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.

Symbols

ProTem has 12 keywords, plus 4 classes of symbols, plus 56 other symbols. Altogether they are:

if then else fi new old for do od result open close
number text name comment
:
:: := ::= = 
< > ≤ ≥ √ ! ? , . | || ( ) { } ⟨ ⟩ + − × / ↑ ↓ ← → ∧ ∨ @ + * ~

A number is formed as one or more decimal digits, followed optionally 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. We shall see that numbers can be negated, added, subtracted, scaled, and so on.

A text begins with a left-double-quote, continues with any number of any characters (but a double-quote (left or right) must be repeated), and concludes with a right-double-quote. Here are four examples.

“abc” “don’t” “Just say “‘no’”.” “’”

A name is either simple or compound. A simple name begins with a letter and continues with any number of letters and digits, except that keywords cannot be names. A compound name is composed of one or more simple names joined with underscore characters. Here are some examples.

simple names: x A1 george refStack
compound name: Hehner_grammars_ProTem

A comment begins with a % that is not in a text, and ends at the end of a line.

The following standard keyboard symbols are unused in ProTem: ^ & ' ` " \ 

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

for “ use " for ” reuse " for + use −=
for ≤ use <= for ≥ use >= for √ reuse ?
for ‘ use ’ for ( use << for ) use >>
for × use & for ↑ use ^ for ↓ use \ 
for → use −→ for ↔ use <-> for ∧ use /
for / use \/ for + reuse + for ~ reuse ~
for // use // for $ use size for ∈ use element
for ⊆ use subset for ∪ use union for ∩ use intersect
for □ use [] for Δ use nand for ∨ use nor
for < use < | for > use > |
Grammar

There are 25 ways of forming a program, and 53 ways of expressing data. (An LL(1/2) grammar and an LR(1/2) grammar are at the end of this document.) Here are the ways of expressing data. To the right of each there are examples and explanations and pronunciations.

<table>
<thead>
<tr>
<th>Data</th>
<th>Pronunciation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>minus, negation, not</td>
</tr>
<tr>
<td>1.2</td>
<td>plus, addition</td>
</tr>
<tr>
<td>data</td>
<td>minus, subtraction</td>
</tr>
<tr>
<td>data</td>
<td>times, multiplication</td>
</tr>
<tr>
<td>data</td>
<td>by, division</td>
</tr>
<tr>
<td>data</td>
<td>to the power, exponentiation</td>
</tr>
<tr>
<td>data</td>
<td>minimum, conjunction, and</td>
</tr>
<tr>
<td>data</td>
<td>maximum, disjunction, or</td>
</tr>
<tr>
<td>data</td>
<td>equals, equation</td>
</tr>
<tr>
<td>data</td>
<td>differs from, discrepancy</td>
</tr>
<tr>
<td>data</td>
<td>less than, strict implication</td>
</tr>
<tr>
<td>data</td>
<td>greater than, strict reverse implication</td>
</tr>
<tr>
<td>data</td>
<td>less than or equal to, implication</td>
</tr>
<tr>
<td>data</td>
<td>greater than or equal to, reverse implication</td>
</tr>
<tr>
<td>data</td>
<td>bunch union</td>
</tr>
<tr>
<td>data</td>
<td>from(including)...to(excluding)</td>
</tr>
<tr>
<td>data</td>
<td>bunch intersection</td>
</tr>
<tr>
<td>data</td>
<td>bunch inclusion</td>
</tr>
<tr>
<td>data</td>
<td>bunch size</td>
</tr>
<tr>
<td>data</td>
<td>string catenation</td>
</tr>
<tr>
<td>data</td>
<td>string from(including);..to(excluding)</td>
</tr>
<tr>
<td>data</td>
<td>string indexing</td>
</tr>
<tr>
<td>data</td>
<td>string modification</td>
</tr>
<tr>
<td>data</td>
<td>“abc”</td>
</tr>
<tr>
<td>data</td>
<td>string length</td>
</tr>
<tr>
<td>data</td>
<td>definite repetition</td>
</tr>
<tr>
<td>* data</td>
<td>indefinite repetition</td>
</tr>
<tr>
<td>[ data ]</td>
<td>list</td>
</tr>
<tr>
<td># data</td>
<td>list length</td>
</tr>
<tr>
<td>data</td>
<td>list catenation</td>
</tr>
<tr>
<td>data</td>
<td>list index, function application, composition</td>
</tr>
<tr>
<td>data</td>
<td>pointer indexing</td>
</tr>
<tr>
<td>{ data }</td>
<td>set</td>
</tr>
<tr>
<td>~ data</td>
<td>set content</td>
</tr>
<tr>
<td>data ∈ data</td>
<td>element of a set</td>
</tr>
<tr>
<td>data ⊆ data</td>
<td>subset</td>
</tr>
<tr>
<td>data U data</td>
<td>set union</td>
</tr>
<tr>
<td>data ∩ data</td>
<td>set intersection</td>
</tr>
<tr>
<td>′ data</td>
<td>power</td>
</tr>
<tr>
<td>$ data</td>
<td>set size</td>
</tr>
</tbody>
</table>
Next we have the ways of forming a program.

