat = \{from: nat \rightarrow (to: nat \rightarrow floor (from + (to–from)×rv/big))\}.
new randNatInit do (seed: (0;..big) \rightarrow rv:= seed) od.
new randNatNext do rv:= mod (rv × 5↑13) big od.
old big. old rv
```

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

```
randNatInit 555555555.
randNatNext.
screen! numtext (randNat 0 10)
```

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

```
new t = i. old i. new i = j. old j. new j = t. 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,

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

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. If $A$ does not reassign $a$, and $B$ does not reassign $b$, then 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 $L_i$.

```
new findmax do (i: (0,..\#L) → (j: (1,..\#L+1) →
if j-i≥2 then findmax (i \ (div \ (i+j) 2)) || findmax ((div \ (i+j)) 2) \ j.
L := i → (L_i \ ∨ \ (L \ (div \ (i+j))) \ 1 \ L_{>\ j}) & 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 $\text{screen! "Hi there."}$ sends the text “Hi there.” to the screen. Output is buffered so it will be available when $\text{screen}$ is ready to receive it. Texts can be joined and sent together.

```
screen! "Answer = "; numtext x; 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 `keys`. Five characters of input are received from channel `keys` by saying

```keys? 5*char```

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

```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

```new digit:= "0", "1", "2", "3", "4", "5", "6", "7", "8", "9"```

and then input

```keys? *" "; (+", "; *, "; digit; *digit; (\(\."; digit; *digit), "); *, "; newline```

This grammar is predefined, and named `formnum`. The shortest 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:= 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

```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,

```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

```new c?!nat```

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

```new c?!nat. c! 7 || do c? 0,..100. x:= c 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 `⊤`, then `b` is executed; if its value is `⊥`, 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 `⊤`, then `b` is executed; if its value is `⊥`, then `c` is executed.
Named Programs

A named program has the syntax

```
newname do program od
```

The name of a named program must be new, just as if it were defined with the keyword `new`. But its scope is just within the `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×m` array `A` of integers (that is, `A: [n*[m*int]]`).

```
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 x; “occurs at”;
        numtext i;
        numtext j
      else j:= j+1. tryThisJ fi od fi od
```

