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,

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

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

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

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

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

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

ProTem uses letters, digits, and a blank space. In addition, there are 12 keywords, plus 4 kinds of lexeme, and 63 other symbols; altogether they are:

```
if then else fi new old for do od result front unit
number text name comment
" " « » _ ` : :: := = + – × / ↑ ↓ → ↔ ∧ ∨ ø $ % ∈ ⊆ ∪ ∩ □ ∆ ∨ ⊲ ⊳
```

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

- Use `for " use `, ` for ” reuse "` for « use << for » use >>
- Use |= for ≤ for ≥ use >= for ‘ use ’
- Use 〈 use par for 〉 use rap
- Use ↑ use ^ for ↓ use \ for → use –> for ↔ use <>
- Use ∧ use / \ for ∨ use \/ for † use + for † use //
- Use ∈ use elt for ⊆ use sub for ∪ use cup
- Use ⊕ use [ ] for ∆ use nand for ∨ use nor
- Use < | for > |

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

```
0 275 27.5 0.21
```

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

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

```
"" "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 and symbol substitutes 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_Hehner  
  «2016-9-8»_«grad recruiting»_DCS

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

Presentation Grammar

A name is one of

- simplename: a simple name (plain or fancy)
- compoundname: more than one simplename joined with underscores

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

- newname: a simplename that is not in the front dictionary
- oldname: a simplename that is in the front dictionary
At each point in a program, an oldname is one of

- variablename: a name defined as a variable
- constantname: a name defined as a constant
- dataname: a name defined as data
- programname: a name defined as a program or procedure
- channelname: a name defined as a channel
- dictionaryname: a name defined as a dictionary

There are 57 ways of expressing data. Some examples, explanations, and pronunciations are shown.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>percentage, divide by 100</td>
</tr>
<tr>
<td>+</td>
<td>plus, identity</td>
</tr>
<tr>
<td>–</td>
<td>minus, negation, not</td>
</tr>
<tr>
<td>+ data</td>
<td>plus, addition</td>
</tr>
<tr>
<td>data – data</td>
<td>minus, subtraction</td>
</tr>
<tr>
<td>data × data</td>
<td>times, multiplication</td>
</tr>
<tr>
<td>data / data</td>
<td>by, division</td>
</tr>
<tr>
<td>data ↑ data</td>
<td>to the power, exponentiation</td>
</tr>
<tr>
<td>data ∧ data</td>
<td>minimum, conjunction, and</td>
</tr>
<tr>
<td>data ∨ data</td>
<td>maximum, disjunction, or</td>
</tr>
<tr>
<td>data ∆ data</td>
<td>negation of minimum, nand</td>
</tr>
<tr>
<td>data ∇ data</td>
<td>negation of maximum, nor</td>
</tr>
<tr>
<td>data = data</td>
<td>equals, equation</td>
</tr>
<tr>
<td>data ≠ data</td>
<td>differs from, discrepancy, exclusive or</td>
</tr>
<tr>
<td>data &lt; data</td>
<td>less than, strict implication</td>
</tr>
<tr>
<td>data &gt; data</td>
<td>greater than, strict reverse implication</td>
</tr>
<tr>
<td>data ≤ data</td>
<td>less than or equal to, implication</td>
</tr>
<tr>
<td>data ≥ data</td>
<td>greater than or equal to, reverse implication</td>
</tr>
<tr>
<td>data , data</td>
<td>bunch union</td>
</tr>
<tr>
<td>data ... data</td>
<td>bunch from(including) to(excluding)</td>
</tr>
<tr>
<td>data ‘ data</td>
<td>bunch intersection</td>
</tr>
<tr>
<td>data : data</td>
<td>bunch inclusion</td>
</tr>
<tr>
<td>∈</td>
<td>elements of a set</td>
</tr>
<tr>
<td>data ∈ data</td>
<td>subset</td>
</tr>
<tr>
<td>data ∪ data</td>
<td>set union</td>
</tr>
<tr>
<td>data ∩ data</td>
<td>set intersection</td>
</tr>
<tr>
<td>data ^ data</td>
<td>power</td>
</tr>
<tr>
<td>data $ data</td>
<td>set size</td>
</tr>
<tr>
<td>“data”</td>
<td>“abc”</td>
</tr>
<tr>
<td>data ; data</td>
<td>string catenation</td>
</tr>
<tr>
<td>data ;.. data</td>
<td>string from(including) to(excluding)</td>
</tr>
<tr>
<td>data ↓ data</td>
<td>string indexing</td>
</tr>
<tr>
<td>data &lt; data data &gt; data</td>
<td>string modification</td>
</tr>
<tr>
<td>↔</td>
<td>string length</td>
</tr>
<tr>
<td>data * data</td>
<td>definite repetition</td>
</tr>
<tr>
<td>* data</td>
<td>indefinite repetition</td>
</tr>
</tbody>
</table>
There are 29 ways of forming a program.