- new name : data create variable with type
- new name = data create data name
- new name :: program create program name
- new name ! create channel
- new name == name create synonym
- new name forward definition
- old name remove or hide
- open name open dictionary
- new open name create and open dictionary
- close name close dictionary
- name := data assign variable
- name ! data to channel send output
- name ? data from channel receive input of this type
- name ! to channel send signal
- name ? from channel receive signal
- name :: program create and call program name (label)
- name call program call program name
- text ::= program specified program; is refined by; is implemented by
- ( name : data → program ) procedure, parameter
- program data procedure argument
- program . program sequential composition
- program || program parallel composition
- if data then program else program fi conditional program
- for name : data do program od controlled program
- do program od parentheses

There is a precedence among the forms of program. It is

0. := ! ? :: ::= if then else fi do od for do od
1. . || left-to-right

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

new A:: B. C || D. E

when fully parenthesized, becomes

do new A:: B od. do do C || D od. E od
Here is the 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 –  left-to-right

5. ; ;.. ‘  infix

6. , ,.. | < > ≤ ≥  infix < > ≤ ≥

7. =  ≠  < > ≤ ≥  infix continuing

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

Whenever “data” appears in an alternative for “program”, the most general form of data is intended, with three exceptions. When a program is argumented, the argument must be on precedence level 0; therefore \( p a b \) means \((p a)\ b\). In a function and in a procedure, the parameter type 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, lists, and functions. We refer to each of these (numbers, characters, binary values, bunches, sets, strings, lists, and functions) as a type.

Numbers

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 \(-1\)). In addition to the 1-operand prefix operators + and – and the 2-operand infix operators + – \times \div \uparrow\downarrow \downarrow\uparrow there are predefined functions such as abs, exp, log, ln, sin, cos, tan, ceil, floor, round, re, im, sqrt, div, and mod (see Predefined Names). Division of integers, such as \( 1/2 \), may produce a noninteger. Exponentiation is 2-operand infix \( \uparrow \); for example, \( 1.2\times10\uparrow3 \) (one point two times ten to the power three). The operator \( \land \) is minimum (top is narrow, does not hold water, arms down). The operator \( \lor \) is maximum (top is wide, holds water, arms up).

In ProTem, subsets of numbers are not considered disjoint types. A natural number is an integer number; an integer number is a real number; a real number is a complex number.

Characters

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 four predefined character names: backspace, tab, return, and end (the end-of-file character). The operators suc and pre give the successor and predecessor respectively.
Binary Values

There are two predefined binary names in ProTem: `true`, and `false`. Negation is –, 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, to characters, to binary values, to strings of ordered items, and to lists of ordered items, with a binary result; the two operands must be of the same type. In the binary order, `false` is below `true`, so \( \leq \) is implication. The 3-operand operator `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, namely:

- `null` - empty
- `nat` - all natural numbers: \( 0, 1, 2, \ldots \)
- `int` - all integer numbers: \( \ldots, -2, -1, 0, 1, 2, \ldots \)
- `real` - all real numbers: \( \ldots, 2^{\uparrow}(1/2), \ldots \)
- `com` - all complex numbers: \( \ldots, (-1)^\uparrow(1/2), \ldots \)
- `char` - all characters: \( \ldots, \text{“a”}, \ldots \)
- `bin` - both binary values: `true`, `false`
- `text` - all texts (character strings): \( \ldots, \text{“abc”}, \ldots \)
- `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 element. For example, the number `2` is an elementary bunch, or synonymously, an 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

\[ x,..,y \]

“\( x \ to \ y \)” (but not “\( x \ through \ y \)”) 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

\[ A : B \]

“\( A \ is \ included \ in \ B \)”

is binary. The size of a bunch is \( \varepsilon \). For examples, \( \varepsilon(0, 1, 2) = 3 \) and \( \varepsilon(null) = 0 \).