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.
outerloop do if r≥d then new dd: nat := d.
  innerloop do r:= r-dd. dd:= dd+dd.
    if r<dd then outerloop else innerloop fi od fi od
```

The calls `outerloop` and `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.

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

$$
\text{«} x' > x \text{» do } x := x + 1 \text{ od}
$$

The specification on the left « $x'$ $>$ $x$ » 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,

$$
\text{«} x' = 0 \text{» do if } x \neq 0 \text{ then } x := x - 1. \text{ «} x' = 0 \text{» fi od}
$$

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

infiniteloop do new $a$ := “a”. screen! $a$. infiniteloop od

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

infiniteloop do new $a$ := “a”. do new $a$ := “a”. screen! $a$. infiniteloop 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.

name do program od
do new name do program od. name od
new name do program od. name. old name

Indexed Program

This example of an indexed program, or for-loop, computes the transitive closure of $A: [n^[n*bin]]$.

for i := 0;..$n$
do for i := 0;..$n$
  do for k := 0;..$n$
    do if $A i j \land A j k$ then $A := (i;k) \rightarrow \top \mid A$ fi od od od

The if then fi can be restated as

$A := (i;k) \rightarrow (A i k \lor (A i j \land A j k)) \mid A$

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.

new $n$ := 1000.
new prime: $[n*bin]$ := $[2^*\bot; (n-2)^*\top]$.
for i := 2;..ceil (sqrt $n$)
do if prime $i$ then for j := i;..ceil ($n/i$) do prime := (i$j) \rightarrow \bot \mid prime od fi od

A for-index is “by initial value”, so

for i := $x$; $x$ do $x := i + 1$ 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),

\[
\text{for } i := 0,..\#A \text{ do } A := i \rightarrow 0 \mid A \text{ od}
\]

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 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. Likewise,

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

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

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

cannot be applied to channel $d$. 
The following procedure \texttt{pps} has three channel parameters. On the first, \texttt{a}, it reads the coefficients of a rational power series; on the second, \texttt{b}, it reads the coefficients of another rational power series; on the last, \texttt{c}, it writes the coefficients of the product power series.

\begin{verbatim}
new pps do \langle a? rat \rightarrow \langle b? rat \rightarrow \langle c! rat \rightarrow \\
a? rat \parallel b? rat. c! a\times b. \\
new a0:= a \parallel new b0:= b \parallel new d?!rat. \\
pps a b d \parallel do a? rat \parallel b? rat. c! a0\times b+a\times b0. \\
loop do a? rat \parallel b? rat \parallel d? rat. \\
c! a0\times b+d+a\times b0. loop od od \rangle \rangle \rangle od
\end{verbatim}

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

\textbf{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 \texttt{abc}, write

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

(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 \texttt{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,

\begin{verbatim}
new abc_x:= 2
\end{verbatim}

defines \texttt{x} in dictionary \texttt{abc} to be the constant \texttt{2}. (It does not matter whether there are spaces before or after the underscore.) This constant can then be used as \texttt{abc_x}. To define new dictionary \texttt{def} within dictionary \texttt{abc} write

\begin{verbatim}
new abc_def
\end{verbatim}

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 \texttt{ProTem} within which there is a dictionary named \texttt{grammars} within which there is a text named \texttt{LL1}. Its name is \texttt{ProTem_grammars_LL1}. You can shorten this name with a new definition.

\begin{verbatim}
new LL1:= ProTem_grammars_LL1
\end{verbatim}

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 \texttt{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 \texttt{old}. For example,

\begin{verbatim}
old abc
\end{verbatim}

And, like any other simple name, its scope cannot be ended by \texttt{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 \texttt{abc} outside a local scope, and constant \texttt{x} in dictionary \texttt{abc} within the local scope, the definition of \texttt{x} within \texttt{abc} remains in effect past the end of the local scope because the definition of \texttt{abc} remains in effect. The name \texttt{abc_x} will no longer be defined when \texttt{abc} is no longer defined. The name \texttt{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 `do od` scope, but not after the second `do od` scope.

In the superscope where the predefined names are defined, there is also a dictionary named `predefined` with all the predefined names in it (except `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 `predefined_i` (unless you have also covered the predefined name `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 uncover the simple name `i` as the imaginary number by the constant definition

```
new i:= predefined_i
```

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

```
A. B
```

```
for x:= A do B od
```

```
A. B
```

```
for x:= A
do B od
```

```
A || B
```

```
A + B
```

```
A
+ B
```

```
if A then B else C fi
```

```
result x: A:= B do C od
```

```
if A then B
else C fi
```

```
result x: A:= B
do C od
```

```
if A
then B
else C fi
```

```
\langle x: A \rightarrow \langle y: B \rightarrow C \rangle \rangle
```

```
\langle x: A \rightarrow \langle y: B \rightarrow C \rangle \rangle
```

### 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:
esc-edit: enter or exit editor
esc-abort: abort program
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:

- only 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 “only 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 and passwords belong to dictionaries, not to people. Dictionary predefined has read-permit “everyone” and write-permit “only 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 (that does not require power) contains the state as it was at the start of the current session, and volatile memory (that requires power) 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, 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 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.

```
new color := “red”, “green”, “blue”.
new brush: color := “red”
```

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

```
new person := “name” → text | “age” → nat.
new p: person := “name” → “Josh” | “age” → 16
```

The fields of \( p \) can be selected in the usual way, for example

```
screen! p “name”
```
prints the text “Josh”. The value of \( p \) can be changed in the usual ways, such as

```
p:= “name” → “Amanda” | “age” → 2
```

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

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

and join new records onto its end.

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

The efficiency of pointers is obtained through the use of the predefined function \( \text{index} \). When applied to a list argument, it yields the deep domain of the list. For example,

```
\text{index} [10; [11; 12]; 13] = 0 , 1;(0, 1) , 2 = 0 , 1;0 , 1;1 , 2
```

The use of \( \text{index} \) 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.

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

We can use \( \text{first} \) in an arithmetic context, for example

```
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

```
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 \( \text{index} \). Here is a tree-structured example.