```
new newname : data := data
new newname := data
new newname = data
new newname do program od
new newname ? ! data
new newname front
new newname unit
new newname
old oldname
dictionaryname front
variablename := data
channelname ! data
channelname ? data
channelname ? ! channelname
newname do program od
programname
 ⟨ newname : data → program ⟩
 ⟨ newname : data → program ⟩
 ⟨ newname ! data → program ⟩
 ⟨ newname ? 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 newname := data do program od
do program od
```

create variable : type := initial value
create constant name and evaluate data
create data name but don't evaluate data
create program name but don't execute program
create channel with type
create dictionary and put it in front
create measuring unit
forward definition
remove or hide
put this dictionary in front
assign variable to value
to channel send output
from channel receive input of this type
input, correct, and echo
create program name and execute program
execute (call) named program
procedure, parameter is constant
procedure, parameter is variable
procedure, parameter is output channel
procedure, parameter is input channel
procedure, data argument
procedure, variable argument
procedure, channel argument
sequential composition
parallel composition
conditional program
indexed program, create local constant parentheses
Here is the precedence of the forms of program.

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

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

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

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

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

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

Only one alternative for “data” contains “program”, and there the most general form of program is intended.

**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 \( \pi \) (an approximation to the ratio of a circle's circumference to its diameter), \( e \) (an approximation to the base of the natural logarithms), and \( i \) (the imaginary unit, or square root of \(-1\) ). Predefined names can be redefined in a new scope. The postfix operator \% means division by 100; for examples, 99% and \( x\% \). There are 1-operand prefix operators + and –. There are 2-operand infix operators + – × / ↑ ↓. There are predefined function names such as abs, exp, log, ln, sin, cos, tan, ceil, floor, round, re, im, sqrt, div, and mod (see **Predefined Names**). Division of integers, such as \( 1/2 \), may produce a noninteger. Exponentiation is 2-operand infix ↑; for example, \( 1.2\times10^3 \) (one point two times ten to the power three). The operator \& is minimum (arms down, does not hold water). The operator ∨ is maximum (arms up, holds water). The operator ∆ is the negation
of minimum. The operator $\neg$ 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: `backspace`, `tab`, `newline`, `click`, `doubleclick`, and `end` (the end-of-file character). Predefined functions `suc` and `pre` give the successor and predecessor respectively.

**Binary Values**

There are two predefined binary constants: `true` and `false`. Negation is $\neg$, conjunction is $\land$, disjunction is $\lor$, nand is $\Delta$, nor is $\nabla$.

The infix 2-operand operators $=$ and $\neq$ apply to all data in ProTem with a binary result; the two operands may even be of different types. The order operators $<$, $\leq$, $\geq$ apply to real numbers (including rationals, integers, and naturals), to characters, to binary values, to strings of ordered items, and to lists of ordered items, with a binary result. In the binary order `false` is below `true`, so $\leq$ is implication. The 3-operand `if x then y else z fi` has binary operand $x$, but $y$ and $z$ are of arbitrary type.

**Bunches**

There are several predefined bunch names:

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

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

Bunch union is denoted by a comma:

$$A, B$$

$A$ union $B$

For example,

$$2, 3, 5, 7$$

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

$$x..y$$

$x$ to $y$

where $x$ and $y$ are integers or characters that satisfy $x \leq y$. 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
\[ A \triangleleft B \quad \text{is included in } B \]
is binary. The size of a bunch is $\varnothing$. For examples, $\varnothing(0, 1) = 2$ and $\varnothing \text{null} = 0$ and $\varnothing(a, b) = b-a$.

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 $\cup$, distribute over bunch union. For examples,
\begin{align*}
-(3, 5) &= -3, -5 \\
(2, 3)+(4, 5) &= 6, 7, 8
\end{align*}
This makes it easy to express the plural naturals ($\text{nat}+2$), the even naturals ($\text{nat}\times2$), the square naturals ($\text{nat}^2$), the natural powers of two ($2^\text{nat}$), 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 $\text{~}$. For example, \text{~}{0, 1} = 0, 1. The size of a set is $\$$. For examples, $\$\{0, 1\} = 2$ and $\$\{\text{null}\} = 0$. The element $\in$, subset $\subseteq$, union $\cup$, and intersection $\cap$ operators are as usual. The power operator $\triangleleft$ takes a bunch as operand and produces all sets that contain only elements of the bunch. For example, $\triangleleft(0, 1) = \{\text{null}\}, \{0\}, \{1\}, \{0, 1\}$.

**Strings**

There is a predefined string name:

\textit{nil} the empty string

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

String catenation is denoted by a semi-colon:

\[ S ; T \quad \text{S catenate } T, \text{S join } T \]
For example,
\[ 2; 3; 5; 7 \]
is a string of four integers. There is also the notation
\[ x;..y \quad x \text{ to } y \quad (\text{same pronunciation as } x;..y) \]
where $x$ and $y$ are integers or characters that satisfy $x \leq y$. Again, $x$ is included and $y$ is excluded. For examples, $0;..10$ is a string consisting of the first ten natural numbers, and $5;..5 = \text{nil}$.

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

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

If $S$ is a string and $n$ is an index of $S$ and $i$ is any item, then $S \downarrow n \triangleright i$ is a string like $S$ except that item $n$ is $i$. For example, $(3; 5; 9)\downarrow2 \triangleright 8 = 3; 5; 8$. 

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

“abc” = “a”; “b”; “c”

“He said ‘Hi’,” = “H”; “e”; “’”; “s”; “a”; “’”; “d”; “’”; “’”; “H”; “’”; “’”; “’”

“abcdefgihj” ↓ (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 catenation precedes bunch union on the precedence table, we have

(3, 4); (5, 6) = 3;5, 3;6, 4;5, 4;6

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

If S is a string and n is a natural number, then

\[ n * S \]

is a string, and

\[ * S \]

is a bunch of strings. For examples,

\[ 3*5 = 5;5;5 \]

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

\[ *5 = \text{nil}, 5, 5;5, 5;5;5, 5;5;5;5, \text{and so on} \]

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

\[ \text{null} * 5 = \text{null} \]

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

Using this semi-distributivity, we have

\[ *a = \text{nat} * a \]

Lists

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

\[ [0; 1; 2] \]

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

\[ # L \]

length of L

\[ \sim L \]

content of L

\[ L n \]

L at n, L at index n

\[ L @ p \]

L at p, L at pointer p

\[ L \uparrow M \]

L catenate M, L join M

\[ L M \]

L composed with M

\[ L \wr M \]

L otherwise M, the selective union of L and M

\[ i \rightarrow x \downarrow L \]

index i is item x and otherwise L

plus the comparisons L=M, L+M, L<M, L>M, L≤M, L≥M.

Here are some examples.

\[ #[0; 1; 2] = 3 \]

the number of items in a list

\[ \sim[0; 1; 2] = 0;1;2 \]

indexing starts at zero

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

\[ [0;..10] \uparrow [10;..20] = [0;..20] \]

\[ [10;..20] [3; 6; 5] = [13; 16; 15] \]

in general, \( (L M)n = L(M n) \)
If a list is indexed with a structure, the result has the same structure. 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 \( M n \).
\[
[10; 11] | [0;..10] = [10; 11; 2;..10]
1→21 | [10; 11; 12] = [10; 21; 12]
\]
The index can be a string, as in
\[
(0;1) \rightarrow 6 \mid [[0; 1; 2]; [3; 4; 5]] = [[0; 6; 2]; [3; 4; 5]]
\]
When a string or list is indexed by a structure, the result has that same structure. For example, let \( S = 10; 11; 12 \). Then
\[
S↓(0, \{1, [2; 1]; 0\}) = S↓0, \{S↓1, [S↓2; S↓1]; S↓0\} = 10, \{11, [12; 11]; 10\}
\]
For another example, let \( L = [10; 11; 12] \). Then
\[
L (0, \{1, [2; 1]; 0\}) = L 0, \{L 1, [L 2; L 1]; L 0\} = 10, \{11, [12; 11]; 10\}
\]
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.

**Functions**

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

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

The \( \Box \) operator gives the domain of a function. For example, \( \Box \langle n: nat \rightarrow n+1 \rangle = nat \).

The notation for applying a function to an argument is the same as that for indexing a list: juxtaposition. Also, composition and selective union can have function operands, and even a mixture of list and function operands.
When the body of a function does not use its parameter, there is a syntax that omits the angle brackets 〈 〉 and unused name. For example,

\[ 2 \rightarrow 3 \]

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

Allowing the body of a function to be a bunch generalizes the function to a relation. For example, \( \text{nat} \rightarrow \text{bin} \) 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 \( \text{bin} \); it is all functions with domain at least \( \text{nat} \) and range at most \( \text{bin} \). As an example of the latter view, we have

\[ \langle n: \text{nat} \rightarrow \text{mod n 2} = 0 \rangle : \text{nat} \rightarrow \text{bin} \]

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 newname : data := data do program od
```

First, a local variable is defined with a type and initial value; its scope is from \( \text{do} \) to \( \text{od} \). 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 local scope; their values may be used, but assigning them is not permitted. Input and output are not permitted.

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

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

Programs

Some program constructs are concerned with dictionaries: adding a name to a dictionary (\texttt{new}), deleting a name from a dictionary (\texttt{old}), putting a dictionary in front (\texttt{front}). 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 add or remove names from a dictionary, including those that put a dictionary in front, are executed in their turn, just like variable assignments and input and output.