Bunches are equal if and only if they consist of the same elements, without regard to order or multiplicity.

In ProTem, all operators whose precedence is before that of bunch union distribute over bunch union. For examples,
\[ -(3, 5) = -3, -5 \]
\[ (2, 3) + (4, 5) = 6, 7, 8 \]

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

Nonempty bunches serve as a type structure in ProTem.

**Sets**

A set is formed by enclosing a bunch in set braces. For examples, \{0, 2, 5\}, \{0..100\}, \{null\}, \{nat\}. The inverse of set formation is \(\sim\). For example, \(\sim\{0, 1\} = 0,1\). The size of a set is \(\$\). For examples, \$\{0, 1\} = 2 and \$\{null\} = 0. The element, subset, union, and intersection operators \(\in\) \(\subseteq\) \(\cup\) \(\cap\) are as usual. The power operator \(\uparrow\) takes a bunch as operand and produces all sets that contain only elements of the bunch. For example, \(\uparrow\{0, 1\} = \{\text{null}\}, \{0\}, \{1\}, \{0, 1\}\).

**Strings**

Just as bunches are unpackaged sets, so strings are unpackaged lists. There is a predefined string name:

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

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

String catenation is denoted by a semi-colon:

\[ S; T \quad \text{“} S \text{ catenate } T \text{”}, \text{“} S \text{ join } T \text{”} \]

For example, \(2; 3; 5; 7\) is a string of four integers. There is also the notation

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

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 \(5;..5\) is the empty string.

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, \((2; 3; 5; 7) \downarrow 2 = 5\). A string can be indexed by a string. For example, \((3; 5; 7; 9) \downarrow (2; 1; 2) = 7;5;7\).

If \(S\) is a string and \(n\) is an index of \(S\) and \(i\) is any item, then \(S \ngtr n \triangleright i\) is a string like \(S\) except that item \(n\) is \(i\). For example, \((3; 5; 9) \ngtr 2 \triangleright 8 = 3;5;8\).

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

\[
\text{“}abc\text{”} = \text{“}a\text{”}; \text{“}b\text{”}; \text{“}c\text{”}
\]

\[
\text{“He said ““Hi”””} = \text{“}H\text{”}; \text{“}e\text{”}; \text{“}”\text{”}; \text{“}s\text{”}; \text{“}a\text{”}; \text{“}l\text{”}; \text{“}d\text{”}; \text{“}”\text{”}; \text{“}H\text{”}; \text{“}i\text{”}; \text{“}”\text{”}; \text{“}”\text{”}.
\]

\[
\text{“abcdefg}h\text{j} \downarrow (3;..6) = \text{“def”}
\]

Strings are equal if and only if they have the same length, and corresponding items are equal.
We allow a bunch of items to be an item in a string. Since string catenation precedes bunch union, we have

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

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

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

\[n * S\]  

“\( n \) copies of \( S \)” or “\( n \) \( S \)’s”

is a string, and

\[*S\]  

“strings of \( S \)” or “any number of \( S \)’s”

is a bunch of strings. For examples,

\[3*5 = 5;5;5\]  
\[*5 = nil, 5, 5;5, 5;5;5, 5;5;5;5, ...\]

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

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

Using this semi-distributivity, we have

\[*a = nat*a\]

**Lists**

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

\[[0; 1; 2]\]

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

\[\# L\]  

“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 \( p \)”

\[L ^+ M\]  

“\( L \) catenate \( M \)”, “\( L \) join \( M \)”

\[L M\]  

“\( L \) composed with \( M \)”

\[L \vert M\]  

“\( L \) otherwise \( M \)”, “the selective union of \( L \) and \( M \)”

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

Here are some examples.

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

(the number of items in a list)

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

\[0;..10 \sim 5 = 5\]  

(indexing starts at zero)

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

\[0;..10 ^+ [10;..20] = [0;..20]\]

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

(in general, \((L M)n = L(M n)\).)