```
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:

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

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

```
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
\[ t := p \rightarrow s | t \]

We can express the information at the node indicated by \( p \) as
\[ t@p \quad \text{or} \quad t@(p; 1) \]

and we can replace the information at this node with the integer 6 using the assignment
\[ t := (p; 1) \rightarrow 6 | t \]

To move up in the tree, we just remove the final item of \( p \), and to make that easy, the predefined
\[ \text{new back} = \langle p: (*\text{nat}) \rightarrow p \downarrow(0;..\leftrightarrow p-1) \rangle \]

allows us to move \( p \) up to its parent by writing
\[ p := \text{back } p \]

The index function is also useful in for-loops. For example,
\[ \text{for } i := \text{index } L \text{ do } L := i \rightarrow L \quad \text{i + 1 | L od} \]

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,
\[ \text{new transform do } \langle \text{magnification: real } \rightarrow \langle \text{translation: real } \rightarrow \quad x := \text{magnification}\times x + \text{translation} \rangle \rangle \text{ od} \]

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.
\[ \text{new magnify do } \langle \text{magnification: real } \rightarrow \text{transform magnification 0} \rangle \text{ od} \]

We can now obtain a three-times magnification of \( x \) in either of these ways.
\[
\begin{align*}
magnify 3 \\
\text{transform 3 0}
\end{align*}
\]

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

Exception handling is provided by bunch union and by | or if. For example,
\[ \text{new divide} = \langle \text{dividend: com } \rightarrow \langle \text{divisor: com } \rightarrow \quad \text{if divisor = 0 then “zero divide” else dividend / divisor fi } \rangle \rangle \]

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
\[ \text{new weekday} = \langle d: (0;..7) \rightarrow 1 \leq d \leq 5 \rangle \]

Then in the expression
\[ (\text{weekday | all} \quad \text{“domain error”}) i \]

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.
\[ \text{inputchoice do if } ?c \text{ then } c? \text{ formnum. P} \]
\[ \quad \text{else if } ?d \text{ then } d? \text{ formnum. Q} \]
\[ \quad \text{else inputchoice fi fi od} \]
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 esc-names and esc-note are the Unix ls and man commands. ProTem's old is Unix's rm. The effect of Unix pipes is obtained by channel parameters. For example, suppose trim is a procedure to trim off leading and following blanks and tabs and newlines from text, and sort is a procedure to sort texts. (Please excuse the informal body since it's not the point of the example.)

new trim do \text{in? text $\rightarrow$ out! text $\rightarrow$ Repeatedly read from in, trim off leading and trailing space, output to out, until end is read.} \\
\text{The final end is output.}} od.

new sort do \text{in? text $\rightarrow$ out! text $\rightarrow$ Repeatedly read from in until end is read and output the sorted texts to out. The final end is output.}} od

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

new pipe?!text. trim keys pipe. sort pipe screen. old pipe

Even better:

new pipe?!text. trim keys pipe \parallel sort pipe screen. old pipe

If sort needs input before it is available from trim, sort waits.

The predefined procedure 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 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 pic is all picture values. It can be used to create a picture-valued variable.