Dictionaries

There is a dictionary named \texttt{predefined} that contains all predefined names. In addition, each new user is given a dictionary, which is their own personal working space, within which they can make any new definitions they want. My personal dictionary is named \texttt{Hehner}.

Each name in a dictionary is defined to be one of the following: a variable name, a constant name, a
data name, a program name, a channel name, or a dictionary name. When a name is defined to be a dictionary, this dictionary also contains names, some of which can be defined as dictionaries, and so on. Therefore there is a tree of dictionaries. Whether this tree has a root, and if so what its name is, are of no consequence.

Suppose there is a text named ProTem within a dictionary named grammars within a dictionary named Hehner within a dictionary named cs within a dictionary named utoronto within a dictionary named ca. Its full compound name is ProTem_grammars_Hehner_cs_utoronto_ca.

Dictionaries have a lookup order: there is a front dictionary, there is a dictionary behind that, and so on. When you first use ProTem, your personal dictionary is in front, with predefined behind it, and other dictionaries behind that. You can create a new dictionary abc by saying

```
new abc front
```

When you create a new dictionary, its definition is put into the dictionary that is currently in front, and then the newly created dictionary is put in front. Your personal dictionary, and any dictionary within it, can be put in front. For example, if grammars is an already existing dictionary within Hehner, I can put it in front by saying

```
grammars front
```

By putting a particular dictionary in front, we can shorten the names we use. If grammars is in front, the text referred to by the lengthy compound name in the previous paragraph can be referred to simply as ProTem. Whenever a new scope is entered (see Scope), a new nameless dictionary is created and put in front. Whenever that scope is exited, its dictionary is deleted.

Simple names are defined in these ways: by the keyword new, as a named program, as a parameter just after \(\langle\), as a for-index, or as a result variable. Whenever a name is defined, its definition is written in the front dictionary. A name being defined must not already be defined in the front dictionary. A name defined by new in the front dictionary can be removed from the front dictionary with the keyword old.

Whenever a simple name is used, it is looked up in the front dictionary; if it is not there, it is looked up in the dictionary just behind the front dictionary; and so on, in order. The first definition found for the name is the one used.

Whenever a compound name is used, it is looked up as follows. The last simple name in the compound name is looked up as described in the previous paragraph. Its definition must be as a dictionary. The simple name before the last one in the compound name is looked up in this one dictionary only. And so on for preceding names in a compound name.

The name s is in dictionary predefined. If the name s is not redefined, then the predefined s can be referred to as just s. If the name s is redefined, this new definition covers, or hides, the predefined s. If the name s is redefined but the name predefined is not redefined, then the predefined s can still be used by the longer compound name s_predefined. If both s and predefined are redefined, we need an even longer compound name.

Any name x in a dictionary D may be covered, or hidden, by another definition of the same name x in another dictionary E in front of the first dictionary D. The first x can still be referred to as x_D if D has not been redefined. The first definition of x can be uncovered by removal of the second definition, or by moving dictionary D to the front.
Variable Definition

Here is an example variable definition.

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

This defines \( x \) to be a variable assignable to any element in \( \text{nat} \), 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 the colon is called the “type” of the variable. The type can be anything except the empty bunch. The type and initial value can depend on previously defined names, including variables. For example,

```
new y: 0,..2x := 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 \( x \). 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, \( \text{text} \) is a predefined bunch equal to \( *\text{char} \), so \( t \) can be assigned to any text, and is initially assigned to the empty text. In the last example, \( u \) is defined as a variable that can be assigned to any text of length less than 20, and is initially assigned to the text “abc”.

Assignment

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

```
x:= x+1
s:= 3 → 5 | s
```

The data on the right of \( := \) must be an element in the type 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.

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 true. In the constant definition of \( xplus1 \) earlier, \( x+1 \)
is evaluated once, at definition time. By contrast, in the data definition of \( x+2 \), \( x+2 \) is not evaluated at definition time; it is evaluated every time \( x+2 \) is used.

A data definition can depend indirectly on a variable. For example,
\[
\texttt{new twoxplus4} = 2 \times \texttt{xplus2}
\]
makes \( \texttt{twoxplus4} \) depend indirectly on the value of variable \( x \).

\textbf{Data Recursion}

In a variable definition, the type and initial value cannot depend on the variable being defined. For example,
\[
\texttt{new no: 0..2no := no} \quad \text{`illegal}
\]
is not allowed due to the two occurrences of \( \texttt{no} \) to the right of the colon. Likewise a constant definition cannot be recursive.

Data definition does allow recursion. The next two examples define \( \texttt{fact} \) and \( \texttt{div} \) to be the factorial function and integer divisor function for natural numbers.
\[
\texttt{new fact} = 0 \rightarrow 1 \mid \langle n: \texttt{nat+1} \rightarrow n \times \texttt{fact}(n-1) \rangle
\]
\[
\texttt{new div} = \langle a: \texttt{nat} \rightarrow \langle d: \texttt{nat+1} \rightarrow \\
\quad \text{if } a < d \text{ then } 0 \text{ else if even } a \text{ then } 2 \times \texttt{div}(a/2) \text{ d else } 1 + \texttt{div}(a-d) \text{ d fi fi} \rangle
\]

Here is a bunch of texts (a grammar). This bunch includes the text \( \text{“a+b+a–a”} \), and many more.
\[
\texttt{new exp = “a”, “b”, exp; “+”; exp, “-”; exp}
\]
This recursive definition is equivalent to the nonrecursive definition
\[
\texttt{new exp = (“a”, “b”, *((“(+”, “-”); (“a”, “b”)))}
\]

Here is a function that eats arguments until it is fed argument \( 0 \).
\[
\texttt{new eat} = \langle a: \texttt{nat} \rightarrow \text{if } a=0 \text{ then } 0 \text{ else eat fi} \rangle
\]
So \( \texttt{eat 5 2 0 = 0} \) and \( \texttt{eat 4 7 3 8 0 = 0} \).

The next example is a pure, baseless recursion.
\[
\texttt{new rec = rec}
\]
Whenever \( \texttt{rec} \) is used, the computation will be nonterminating.

A final example defines all binary trees with integer nodes.
\[
\texttt{new tree} = [\texttt{nil}, [\texttt{tree}; \texttt{int}; \texttt{tree}]]
\]

\textbf{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
\[
\texttt{new five:= 5} \\
\texttt{new five = 5}
\]
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.
\[
\texttt{new csix:= 5+1} \\
\texttt{new dsix = 5+1}
\]
If the definition is never used, \texttt{dsix} is more efficient. If the definition is used once, they are equally efficient. If the definition is used two or more times, \texttt{csix} is more efficient. Here is a more interesting example.

\begin{verbatim}
new cdouble=YES := (n: (0..10) \rightarrow 2\times n)
new ddouble = (n: (0..10) \rightarrow 2\times n)
\end{verbatim}

The constant definition \texttt{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 \texttt{cdouble} is used by applying it to an argument, that argument indexes the list. The data definition \texttt{ddouble} does not evaluate the function. Each time \texttt{ddouble} is used by applying it to an argument, the body of the function is evaluated. Which one is more efficient depends on the size of the domain, the complexity of the result, and the number of times the definition is used.

**Program Definition**

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

\begin{verbatim}
new switchends do s:= 0 \rightarrow s 9 | 9 \rightarrow s 0 | s od
\end{verbatim}

Execution of this definition creates the program name \texttt{switchends}, but does not execute program \texttt{switchends}. After execution of this definition, the name \texttt{switchends} can be used to cause execution of the program it names. Program definitions can be recursive.

The names used in a program definition, in the previous example \texttt{s}, are those visible at the time the definition is executed, that is, at the time this definition adds the name \texttt{switchends} to the dictionary. At the time \texttt{switchends} is called, causing execution of the assignment of \texttt{s}, variable \texttt{s} may not be visible, but it is assigned nonetheless.

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

**Measuring Unit Definition**

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

\begin{verbatim}
new km:= 1000\times m
\end{verbatim}

to make \texttt{km} be a kilometer, and

\begin{verbatim}
new h:= 3600\times s
\end{verbatim}

to make \texttt{h} be an hour. So \(1 \times \texttt{m/s} = 3.6 \times \texttt{km/h}\) evaluates to \texttt{true}. To assign a variable to a quantity with units attached, the variable's type must have compatible units attached. For example,

\begin{verbatim}
new speed: real\times \texttt{m/s} := 3.6 \times \texttt{km/h}
\end{verbatim}

assigns \texttt{speed} to \(1 \times \texttt{m/s}\). For another example,

\begin{verbatim}
new sheet unit. new quire:= 25\times \texttt{sheet}. new ream:= 20\times \texttt{quire}.
new order: nat\times \texttt{sheet} := 3\times \texttt{ream}
\end{verbatim}

assigns \texttt{order} to \(1500\times \texttt{sheet}\). When the value \(5 \times \texttt{m/s}\) is converted to text by \texttt{numtext}, the result is “5 \texttt{m/s}” without the \times sign and without evaluating the unknown real value \texttt{m/s}.
Forward Definition

A forward definition, for example