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

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

By using the \(@\) operator, a string acts as a pointer to select an item from within an irregular structure. If the list \( L \vert M \) 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 \( M n \).

\[10; 11 \vert [0;..10] = [10; 11; 2;..10]\]

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

Let \(p\) be a fresh name, let \(D\) be a bunch of items, and let \(B\) be an element (possibly using \(p\) as an element of \(D\)). Then

\[
\langle p: D \rightarrow B \rangle
\]

is a function in parameter \(p\) with 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

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

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

The notation for applying a function to an argument is the same as that for indexing a list: juxtaposition. Also, composition and selective union can have function operands, and even a mixture of list and function operands.

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

\[2 \rightarrow 3\]

abbreviates \(\langle n: 2 \rightarrow 3 \rangle\). An example of its use is

\[1 \rightarrow 21 | [10; 11; 12] = [10; 21; 12]\]

We allow domains to be strings in the following circumstances.

\[\text{nil} \rightarrow x | f = x\]

\[(x;y) \rightarrow z | f = x \rightarrow (y \rightarrow z | f) \rightarrow f\]

Thus, for example,

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

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

\[(f, g) (x, y) = fx, fy, g x, g y\]

Allowing the body of a function to be a bunch generalizes it to a relation. For example, \(nat \rightarrow bin\) can be viewed in any of the following three equivalent ways: it is a function (with unused and therefore omitted parameter) that maps each natural to \(bin\); it is a relation relating each natural to each binary value; it is all functions with domain \(nat\) and range \(bin\). As an example of the last view, we have

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

If \( c \) is the name of an input channel, then
\[
\sqrt{c}
\]
is a binary expression saying whether there is currently any unread input on channel \( c \).

Programmed Data

**result** name : data do program **od**

First, a local variable is introduced. Then the program is executed, but changes to nonlocal variables are made on local copies. The result is the final value of the newly introduced 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: real
do sum:= 1.
   **new** term: real. term:= 1.
   **for** i: 1;..15 **do** term:= term/i. sum:= sum+term **od** **od**

There are no side effects. Suppose \( x \) is a natural variable with value 5. Then evaluation of

**result** y: int **do** x:= x+1. y:= x **od**
yields 6, but variable \( x \) remains unchanged with value 5.

Names and Dictionaries

Each name in a dictionary is defined to be one of the following: a variable, a data name, a program name, a channel, or a dictionary name. When a name is defined to be a dictionary, this dictionary also can contain 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. There is a dictionary named \( ca \), within which there is a dictionary named \( utoronto \), within which there is a dictionary named \( cs \), within which there is a dictionary named \( Hehner \), within which there is a dictionary named \( grammars \), within which there is a text named \( ProTem \). This text can be referred to as \( ca_{utoronto}_{cs}_{Hehner}_{grammars}_{ProTem} \).

A dictionary is either closed or open. We can **open** a closed dictionary, and **close** an open dictionary. By opening dictionaries, we can shorten the names we use. The text referred to by the lengthy compound name in the previous paragraph can be referred to simply as **ProTem** if the dictionary \( grammars \) is open. The predefined names include a dictionary named \( complex \), within which there is a name \( i \). It can always be referred to as \( complex_i \). If we are going to refer to it often, we might want to shorten this. We do so by saying **open** \( complex \), and then we can say just \( i \).

Whenever a simple name is used, it is looked up in the open dictionary that was opened last; if it is not there, it is looked up in the open dictionary that was opened next-to-last; and so on. The first definition found for the name is the one used. If the name is not in any open dictionary, it is unknown (even though it may be in some closed dictionaries).

Whenever a compound name is used, it is looked up as follows. The first simple name in the compound name is looked up in the usual way (starting with the open dictionary that was opened last). Its definition must be as a dictionary. The second simple name in the compound name is looked up in this one dictionary (whether open or closed). If there is a third name in the compound name, then the second name must be defined as a dictionary, and the third name is looked up in that dictionary. And so on for subsequent names in a compound name.
Names are defined by language constructs beginning with *new*, and as function parameters, and as procedure parameters, and as for-loop parameters, and as *result* variables. Whenever a simple name is defined, its definition is written in the open dictionary that was opened last (it must not already be there). When a compound name is defined, the last simple name in the compound name is placed in the dictionary referred to by the compound name minus its last simple name.