new p: pic:= [x*[y*[0]]]

The name pic is defined as \([x*[y*(0,z)]]\) where \(x\) is the number of pixels in the horizontal direction, \(y\) is the number of pixels in the vertical direction, and \(z\) 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 \(p\) as \(p\,3\,4\).

Another predefined name is movie, defined as *pic. The operations on movies are just those of strings, such as join. 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.

There is a predefined program browse that opens a web browser, and predefined channels mailin and mailout for receiving and sending email. Any other “apps” become predefined names.

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

\[ \text{assert } x \leq y \]

abbreviates \[ \text{if } -(x \leq y) \text{ then screen! “assert failure”. stop fi} \]

string item assignment

\[ S \downarrow 3 := 5 \]

abbreviates \[ S := S \downarrow 3 \mapsto 5 \]

list item assignment

\[ L 3 := 5 \]

abbreviates \[ L := 3 \mapsto 5 \]

\[ L 3 4 := 5 \]

abbreviates \[ L := (3;4) \mapsto 5 \]

name grouping

\[ \text{new } x, y \text{: int} := 0 \]

abbreviates \[ \text{new } x \text{: int} := 0 \text{ || new y } \text{: int} := 0 \]

\[ \text{old } x, y \]

abbreviates \[ \text{old } x \text{|| old y} \]

\[ \langle a, b: \text{nat } \mapsto a + b \rangle \]

abbreviates \[ \langle a: \text{nat } \mapsto \langle b: \text{nat } \mapsto a + b \rangle \rangle \]

\[ x, y := 0 \]

abbreviates \[ x := 0 \text{ || y} := 0 \]

looping constructs

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

\[ \text{loop } n := n - 1 \text{ until } n = 0 \text{ pool abbreviates} \]

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

\[ \text{loop } n := n - 1. \text{ exit when } n = 0. \text{ m:= m+1 pool abbreviates} \]

\[ \text{loop } n := n - 1. \text{ if } -(n = 0) \text{ then m} := m + 1. \text{ loop fi od} \]

dictionary parameters and arguments

\[ \langle \text{ simplename } \_ \mapsto \text{ program } \rangle \]

procedure, parameter is dictionary

\[ \text{program dictionaryname} \]

procedure, dictionary argument

As a direct counterpart to the Unix cd command, we considered

\[ \text{go dictionaryname} \]

to allow names in that dictionary to be referred to without stating the dictionary. For example, if we have dictionary \( \text{abc} \), and within it names \( x \) and \( y \), we can refer to these names as \( \text{abc}_x \) and \( \text{abc}_y \). By saying

\[ \text{go abc} \]

we can then refer to them as just \( x \) and \( y \). But the interaction between \( \text{go} \) and scope is complex, so we left out \( \text{go} \). We can still shorten each reference individually. For example,

\[ \text{new } x = \text{abc}_x. \]

\[ \text{new } y = \text{abc}_y \]

We also considered the alias creation construct

\[ \text{new } \text{newname oldname} \]

It might be handy to shorten all names that are deep within several dictionaries. For example, if dictionary \( a \) contains dictionary \( b \) which contains dictionary \( c \) which contains dictionary \( d \), then

\[ \text{new } d \_a \_b \_c \_d \]

allows us to shorten all names within \( a_b_c_d \), for example, from \( a_b_c_d_x \) to \( d_x \). But aliases create confusion, and difficulties for verification, so we did not include alias creation in ProTem.

There is no direct counterpart to the import construct or frame construct in ProTem. 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

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

**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
```