```protem
new abc
```

is a notice that a definition will follow later. It is used, for example, when definitions are mutually recursive. (See Scope.)

Name Removal

Names added to the front dictionary with the keyword `new` can be removed from the front dictionary 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 removed from a dictionary, its definition will remain as long as there is an indirect way to refer to it. For example,

```protem
new s: [*all] := [nil].
new push do 〈x: all → 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 from the dictionary, leaving the other names dependent upon an anonymous variable.

The predefined names include `randomNat`, `randomNatInit`, and `randomNatNext`. They might have been defined (by an administrator whose personal dictionary includes `predefined`) as:

```protem
new big:= 2↑31.
new rv: 0,..big := 123456789.
new randomNat = 〈from: nat → (to: nat → floor (from + (to–from)×rv/big))〉.
new randomNatInit do 〈seed: (0,..big) → rv:= seed〉 od.
new randomNatNext do rv:= mod (rv × 5↑13) big od.
old big. old rv.
```

Constant `big` and variable `rv` are now hidden; their names are removed from the dictionary, but `randomNat`, `randomNatInit`, and `randomNatNext` still use them. We can use these definitions in the following way:

```protem
randomNatInit 5555555555.
r
randomNatNext.
screen! numtext (randomNat 0 10).
```

We can get rid of a dictionary name `d` defined in the front dictionary by saying

```protem
old d
```

Removing a dictionary name by `old` also removes all names in that dictionary. The dictionary remains in existence, anonymously, as long as something refers to it or to its contents.

Sequential Composition

Sequential composition is denoted by a period. It is an infix connective. In other words, the period comes between and joins two programs. Unlike the period in English, the period in ProTem does not terminate a program that is not sequentially followed by another program.
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,

\[
\begin{align*}
\text{new } &a: \text{nat} := 1. \\
\text{new } &b: \text{nat} := 2. \\
\text{new } &c = a+b. \\
a := &4 \parallel b := 8
\end{align*}
\]

In the 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. Just after the assignment \( a := 4 \), variable \( a \) has value 4, constant \( b \) has value 2, and data \( c \) has value 6. Just after the assignment \( b := 8 \), constant \( a \) has value 1, variable \( b \) has value 8, and data \( c \) has value 9. 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 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 \( L \ i \).

\[
\begin{align*}
\text{new } &\text{findmax} \ do \ (i: (0,..\#L) \rightarrow (j: (1,..\#L+1) \rightarrow \\
\quad &\text{if } j-i \geq 2 \text{ then } \text{findmax} (i \ (\text{div} (i+j) 2) \parallel \text{findmax} (\text{div} (i+j) 2) \ j). \\
\quad &L := i \rightarrow (L \ i \lor (L \ (\text{div} (i+j) 2) \mid L \ fi)) \ od)
\end{align*}
\]

After execution of \( \text{findmax } 0 \ (\#L) \), the maximum value in the original 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

\[
\begin{align*}
\text{screen}! \ &\text{“Hi there.”}
\end{align*}
\]

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

\[
\begin{align*}
\text{screen}! \ &\text{“Answer = ”; numtext } x; \ \text{newline}
\end{align*}
\]

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.

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

\[
\begin{align*}
\text{keys}? \ &5*\text{char}
\end{align*}
\]

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

\[
\begin{align*}
\text{keys}? \ &\text{text; newline}
\end{align*}
\]
reads text up to and including a newline character. To receive spaces followed by a text that can be interpreted as a signed number, define

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

and then input

\[
\text{keys} \ ? \, \* \, \text{digit} ; \, (\text{\text{\text{\text{"."}}} \, \text{digit} ; \, \* \, \text{digit}) \, , \, \text{\text{\text{\text{""}}}}) \, ; \, (\text{\text{\text{\text{"%}}} \, \text{""})}
\]

This grammar is predefined, and named formnum.

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

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

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

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

There is a second form of input that reads from a text channel and simultaneously writes on a text channel. For example,

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

reads text from channel keys, corrected according to backspace characters, up to and including the next newline character, and echoes the input on the screen character by character and correction by correction. The newline character is consumed and echoed, but not included in the value of keys.

If \(c\) is the name of an input channel, then the input test

\[
? \ c
\]

is a binary expression saying whether there is currently any unread input on channel \(c\).

Channel Definition

The definition

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

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

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

assigns \(x\) to \(7\). 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 programs \(\text{if then fi}\) and \(\text{if then else fi}\) are as usual. An “assert” program is obtained according to the following example.

\[
\text{if} \ x \gg y \ \text{then screen}! \text{“appropriate error message”}. \ \text{stop fi}
\]

Named Programs

A named program has the syntax

\[
\text{newname do program od}
\]

The name must be new within the front dictionary. The name is attached to the program (like a program definition), and the program is executed (unlike a program definition). The program name is known only within the program to which it is attached; after that, it is again new and can be
reused. One purpose of this naming is to make loops. Here is a two-dimensional search for $x$ in an $n \times m$ array $A$ of integers (that is, $A : [n[^*m[^*int]])$).

```plaintext
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.

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

```plaintext
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.

```plaintext
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 := 2xnxy + y ↑ 2
else n := n/2 – 1. Fib. n := x. x := 2xxy + y ↑ 2. y := n ↑ 2 + y ↑ 2 + x fi fi od
```