Names defined by *new* can be removed from a dictionary with the keyword *old* (it must already be there). Further details and examples will be presented later.

**Programs**

About half of the program constructs are concerned with dictionaries: adding names (*new*), deleting names (*old*), opening a dictionary (*open*), and closing a dictionary (*close*). The other half are variable assignment, input, output, and a variety of ways of combining programs to form larger programs.

**Variable Definition**

Here is an example variable definition (declaration).

```
new x: 0..10
```

This defines *x* to be a variable assignable to any element in 0..10, and initially assigned to an arbitrary element in that bunch. In other words, *x* is defined so that *x*: 0..10 is always true, even initially. But the subsequent program cannot depend on any particular initial value. There is no such thing as “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 can depend on previously defined names, including variables.

If you want a variable to be defined with a specific initial value, just follow the definition with an assignment. Here are three examples.

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

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

**Assignment**

Assignment is as usual: the data on the right must be an element in the type of the variable on the left. Here are two examples using the definitions of the previous section.

```
x:= 5
s:= 3 → 5 | s
```
Data Definition

Data definition gives some data a name. Here are four examples.

\begin{verbatim}
new size = 10
new range = 0..size
new piBy2 = pi / 2
new y = s x
\end{verbatim}

The first three names are constants because their definitions use only constants (\( \pi \) is a predefined constant). The fourth definition makes \( y \) depend on variables \( s \) and \( x \) defined previously; the value of \( y \) changes according to the values of \( s \) and \( x \) so that \( y = s \times x \) is always true. We may call \( s \) and \( x \) “independent variables”, and \( y \) a “dependent variable”. Notice the difference between this and

\begin{verbatim}
new z; s x
\end{verbatim}

Here, \( z \) is defined as an independent variable whose type is a single value, namely, the value of \( s \times x \) when this definition is executed. It therefore has that value. Its value does not change when \( s \) and \( x \) change.

The next two examples define \( \text{fact} \) and \( \text{div} \) to be the factorial function and integer divisor function for natural numbers. They are both constants. Note the use of recursion.

\begin{verbatim}
new fact = 0 → 1 \langle n: (nat+1) → n \times \text{fact}(n–1) \rangle

new div = \langle a: nat → (d: (nat+1) → 
  if (a < d) then 0 
  else if even a then 2 \times \text{div}(a/2) \times d 
  else 1 + \text{div}(a–d) \times d \rangle
\end{verbatim}

A final example defines all binary trees with integer nodes.

\begin{verbatim}
new tree = [nil], [tree; int; tree]
\end{verbatim}

Program Definition

Program definition gives a program a name. For example,

\begin{verbatim}
new switchends:: s:= 0 → (s 9) \langle 9 → (s 0) \mid s \rangle
\end{verbatim}

The double colon is pronounced “is”. Execution of this definition creates the program name \text{switchends} , but does not execute program \text{switchends} . After execution of this definition, the name \text{switchends} can be used to cause execution of the program it names. Definitions can be recursive.

One of the predefined program names is \text{ok} , whose execution does nothing. It is used, for example, with \text{if} . (See Conditional Program.)

Forward Definition

The “forward definition” is a notice that a definition will follow later. It is used, for example, when definitions are mutually recursive. (See \textbf{Scope}.)

Name Removal

Names are added to a dictionary with the keyword \textbf{new}, and they are removed from a dictionary with the keyword \textbf{old}. 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,
new s: [*all].  s:= [nil].
new push:: (x: all → s:= s + [x]).
new pop:: s:= s [0..#s–1].
new top = s (#s–1).
new empty = s=[nil].
old s.

The names push, pop, top, and empty are now defined for everyone's 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.

Dictionaries

The syntax

new open d

is used to create a new dictionary, entering its name d in the open dictionary that was opened last, and then opening d. The syntax

open d

is used to open an existing but closed dictionary d. The syntax

close d

is used to close an open dictionary.

The predefined names include a dictionary named random, within which there are three names: init, next, and value. It might have been defined as:

new open random.
new big = 2↑31.
new rv: 0..big.
new init:: (seed: (0..big) → rv:= seed).
new next:: rv:= mod (rv × 5↑13) big.
new value = ⟨from: real → (to: real → from + (to–from)×rv/big)⟩.
old big.  old rv.
close random.