ProTem does not evaluate the application of the negation operator \(-\) to its operand 3; it just prints
the operator and operand. Similarly

```
screen! numtext (1/0)   should print 1/0
screen! numtext ([0; 1] 2) should print [0; 1] 2
screen! numtext (\(r: \text{rat} \rightarrow 5\)) (1/0)) should print 5
screen! bintext (1/0 = 1/0) should print \(\top\)
screen! bintext ([0; 1] 2 = [0; 1] 2) should print \(\top\)
```

Due to the difficulty of implementation, it is permissible for an implementation to behave differently.

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 “Apology: this
implementation is too limited to accommodate your program.”. An “error” message tells a
programmer to correct the error; there is no other option. An “apology” 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 an “apology” 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

$$\text{nat int rat bin text } [n^\text{type}]$$

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 accommodate programs that previous implementations could not accommodate.

**Predefined Names**

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

- **variable** (evaluated; assignable)
- **constant** (evaluated; not assignable)
- **data** (unevaluated; evaluation upon use; not assignable)
- **program** (unexecuted; execution upon use)
- **channel**
- **unit**
- **dictionary**

Some definitions use $\S$ or $\exists$, which are defined in *a Practical Theory of Programming*.

**abs**: $\text{com} \rightarrow \text{real data}$ Absolute value. $\text{abs } x = \sqrt{r x + 2 + im x + 2}$.

**all** $\text{data}$ All ProTem items.

**arc**: $\text{com} \rightarrow \S(r: \text{real} \rightarrow 0 \leq r < 2 \pi) \text{ data}$ The angle or arc of a complex number.

**arccos**: $\S(r: \text{real} \rightarrow -1 \leq r \leq +1) \rightarrow \S(r: \text{real} \rightarrow 0 < r < \pi/2) \text{ data}$ A trigonometric function.

**arcsin**: $\S(r: \text{real} \rightarrow -1 \leq r \leq +1) \rightarrow \S(r: \text{real} \rightarrow 0 < r < \pi/2) \text{ data}$ A trigonometric function.

**arctan**: $\text{real} \rightarrow \S(r: \text{real} \rightarrow 0 < r < \pi/2) \text{ data}$ A trigonometric function.

**asm** $\text{program}$ 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.

**await** $\text{program}$ A program with one constant parameter of type $\text{real}\times s$. If the argument represents the present or a future 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 $\text{time}$ and $\text{wait}$ and $s$. 
back: *nat → *nat data  back (s; i) = s.
bin = T, ⊥ constant
bintext: bin → text constant bintext ⊤ = “T” and bintext ⊥ = “⊥”.
browse program A browser program with one text input parameter. If the input text is a URL, the
addressed page is displayed. Otherwise the text is used as a query to your choice of search
engine.
ceil: real → int data  r ≤ ceiling r < r+1
char data The characters.
charnat: char → nat data A one-to-one function with inverse natchar.
click: char constant
com data The complex numbers.
cos: real → \$(r; real → −1 ≤ r ≤ +1\}$ data A trigonometric function.
cosh: com → com data A hyperbolic function.
cursor: nat; nat data A data name whose value is the current cursor position.
delete: char constant
div: real → \$(r; real → r>0) → int data  div a d is the integer quotient when
a is divided by d.
(0 ≤ mod a d < d) ∧ (a = div a d \times d + mod a d)
doubleclick: char constant
e = 2.718281828459045 (approximately) constant The base of the natural logarithms.
encode: text → text data A not easily invertible function.
end: char constant The end-of-file character. It is greater than all letters, digits, punctuation
marks, space, tab, and newline.
eval: text → all data If the argument represents a ProTem data expression, the evaluation is that of
the represented data. It “unquotes” its argument. In eval “x”, the “x” refers to whatever x
refers to at the location where eval “x” occurs.
even: int → bin data A function that says whether its argument is even or odd.
exec program A program with one text parameter. If the input represents a ProTem program, the
execution is that of the represented program. It “unquotes” its argument. If applied to
“x:= x+1”, the “x” refers to whatever x refers to at the location where exec “x:= x+1”
occurs.
exp: com → com data e↑x.
false = ⊥ constant A binary value.
find: all → all → nat data If i is an item in string S, then find i S is the index of its first
occurrence; if not, then find i S = ⊥.
fit: int → text → text data If i≥0 then fit i t is a text of length i obtained from t by either chopping
off excess characters from the right end or by extending t with spaces on the right end. If
i≤0 then fit i t is a text of length –i obtained from t by either chopping off excess
characters from the left end or by extending t with spaces on the left end.
floor: real → int data floor r ≤ r < 1 + floor r
form: nat → nat → (nat+1) → real → text data Format a real number. form d e w r is a text
representing real r with the final digit rounded. d is the number of digits after the decimal
point; if d=0 the point is omitted. e is the number of digits in the exponent; if e>0 the
decimal point will be placed after the first significant digit; if e=0 the “\times10^e” is omitted
and the decimal point will be placed as necessary. w is the total width; if w is greater than
necessary, leading blanks are added; if w is less than sufficient, the text contains stars.
form 4 1 1 2 pi = “3.1416\times10^1 \pi”. form 2 0 6 (−pi) = “−3.14”.
form 0 0 3 5 = “5”. form 0 0 3 (−5) = “−5”. form 0 0 2 1 2 3 = “**”.
formnum: text data A text format for numbers. It is useful for reading a number from a text
channel. The number may be preceded by spaces.
g unit Representing mass in grams.
i: sqrt (-1) constant An imaginary number.