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

```plaintext
« x' » x do x := x + 1 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,
« \( x' = 0 \) » \textbf{do if} \( x \neq 0 \) \textbf{then} \( x := x - 1 \). « \( x' = 0 \) » \textbf{fi od}

In the \textit{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.

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

\begin{verbatim}
new \textit{name} do \textit{program} od.  \textit{name} .  old \textit{name}
\end{verbatim}

\begin{verbatim}
do new \textit{name} do \textit{program} od.  \textit{name} od
\end{verbatim}

\begin{verbatim}
\textit{name} do \textit{program} od
\end{verbatim}

Indexed Program

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

\begin{verbatim}
for \( j := 0;..n \) do for \( i := 0;..n \) do for \( k := 0;..n \) do
   \textit{A} := (i;k) \rightarrow (A i k ∨ (A i j ∧ A j k)) | A od od od
\end{verbatim}

The assignment can be restated as

\begin{verbatim}
if \( A i j ∧ A j k \) then \( A := (i;k) \rightarrow true \) \textbf{|} \textit{A fi}
\end{verbatim}

if you prefer. The name being defined by \textit{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 \textit{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.

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

A \textit{for} index is “by initial value”, so

\begin{verbatim}
for \( i := x; x \textbf{do} x := i+1 \textbf{ od}
\end{verbatim}

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 \( \ldots \) rather than \( ;.. \) as earlier),

\begin{verbatim}
for \( i := 0;..\#A \textbf{ do } A := i \rightarrow 0 \textbf{|} A \textbf{ od}
\end{verbatim}

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.)

Procedures

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

\begin{verbatim}
\langle y: \textit{real} \rightarrow x := xy \rangle
\end{verbatim}

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. For example,
〈y: real → x:= x×y〉 3
which is the same as
x:= x×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
〈i: int → x:= i. y:= i) (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).
〈x: int → x:= 3)〉
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
〈x: int → x:= 3. y:= 4)〉
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.
〈c! text → c!”abc”)〉
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,
〈c? text → c?. screen! c)〉
can be applied to any input channel that delivers text. But
〈c! text → c!”abc”. d! “def”)〉
cannot be applied to channel d.

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

Format

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

A. B
or
A. or
B
for x:= A do B od
for x:= A do B od
Scope

A 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. The scope of a name is the part of a program in which the name is defined. Scopes are limited by `do od`, `then fi`, `then else`, `else fi`, and `〈 〉` brackets. Each of these five pairs is a scope opener and a scope closer. A scope opener creates a new unnamed empty dictionary, and puts it at the front, making it the dictionary into which newly defined names are entered. This dictionary is deleted at the corresponding scope closer. With the exception of forward definitions, names must be defined before they can be used.

A name defined by the keyword `new` must be new (not defined in the front dictionary), and simple (not compound). Its scope extends from its definition, through all following sequentially composed programs, to the scope closer for its scope. But it may be covered by a definition in a new front dictionary, due to either a more local scope or the use of `front`. For example, letting $A, B, C, D, \text{ and } E$ stand for arbitrary program forms (but not `new` or `old` or `front`), in

$$A. \text{new } x : \text{int} := 0. \quad B. \quad \text{do } C. \quad \text{new } x : \text{bin} := \text{true}. \quad D. \quad \text{od}. \quad E.$$

the definition of $x$ as an integer variable is not yet in effect in $A$, but it is in effect in $B, C, \text{ and } E$. The definition that makes $x$ a binary variable is in effect in $D$. None of $A, B, C, D, \text{ or } E$ can contain a redefinition of $x$ unless it is within further `do od`, `then fi`, `then else`, `else fi`, or `〈 〉` brackets.

A name defined by `new` in the front dictionary can be removed from the front dictionary with the keyword `old`, ending its scope early. So in

$$\text{new } x := 0. \quad A. \quad \text{old } x. \quad B$$

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 previous unclosed scope opener. After `old $x$`, the name $x$ is again new and available for definition. However,

$$\text{new } x := 0. \quad \text{do old } x. \quad A \quad \text{od}$$

is not allowed; a scope cannot be ended by `old` within a subscope.

Suppose a name is defined within a loop. For example, the name $a$ in

$$\text{infiniteloop do new } a := \text{“a”}. \quad \text{screen! } a. \quad \text{infiniteloop od}$$

Executing this loop prints an infinite sequence of the letter “a”. Replacing the call with the called program, it is equivalent to
\texttt{infiniteloop do new \texttt{a}:= "a". screen! a. \\
do new \texttt{a}:= "a". screen! a. infiniteloop od od}

In a general recursion, each call opens a new dictionary, 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 dictionary and its definitions cannot be used again, so the new empty dictionary replaces the old one.

If a name is defined by \texttt{new} outside all scope limiters, its scope ends only with \texttt{old}. Its scope does not end with the end of a computing session, not even by switching off the power. Variables defined outside all scope limiters serve as “files”. A predefined name cannot have its scope ended by \texttt{old}, but it can be hidden by a programmer's redefinition of the same name.

Since \{ opens a new scope, the parameter can be any simple name, even one that has already been defined in the enclosing scope. The corresponding \} closes its scope. A \texttt{for} index begins its scope after the corresponding \texttt{do} and ends its scope at the corresponding \texttt{od}. Consequently, the \texttt{for} index can be any simple name, even one that has already been defined in the scope that encloses the \texttt{for}-loop. Likewise a \texttt{result} variable begins its scope after the corresponding \texttt{do} and ends its scope at the corresponding \texttt{od}. Consequently, the \texttt{result} variable can be any simple name, even one that has already been defined in the scope that encloses the programmed data.

The name defining a named program must be \texttt{new}, just as if it were defined with the keyword \texttt{new}. But its scope is just within the \texttt{do od} pair that it names. After that, it is again new.

In a variable definition, constant definition, channel definition, \texttt{for} index definition, function parameter definition, procedure parameter definition, and \texttt{result} variable definition, the name being defined cannot be used in the type or initial value; its scope begins after the type and initial value.

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, in

\begin{verbatim}
\texttt{new \texttt{f}:= 3. do new \texttt{f}. new \texttt{g} = \ldots f \ldots g \ldots. new \texttt{f} = \ldots f \ldots g \ldots. \texttt{B od}}
\end{verbatim}

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

When the dictionary lookup order is changed by the use of \texttt{front}, the reordering lasts until the close of the scope in which it occurred, or until reordered again. The reordering of dictionaries obeys the scope rules. In a program of the form

\begin{verbatim}
A. do \texttt{B od}. C
\end{verbatim}

all names in all dictionaries, and their lookup order, are the same at the start of \texttt{C} as they were at the end of \texttt{A}, regardless of any local changes within \texttt{B}.

To execute a program stored on someone else's computer, just invoke that remote program using its full address (\texttt{programname_computername}). 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.
**Miscellaneous**

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

```
"""↓(0;0;(0;..32);31;31;(1;..31))"""↓(0;0;(0;..32);31;31;(1;..31))
```

The ProTem equivalent of enumerated type is shown here.

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

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

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

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

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

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

and catenate new records onto its end.

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

The efficiency of pointers is obtained through the use of the predefined name `index`.