Variable rv is now hidden; its name is removed from the dictionary, but init, next, and value still use it. We can use the definitions in this dictionary in the following way:

random_init 123456789.
random_next.
screen! numtext (random_value 0 1).

Or, if we are going to use them often, we may want to shorten what we say as follows:

open random.
init 123456789.
next.
screen! numtext (value 0 1).

We can get rid of a dictionary name d by saying

old d

Removing a dictionary name by old also removes all names in that dictionary. The dictionary remains in existence, closed and anonymous, as long as something refers to it or to its contents.
Synonym Definition

The syntax

    new a == b

makes name a a synonym of name b. The two names are now equivalent in every way. Synonym definition can be used to rename a variable or channel or dictionary as follows.

    new newname == oldname. old oldname

It can be used to move a name from one dictionary to another as follows:

    new toDict_name == name. old name

or as follows:

    new name == fromDict_name. old fromDict_name

depending on which dictionary was opened last.

Output and Input

The channels screen, printer, keys, cursor, and time are predefined.

The program

    screen! “Hi there”

sends the text “Hi there” to the screen. A string of outputs can be sent together

    screen! “Answer = ”; numtext x; “ meters”

This is equivalent to

    screen! “Answer = “. screen! numtext x. screen! “ meters”

One integer of input is requested on channel keys by the program

    keys? int

If input is not yet available, it is awaited. When the input is received, it is referred to simply as keys.

Sequential Composition

Sequential composition is denoted by a period (.). It is an infix connective.

Parallel Composition

For programs P and Q that assign different variables, or different parts of a structured variable, the parallel composition of P and Q is denoted P || Q. Each program can use the variables assigned by the other, but all occurrences of variables assigned by the other program refer to their initial value. 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.

Channel Definition

The definitions

    new c!
    new d!

define c and d to be channels. They can be used, even without parallelism, just as buffers. For example,

    c! 5. c! 7. c? int. x:= c. c? int. y:= c
assigns $x$ to 5 and $y$ to 7. More often, channels are defined for communication between parallel programs.

```
do c! 7. d? int. x:= d od
|| do d! 5. c? int. y:= c od
```

The output in one program can be input in all parallel programs independently. However, two parallel programs cannot use the same channel for output.

### Conditional Program

The if is as usual. There is no one-tailed if in ProTem; the ProTem equivalent is shown in the following example.

```protem
if x > y then x:= y else ok fi
```

An “assert” program is obtained according to the following example.

```protem
if x > y then ok else screen! “appropriate error message”. stop fi
```

### Named Programs

A named program has the syntax

```
name :: program
```

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. 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, $A: [n*[m*int]]$).

```protem
new i: nat. i:= 0.
tryThisI:: if i=n then screen! x; “ does not occur.”
else new j: nat := 0.
tryThisJ:: if j=m then i:= i+1. tryThisI
else if A i j = x then screen! x; “ occurs at ”; i; j
else j:= j+1. tryThisJ fi fi fi
```

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

```protem
r:= a.
outerloop:: if r<d then ok
else new dd: nat. dd:= d.
innerloop:: do r:= r/dd. dd:= dd+dd.
if r<dd then outerloop else innerloop fi od fi
```

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 $f_n$ is the $n$th Fibonacci number, and it does so in $\log n$ time.

```protem
F:: if n = 0 then x:= 0. y:= 1
else if odd n then n:= (n–1)/2. F. n:= x. x:= x↑2 + y↑2. y:= 2×n×x+y↑2
else n:= n/2 – 1. F. n:= x. x:= 2×x×y + y↑2. y:= n↑2 + y↑2 + x fi fi
```

The following two lines are equivalent to each other.

```protem
P:: Q
do new P:: Q. P od
```
Specified Program

A program can optionally include a specification in the form of a text. For example,

\[ x' := x + 1 \]

The symbol \( ::= \) can be pronounced “is refined by” or “is implemented by”. If the specification is written within the language that the prover understands, the prover attempts to prove that the specification is refined (implied, implemented) by the program. If the program includes, within it, another specified program, it is the specification, not the program, that is used in the outer proof. If the prover fails to understand the specification, or fails to prove the refinement, it informs the programmer, and treats the specification as a comment.