im: com real data The imaginary part of a complex number.

index data A function that applies to a list and gives its deep domain (a bunch of strings of indexes). It is a signal to the implementation that the strings in it will be used only as indexes to the list. It can therefore be implemented as a memory address (pointer).

int data The integers.

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

lb: \$(r: real \to r>0) \to real data\) The binary logarithm (base 2).

ln: \$(r: real \to r>0) \to real data\) The natural logarithm (base e).

log: \$(r: real \to r>0) \to real data\) The common logarithm (base 10).

m unit Representing distance in meters.

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

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

match: *all all nat data If pattern occurs within subject, then match pattern subject is the index of its first occurrence. If not, then match pattern subject = \null\. 

maxint: int constant The maximum representable integer (machine dependent).

maxnat: nat constant The maximum representable natural (machine dependent).

minint: int constant The minimum representable integer (machine dependent).

mod: real \to \$(r: real \to r>0) \to real data\) mod a d is the remainder when a is divided by d .

\(0 \leq \text{mod} \ a \ d < d\) \land (a = \text{div} \ a \ d \times d + \text{mod} \ a \ d

movie = *pic data

nand: (bin, real) \to (bin, real) \to (bin, real) data An alternative for \(\sqcap\).

nat data The natural numbers.

natchar: charnat char \to char data A one-to-one function with inverse charnat.

newline: char constant The return or newline character.

nil constant The empty string.

nor: (bin, real) \to (bin, real) \to (bin, real) data An alternative for \(\vee\).

null constant The empty bunch.

numtext: com \to text data A text representation of a number. See also \text{form}.

odd: int \to bin data

ok program A program whose execution does nothing and takes no time.

ord = real, char, bin, fall, *ord, [ord] data The ordered type, for which \(< > \leq \geq\) are defined.

pi = 3.141592653589793 (approximately) constant The ratio of a circle's circumference to its diameter.

pic = [x*y*(0..z)]\] data where \(x\) is the number of pixels in the horizontal dimension, \(y\) is the number in the vertical dimension, and \(z\) is the number of pixel values.

pre: char \to char constant The character predecessor function.

predefined dictionary A dictionary containing all predefined names except predefined.

printer?!text channel To the printer, it is an input channel; to all other programs, it is an output channel.

randNat: nat nat nat data A reasonably uniform function, dependent on a hidden variable, over the interval from (including) the first argument to (excluding) the second argument.

randNatInit program A program with one constant natural parameter. Its execution assigns a hidden variable to the natural value.

randNatNext program A program. Its execution assigns a hidden variable to the next value in a random sequence.

randReal: real real real data A reasonably uniform function, dependent on a hidden variable,
over the interval between the arguments.

`randRealInit` program A program with one constant real parameter. Its execution assigns a hidden variable to the real value.

`randRealNext` program A program. Its execution assigns a hidden variable to the next value in a random sequence.

`rat` data The rational numbers.

`re`: `com`→`real` data The real part of a complex number.

`real` data The real numbers.

`round`: `real`→`int` data $r-0.5 \leq \text{round } r < r+0.5$

`s unit` Representing time in seconds.