```protem
new index := text→*nat
```

When applied to a text argument, it yields the result `*nat`. The use of `index` is a signal to the implementation that the natural numbers will be used only as indexes into the structure whose name is given by the text argument (and the implementation will check that this is so). For example, we can define a linked list `G` as follows.

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

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

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

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

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

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

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

```protem
new tree = [nil], [tree; all; tree].
new t: tree := [nil].
new p: (index “t”) := nil
```
To move $p$ down to the left in the tree we reassign it this way:

$$p := p; 0$$

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

$$t := p \rightarrow s \mid t$$

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

$$t@p 1 \quad \text{or} \quad t@(p; 1)$$

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

$$t := (p;1) \rightarrow 6 \mid t$$

To move up in the tree, we just remove the final item of $p$, and to make that easy, the predefined

$$\text{new back} = \langle p: (*\text{nat}) \rightarrow p↓(0;\leftrightarrow p–1) \rangle$$

allows us to move $p$ up to its parent by writing

$$p := \text{back} p$$

The procedure of some other programming languages is a combination of naming and parameterization. For example,

$$\text{new transform do } \langle \text{magnification: real } \rightarrow \langle \text{translation: real } \rightarrow \text{x := magnification} \times x + \text{translation} \rangle \rangle \text{ od}$$

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.

$$\text{magnify 3}
\text{transform 3 0}$$

In some other programming languages, the “function” is a combination of naming, parameterizing, and programmed data. For example,

$$\text{new fact = } \langle n: \text{nat } \rightarrow \text{result } f: \text{nat } := 1 \text{ do } i := 0;..n \text{ do } f := f \times (i+1) \text{ od } \text{ od} \rangle$$

Exception handling is provided by bunch union or by the $\mid$ operator. For example,

$$\text{new divide = } \langle \text{dividend: com } \rightarrow \langle \text{divisor: com } \rightarrow
\text{ if divisor = 0 then “zero divide” else dividend / divisor fi } \rangle \rangle$$

We can state the type of result returned by this function as

$$\text{com, “zero divide”}$$

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

$$\text{new weekday = } \langle d: (0,..7) \rightarrow 1\leq d\leq5 \rangle$$

Then in the expression

$$(\text{weekday } \mid \text{all} \rightarrow \text{“domain error”}) \ i$$

if $i$ fails to be an integer in the range 0,..7, the left side “catches” the exception and “throws” it to the right side, where it is “handled”.

The effect of an input choice connective can be obtained as follows.
Unix directories are dictionaries. Unix files are variables. The Unix cd command is approximated by `front`. The Unix pwd command is the predefined names `frontmost` and `dictionaries`. The Unix ls command is the predefined name `dictionary`. Unix rm is `old`. 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 ⟨in? text → ⟨out! text → repeatedly read from in, trim off leading and trailing space, output to out, until end is read.
The final end is output ⟩⟩ od.
new sort do ⟨in? text → ⟨out! text → 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 || sort pipe screen. old pipe
```

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

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

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

They are transitive through “use” and “call” without requiring the implementation to do a transitive closure (it just checks the comments at the head of the needed data names and program names).

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.

**Object Orientation**

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.
Graphics

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

```prolog
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 catenation. To help in the creation of movies, one of the pixel values should be “transparent”, and one of the operations on pictures should be overlaying one picture on another.

Editing

The command control-e (hold down the control key and type an e) invokes an editor for creating, modifying, or deleting any definition (variable name, constant name, data name, program name, channel name, or dictionary name). In the editor, control-e exits the editor, throws away old definitions that have been modified or deleted, along with all definitions that depend on them, and compiles and saves the new definitions.

Security

Any dictionary may contain a constant definition of the name `password`, such as

```prolog
new password:= encode "Smith" ` my mother's maiden name
```

where `encode` is a not-easily-invertible function from texts to texts. If a dictionary contains the constant `password`, the text will be requested when an attempt is made to use the dictionary or to refer to its contents. Passwords belong to dictionaries, not to people.

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. When control-q is typed, a session ends and a new one begins. 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. When the computer is turned off, a session ends.

At the start of a session, the dictionary order is the same as it was at the end of the previous session, but all passwords are required for dictionaries that include a `password` definition. A password will not be requested twice within the same session for the same dictionary.

Sessions do not define the lifetime of definitions (variables, constants, data, programs, channels, dictionaries). 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 nonlocal variables whose values are stored in volatile memory (that requires power), and whose values outlast a session, to be saved in nonvolatile memory.
Error Recovery

It is essential to be able to abort the execution of a program, especially if you suspect that its execution will take forever. The undo command (control-u) not only aborts execution, but also returns to the state (except for input and output) prior to the start of execution of the aborted program. The undo command can even be issued after the completion of execution of a program, before the start of the next one, acting as the magical inverse of the previous program.

On many computers, undo can be implemented just by doing nothing; nonvolatile memory contains the state as it was before the start of the previous program, and volatile memory contains the current state, which is stored in nonvolatile memory at the start of execution of the next program. (When the execution of a program runs over five minutes, or causes a massive state change, the current state may be saved temporarily in nonvolatile memory, to become permanent when the possibility of undoing it has passed.)

A second level of error recovery, control-s, undoes a session. Implementing it requires capturing the state at the start of a session. Although this is expensive, it is hoped that it can serve also as system backup, performed automatically and incrementally with a frequency that matches file use.

The final kind of error recovery works in conjunction with session undo. It requires ProTem to keep a text file named session consisting of all keystrokes since the start of the 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, perhaps using the text editor, and then executes the result.

    exec copy

This gives us perfectly flexible error recovery for the modest cost of a keystroke file.

Command Summary

There are four “commands” in ProTem that are not presented in the grammar. They cannot be part of a stored program. They can be used only by a human at a keyboard. They are:

    control-e  enter or exit editor
    control-q  quit session and start a new session
    control-u  undo program
    control-s  undo session

Intentionally Omitted Features

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

    assertion
    assert x ≤ y  abbreviates if x > y then screen! “assert failure”. stop fi
    list item assignment
    A 3:= 5  abbreviates A := 3→5 | A
    A 3 4:= 5  abbreviates A := (3;4)→5 | A
Implementation Philosophy

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

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

```
screen! numtext (-3)                                   prints -3
```

We do not evaluate the application of the minus operator to the number 3, so the implementation 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: rat → 5) (1/0))                  should print 5
screen! bintext (1/0 = 1/0)                           should print true
screen! bintext ([0; 1] 2 = [0; 1] 2)                 should print true
```

No general-purpose programming language has ever been, or will ever be, implemented entirely. Every such language is infinite; every implementation is finite. There is always a program too big for the implementation. There is a multitude of size limitations: the parse stack might overflow, the dictionary (symbol table) might be too small, the forward branch fixup list might be exceeded, and so on. It would be ugly to define a programming language by listing all the size limitations of programs. And it would be counter-productive because it would exclude implementations that can accommodate larger programs.

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

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

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

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

\[ \text{nat} \text{ int} \text{ rat} \text{ bin} \text{ text} \left[ \text{n}^{*}\text{type} \right] \]

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

**Predefined Names**

There is a dictionary named \textit{predefined} . Here are the names in it. Each name is one of:

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

Some definitions use \( \mathcal{S} \) or \( \exists \), which are defined in \textit{a Practical Theory of Programming}.