`screen?!text channel` To the screen, it is an input channel; to all other programs, it is an output channel.

`session: text` data A text data name whose value is all keystrokes on channel `keys` since the start of a session.

`sign`: `real`→$(-1, 0, 1)$ data

`sin`: `real`→$\{r: \text{real } \rightarrow -1 \leq r \leq +1\}$ data A trigonometric function.

`sinh`: `com`→`com` data A hyperbolic function.

`sort`: `*ord`→`*ord` data Sorts in nondecreasing order.

`sqrt`: `com`→`com` data The principle square root.

`stop` program A program whose execution does nothing and takes forever so that no computation can follow.

`subst`: `all`→`all`→`*all`→`*all` data `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` constant The character successor function.

`tab`: `char` constant

`tan`: $(\{r: \text{real } \rightarrow -\exists(i: \text{int } \rightarrow r = (2i + 1)\times \pi)\}) \rightarrow \text{real data}$ A trigonometric function.

`tanh`: `com`→`com` data A hyperbolic function.

`text = *char` data

`textnum: text`→`*com` data 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`→`(realxs)` data 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” = –68675727.5xs`.

`time?!realxs` channel 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`: `(realxs)`→`int`→`text` data 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 (–68675727.5xs) (–5) = “1947 September 16 at 14:24:32.5 UTC–5”`

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

`true = \top` constant A binary value.

`wait` program A program with one constant parameter of type `realxs`. If the argument is nonnegative, its execution does nothing and 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/s/s. ` 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 numparters := 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, numparters
  | (“x”, “y”) → nat )] ` box position on screen
  := [numboxes * ((“ahead left”, “ahead right”, “behind left”, “behind right”) → 0
  | “beside” → 0
  | “above” → numparters ` indicates no porter above
  | (“x”, “y”) → 0 )].

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

infiteloop
  do  time? real. ` the time of the start of each iteration of the infiteloop
    new p: index porter:= 0. ` p:= the porter that arrived at its current position first
    new t: realxs:= 10↑38x. ` 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
      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 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/s^2 := max accel. ` 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 ≤ max distance
then new desired speed = `according to porter pa
〈pa: (index porter, num porters) →
   if pa = num porters then speed limit
   else (√ ( porter pa “speed”↑2 + 2×max accel×d
           + (max accel×cushion)↑2 )
           – max accel×cushion ) ∧ speed limit fi ).
accel := ( (∧ desired speed (box b “above”)
           ∧ desired speed (port (box b “beside”) “above”))
           – porter p “speed”)
       × impatience)
       ∨ – max accel ∧ max accel.
if box b “above” = num porters = port (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”) → num porters \ box. draw b “grey”.
randNatNext.
b := box b if randNat 0 2 = 0 then “ahead left” else “ahead right” fi.
if box b “porter” < num porters then draw b “red”. stop fi. ` crash
porter := (p; “below”) → b \ porter. box := (b; “above”) → p \ box. draw b “blue”.
old b.
new speed := √ ( porter p “speed”↑2 + 2×max accel×m ) ∧ speed limit.
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+visual delay time).
infinitleap 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 numtext

new shl = \(n: \text{nat} \rightarrow (m: \text{nat} \rightarrow \text{` shift } n \text{ left } m \text{ places}; \ n \times 2^m)
\)
data r: \text{nat}:= n \text{ do for } i:= 0;..m \text{ do } r:= r \times 2 \od\).