- \textit{abs}: \( \text{com} \rightarrow \text{real} \text{ dat} \) Absolute value. \( \text{abs} \ x = \sqrt{r \times e + i \times m} \).
- \textit{all}: \( \text{dat} \) All ProTem items.
- \textit{arc}: \( \text{com} \rightarrow \mathcal{S}(r: \text{real} \rightarrow 0 \leq r < 2\pi) \text{ dat} \) An approximation to the angle or arc of a complex number.
- \textit{arccos}: \( \mathcal{S}(r: \text{real} \rightarrow -1 \leq r \leq +1) \rightarrow \mathcal{S}(r: \text{real} \rightarrow 0 < r < pi/2) \text{ dat} \) An approximation to a trigonometric function.
- \textit{arcsin}: \( \mathcal{S}(r: \text{real} \rightarrow -1 \leq r \leq +1) \rightarrow \mathcal{S}(r: \text{real} \rightarrow 0 < r < pi/2) \text{ dat} \) An approximation to a trigonometric function.
- \textit{arctan}: \( \text{real} \rightarrow \mathcal{S}(r: \text{real} \rightarrow 0 < r < pi/2) \text{ dat} \) An approximation to a trigonometric function.
- \textit{asm pro} A machine-dependent program with one text input parameter. If the input represents an assembly-language program, the execution is that of the represented assembly-language program.
- \textit{await pro} 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. See \textit{time} and \textit{wait} and \( s \).
- \textit{back}: \( *\text{nat} \rightarrow *\text{nat} \text{ dat} \) \( \text{back} \ (s; i) = s \).
backspace: char con
bin = true, false con
bintext: bin→text con bintext true = “true” and bintext false = “false”.
ceil: real→int dat r ≤ ceil r < r+1
char dat The characters.
charnat: char→nat dat A one-to-one function with inverse natchar .
click: char con
com dat The Complex numbers.
cos: real→§(r: real → -1 ≤ r ≤ +1) dat An approximation to a trigonometric function.
cosh: com→com dat An approximation to a hyperbolic function.
cursor: nat; nat dat A data name whose value is the current cursor position.
dictionaries: text dat The Names of the dictionaries in their current order, front first.
dictionary: text dat A text data name whose value is a readable summary of the content of the front dictionary.
div: real→§(r: real → r>0) → int dat div a d is the integer quotient when a is divided by d.
(0 ≤ mod a d < d) ∧ (a = div a d × d + mod a d)
doubleclick: char con
e = 2.718281828459045 (approx) con An approximation to the base of the natural logarithms.
encode: text→text dat A not easily invertible function.
end: char con The end-of-file character. It is greater than all letters, digits, punctuation marks, space, tab, and newline .
eval: text→*all dat 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 dat A function that says whether its argument is even or odd.
exec pro 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 dat An approximation to e↑x .
false: bin con A binary value.
find: all→*all→nat dat 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 = ↔S .
fit: int→text→text dat 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 dat floor r ≤ r < 1 + floor r
form: nat→nat→(nat+1)→real→text dat 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 “×10↑” 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 12 pi = “3.1416×10↑0”. form 2 0 6 (–pi) = “–3.14”. form 0 0 3 5 = “5”. form 0 0 3 (–5) = “–5”. form 0 0 2 123 = “***”.
formnum: text dat A text format for numbers. It is useful for reading a number from a text channel. The number may be preceded by spaces.
frontmost: text dat A text data name whose value is the compound name of the frontmost dictionary that has a name, out to an arbitrary distance. For example,
grammars_Hehner_cs_utoronto_ca

g unit con A unit representing mass in grams.
i = sqrt (-1) con The imaginary unit.
im: com→real dat The imaginary part of a complex number.
index = text→*nat dat A signal to the implementation that the string will be used only as an index to the indicated structure.
int dat The integers.
keys?! text cha To the program that monitors key presses, it is an output channel; to all other programs, it is an input channel.
lb: §(r: real → r>0) → real dat An approximation to the binary logarithm (base 2).
ln: §(r: real → r>0) → real dat An approximation to the natural logarithm (base e).
log: §(r: real → r>0) → real dat An approximation to the common logarithm (base 10).
m unit con A unit representing distance in meters.
mailin?! text. To the program that handles incoming mail, it is an output channel; to all other programs, it is an input channel.
mailout?! text cha 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 dat If pattern occurs within subject, then match pattern subject is the index of its first occurrence. If not, then match pattern subject = subject.
maxint: int con The maximum representable integer (machine dependent).
maxnat: nat con The maximum representable natural (machine dependent).
minint: int con The minimum representable integer (machine dependent).
mod: real → §(r: real → r>0) → real dat mod a d is the remainder when a is divided by d.
(movie = *pic dat
nat dat The natural numbers.
natchar: charnat char → char dat A one-to-one function with inverse charnat.
newline: char con The return or newline character.
nil con The empty string.
nul con The empty bunch.
numtext: com→text dat A text representation of a number. See also form.
odd: int→bin dat
ok pro A program whose execution does nothing and takes no time.
ord = real, char, bin, [*ord] dat The ordered type, for which < > ≤ ≥ are defined.
pi = 3.141592653589793 (approximately) con An approximation to the ratio of a circle's circumference to its diameter.
pic = [x*[y*(0..z)]] dat 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→char con The character predecessor function.
printer?! text cha To the printer, it is an input channel; to all other programs, it is an output channel.
randomNat: nat→nat→nat dat A reasonably uniform function, dependent on a hidden variable, over the interval from (including) the first argument to (excluding) the second argument.
randomNatInit pro A program with one constant natural parameter. Its execution assigns a hidden variable to the natural value.
randomNatNext pro A program. Its execution assigns a hidden variable to the next value in a random sequence.
randomReal: real→real→real dat A reasonably uniform function, dependent on a hidden variable, over the interval between the arguments.
randomRealInit pro A program with one constant real parameter. Its execution assigns a hidden
variable to the real value.

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

rat dat  The rational numbers.

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

real dat  The real numbers.

round: real→int dat  \(-0.5 \leq \text{round} \ r < r+0.5\)

s unit com  A unit representing time in seconds.

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

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

sign: real → (\(-1, 0, 1\)) dat  An approximation to a trigonometric function.

sin: real → §\(\langle r: \text{real} \rightarrow -1 \leq r \leq +1 \rangle\) dat  An approximation to a trigonometric function.

sinh: com→com dat  An approximation to a hyperbolic function.

sort: *ord→*ord dat  Sorts in nondecreasing order.

sqrt: com→com dat  An approximation to the principle square root.

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

subst: all→all→*all→*all dat  subst x y s  is a string formed from s by replacing all occurrences of y with x. Substitute x for y in s.

suc: char→char com  The character successor function.

tan: (§\(\langle r: \text{real} \rightarrow -\exists\langle i: \text{int} \rightarrow r = (2\times i + 1)\times\pi\rangle\rangle\)) → real dat  An approximation to a trigonometric function.

tanh: com→com dat  An approximation to a hyperbolic function.

text = *char dat  An approximation to a hyperbolic function.

textnum: text→com dat  If the argument represents a number, possibly preceded by spaces, the result is the represented number.

texttime: (int\(\times\)s) dat  If the argument represents a time, the result is the represented time in seconds since or before 2000 January 1 at 0:00 UTC (the midnight that begins 2000 January 1 at longitude 0). For example

texttime “1947 September 16 at 19:24 UTC” = \(-68675760\times s\).

time?! real\(\times\)s cha  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). Times before then are negative.

timetext: (real\(\times\)s)→text dat  A readable form of the time in seconds since or before 2000 January 1 at 0:00 UTC (the midnight that begins 2000 January 1 at longitude 0). Times before then are negative.

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

true: bin com  A binary value.

wait  pro  A program with one constant parameter of type real\(\times\)s. If the argument is nonnegative, its execution does nothing but takes the length of time in seconds given by the argument. If the argument is nonpositive, its execution does nothing. 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 numporters:= 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”, numporters
   | (“x”, “y”) → nat )] ` box position on screen
:= [numboxes * ((“ahead left”, “ahead right”, “behind left”, “behind right”) → 0
   | “beside” → 0
   | “above” → numporters ` indicates no porter above
   | (“x”, “y”) → 0 )].

new porter: [numporters * ("below" → index “box” ` what’s beneath
   | “arrival time” → real×s ` arrival time at this box
   | “speed” → real×m/s )] ` current speed
:= [numporters * (“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. x:= textnum keys l box.
    box:= (b; “beside”) → textnum keys l box.
  screen! “What are the x and y coordinates of box ”; numtext b; “? ”.
    keys! screen. x:= textnum keys l box.
    draw b “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.

randomNatInit 123456789. ` initialize a random number generator

` end of initialization, start of simulation

infinilooop
  do time? real. new iterationstarttime:= time.

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

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

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

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

` using boxesToDo calculate accel for porter p

nextbox do new b := (boxesToDo ↓ 0) 0. ` the box we are looking at
    new d := (boxesToDo ↓ 0) 1. ` its distance ahead of porter p
    boxesToDo := boxesToDo ↓ (1↓..¬(boxesToDo)
    if d ≤ maxdistance then new desiredspeed = ` according to porter pa
        ⟨pa: (index “porter”, numporters) →
        if pa = numporters then speedlimit
        else ( sqrt ( porter pa “speed” ↑ 2 + 2 × maxaccel × d
               + (maxaccel × cushion) ↑ 2 )
               − maxaccel × cushion ) ∧ speedlimit fi ).
        accel := ( ( ( desiredspeed (box b “above”) )
                   ∧ desiredspeed (porter (box b “beside”) “above”))
              − porter p “speed”)
        × impatience)
    ∨ ¬maxaccel ∧ maxaccel.
    if box b “above” = numporters = porter (box b “beside”) “above”
    then ` add boxes ahead to queue and continue
        boxesToDo := boxesToDo; [box b “ahead left”; d+1×m].
        if box b “ahead left” ≠ box b “ahead right”
        then boxesToDo := boxesToDo; [box b “ahead right”; d+1×m] fi.
    nextbox
    else if ¬(boxesToDo > 0 then nextbox fi fi fi od.

old boxesToDo.

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

await (iterationstarttime + visualdelaytime).
old speed. old accel. old p. old iterationstarttime.
infinitaloop od od `end of simport
Another Example Program

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

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

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

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

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

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

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

for length:= 1;..15
do for string:= 0;..(shl 1 length) ` each string of that length
    do for quote:= 0;..length ` each quote position (at least one bit to left of quote)
        do if even (shr string (length–1)) \ne even (shr string (quote–1)) ` roll-normalized
            then if ` repeat-normalized
                result repeatnorm: bin := true
                do new len: nat = \text{div} (length–quote) 2. ` the length of the possibly repeating part
                    trythislen do if len>0 \text{` 1} \le \text{len} \le (\text{length–quote})/2
                        then new extract = \(\langle i: \text{nat} \rightarrow (l: \text{nat} \rightarrow \text{` index } i \text{ length } l \rangle \)
                            shr string i – shl (shr string (i+l)) i \rangle\).
                    new ex:= extract quote len.
                    if ` the negative part is a repetition (twice or more) of ex
                        result r: bin = true
                        do new i: nat := quote+len. ` i+len \le length
                            iloop do new ey:= extract i len.
                                if ex=ey then i:= i+len. ` i\le length
                                if i\le length
                                    then iloop
                                else r:= false fi fi
                        else r:= false fi od od
                    then repeatnorm:= false
                    else len:= len–1. trythislen fi fi od od
            then for point:= 0;..length+1 ` each point position (right end, interior, left end)
                do if ` the rightmost bit is 1 or it’s to the left of quote or point
                    odd string \lor quote=0 \lor 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 \(1\) below it. When the stack is empty, the sequent is executed, the parse stack is reinitialized, and parsing resumes.

program sequent aftersequent
sequent phrase afterphrase
aftersequent . program 
empty
phrase new name afternewname
old name
do program od arguments 
if data then program elsepart fi arguments
for name := data do program od
\(\langle\) name parameterkind primary \(\rightarrow\) program \(\rangle\) arguments 
name aftername
elsepart else program
empty
parameterkind :
::
!
?

aftername front
:= data 
! data
? echoordata
do program od
arguments
echoordata ! name
data
afterphrase \(\|\) sequent 
empty
afternewname : data := data 
= data 
:= data
? ! data
do program od
front
unit
empty

data comparand aftercomparand
comparand element afterelement
element item afteritem
item term afterterm
term factor afterfactor
factor # factor
- factor
~ factor
+ factor
? factor
□ factor
\ factor
\ factor
* factor
ε factor
$ factor
↔ factor
primary afterprimary

primary number
text
if data then data else data fi arguments
result name : data := data do program od arguments
{ data }
[ data ] arguments
( data ) arguments
⟨ name : primary → data ⟩ arguments
name arguments

arguments number arguments
text arguments
if data then data else data fi arguments
result name : data := data do program od arguments
{ data }
[ data ] arguments
( data ) arguments
⟨ name : primary → data ⟩ arguments
name arguments
empty
A name control procedure is responsible for classifying names. For efficiency, the productions (except possibly the last) for each nonterminal should be placed in order of frequency. The following nonterminals have only one production each, so they can be eliminated: program sequent data comparand element item term.
LR(0) Grammar

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

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

```
program          sequent
                program . sequent

sequent          phrase
                 sequent || phrase

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

procedure       \( \langle \text{name} : \text{primary} \rightarrow \text{program} \rangle \)
                 \( \langle \text{name} :: \text{primary} \rightarrow \text{program} \rangle \)
                 \( \langle \text{name} ! \text{primary} \rightarrow \text{program} \rangle \)
                 \( \langle \text{name} ? \text{primary} \rightarrow \text{program} \rangle \)
                 procedure argument
                 name

data             data = comparand
                 data ≠ comparand
                 data < comparand
                 data > comparand
                 data ≤ comparand
```
data ≥ comparand
data : comparand
data ∈ comparand
data ⊆ comparand
comparand

comparand
comparand , element
comparand ... element
comparand | element
comparand ♦ data ♦ element
element

element ; item
element ;.. item
element ‘ item
item

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

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

factor
+ factor
– factor
∈ factor
$ factor
⇔ factor
# factor
~ factor
? factor
□ factor
iêu factor
* factor
primary * factor
primary → factor
primary ↑ factor
primary ↓ factor
primary
A name control procedure is responsible for classifying names.