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

new gcd = \(a: (\text{nat}+1) \rightarrow (b: (\text{nat}+1) \rightarrow \text{` greatest common divisor of } a \text{ and } b
\)
\)
if \(a=b\) then a else if \(a<b\) then gcd a (b–a) else gcd (a–b) b fi fi\).

new norm do (\text{num}:: (\text{nat}+1) \rightarrow (\text{denom}:: (\text{nat}+1) \rightarrow \text{` normalize num/denom
\)
\)
new g:= gcd \text{num} \text{denom}.
\)
um:= \text{num}/g. \text{denom}:= \text{denom}/g\) od.

new count: \text{nat}:= 0. (` number of examples

new qlen: \text{nat}:= 0. (` total length of quote representations

new rlen: \text{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 ` even \(\text{sh} \text{r } \text{string} \ (\text{length}–1)\) \text{ or } \text{even} \(\text{sh} \text{r } \text{string} \ (\text{quote}–1)\)` roll-normalized
\)
then if ` repeat-normalized
\)
result repeatnorm: \text{bin}:= T
\)
do new len: \text{nat} = \text{div} \ (\text{length}–\text{quote}) 2. ` the length of the possibly repeating part
\)
trythislen do if len>0 ` 1 \text{\leq} \text{len} \text{\leq} \ (\text{length}–\text{quote})/2
\)
then new extract = \(i: \text{nat} \rightarrow (l: \text{nat} \rightarrow \text{` index } i \text{ length } l
\)
\)
shl \text{string} i – \text{shl} \ (\text{shl} \text{string} \ (i+l)) \ l \]\).\)
\)
new ex:= extract \text{quote} \text{len}.
\)
if ` the negative part is a repetition (twice or more) of \text{ex
\)
result \text{r}: \text{bin}:= T
\)
do new i: \text{nat}:= \text{quote}+\text{len}. ` \text{i+len} \text{\leq} \text{length
\)
\)
iloop do new ey:= extract \text{i} \text{len}.
\)
if ey=ey then i:= i+\text{len}. ` \text{i\leq} \text{length
\)
if i<\text{length}
\)
then if i+\text{len} \text{\leq} \text{length
\)
loop
\)
else \text{r}:= \bot \text{ fi fi
\)
else \text{r}:= \bot \text{ fi odd \text{od}
\)
\)
do if ` the rightmost bit is 1 or it's to the left of quote or point
\)
odd \text{string} \lor \text{quote}=0 \lor \text{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 od 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($^{1/2}$). 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 simplename := data do program od
              \{ simplename 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 term afterterm
term factor afterfactor
factor # factor
– factor
~ factor
+ factor
? factor
☐ factor
◊ factor
¢ factor
$ factor
↔ factor
primary afterprimary
primary number
text
⊤
⊥
if data then data else data fi arguments
result simplename : data := data do program od arguments
{ data }
[ data ] arguments
( data ) arguments
〈 simplename : primary → data 〉 arguments
name arguments
arguments number arguments
text arguments
⊤ arguments
⊥ arguments
if data then data else data fi arguments
result simplename : data := data do program od arguments
{ data }
[ data ] arguments
( data ) arguments
〈 simplename : 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 term name.
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
  simplename do program od
  if data then program fi
  if data then program else program fi
  for simplename := data do program od
  do program od
  procedure

procedure
  \{ simplename : primary \rightarrow program \}
  \{ simplename :: primary \rightarrow program \}
  \{ simplename ! primary \rightarrow program \}
  \{ simplename ? primary \rightarrow program \}
  procedure argument
  name

data
  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 ; term
element ;.. term
element ;; term
element ' term
element + term
element – term
term
term
term × factor
term / factor
term ∧ factor
term ∨ factor
term ∆ factor
term ∨ factor
factor

factor
+ factor
− factor
ε factor
$ factor
↔ factor
# factor
~ factor
? factor
□ factor
♀ factor
* factor
primary * factor
primary → factor
primary ↑ factor
primary ↓ factor
primary

primary
primary argument
primary @ argument
primary %
argument
A name control procedure is responsible for classifying names.

**Acknowledgements**

Theo Norvell wrote an MSc thesis in 1988 titled “Expressions, Types, and Data Structures in ProTem”. Hugh Redelmeier acted as design consultant and critic in 1990. Brian Parkinson found a bug in the implementation in 1990. The design of ProTem has been improved since then, and the old implementation is now out-of-date. A new implementation is partially written.