Naming and specification are independent, and can be used together. For example,

\[ addRest:: s' = s + \sum L [n;..#L] := \] 

When a specified program is named (as in the previous line), the meaning of the name is the specification, not the program. So the meaning of \( addRest \) is “\( s' = s + \sum L [n;..#L] \)”, including its recursive occurrence.

Controlled Program

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

\[
\begin{align*}
\text{for } i: 0;..n & \text{ do for } j: 0;..n \\
& \text{ do for } k: 0;..n \\
& \text{ do } A := (i;k) \rightarrow (A i k \lor (A i j \land A j k)) | A \od \od \od
\end{align*}
\]

The assignment can be restated as

\[
\text{if } A i j \land A j k \text{ then } A := (i;k) \rightarrow true | A \text{ else ok fi}
\]

if you prefer. The name being introduced by \textbf{for} is known only within the loop body, and it is known there as a data name. It is not a variable, and so it is not assignable. We call it the \textbf{for} parameter.

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

\[
\begin{align*}
\text{new } n &= 1000. \\
\text{new } prime: [n*bin]. \text{ prime}:= [2*false; (n–2)*true]. \\
\text{for } i: 2;..\text{ceil} \left( \sqrt{n} \right) & \text{ do if } prime i \text{ then for } j: i;..\text{ceil} \left( n/i \right) \text{ do } prime := (ixj) \rightarrow false | prime \od \text{ else ok fi od}
\end{align*}
\]

The \textbf{for} parameter is “by initial value”, so

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

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

After the \textbf{for} we can have any string expression; the parameter stands for each item in the string, in sequence. We can also have any bunch expression; the parameter stands for each element of the bunch, in parallel. As an example,

\[
\text{for } i: 0;..n \text{ do } A := i \rightarrow 0 | A \od
\]

makes the first \( n \) 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 be parameterized, as in this example.
\[ \langle y: \text{num} \rightarrow x := xy \rangle \]
A program with one or more parameters is called a “procedure”. A procedure of two parameters is a procedure of one parameter whose body is a procedure of one parameter. A procedure can be argumented in the same way that lists are indexed and functions are argumented. For example,
\[ \langle y: \text{num} \rightarrow x := xy \rangle 3 \]
which is the same as
\[ x := x \times 3 \]

A procedure’s parameter is known only within the procedure body, and it is known there as a data name. It is not a variable, and so it is not assignable. It is “by initial value”, so
\[ \langle i: \text{int} \rightarrow x := i, y := i \rangle (x+1) \]
gives both \( x \) and \( y \) a final value one greater than \( x \)'s initial value.

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.

\[
\begin{align*}
\text{A. B} & \quad \text{for } x: A \text{ do } B \text{ od} \\
\text{or} & \\
A. & \quad \text{for } x: A \\
B & \quad \text{do } B \text{ od} \\
\text{or} & \\
\text{if } A \text{ then } B \text{ else } C \text{ fi} & \quad \text{result } x: A \text{ do } B \text{ od} \\
\text{or} & \\
\text{if } A \text{ then } B \\
\text{else } C \text{ fi} & \quad \text{result } x: A \\
\text{or} & \\
\text{if } A \\
\text{then } B \\
\text{else } C \text{ fi} & \quad \langle x: A \rightarrow B \rangle \\
\text{or} & \\
A \ || \ B & \quad \langle x: A \rightarrow \ \\
\text{or} & \\
A. & \quad A \ + \ B \\
\text{or} & \\
B & \quad A \\
\text{or} & \\
\text{|| } B & \quad A \ + \ B
\end{align*}
\]
Scope

In general, scopes are limited by `do od` and `{ }` brackets.

A name introduced by the keyword `new` must be fresh, i.e. not defined since the previous `do` or `{`. Its scope extends from its definition to the next `od` or `}`. But it may be covered by a definition in a more local scope. For example, letting $A, B, C, ...$ stand for arbitrary program forms, in

A. `new x: int. B. do C. new x: bin. D od. E`

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

A name introduced by `new` can be removed from the dictionary by using `old`, ending its scope early. So in

```
new x = 0. A. old x. B
```

the definition of $x$ is in effect in $A$ but not in $B$. Within $B$, the name $x$ has the same meaning (if any) that it had before the previous `do` or `{`. After `old x`, the name $x$ is again fresh and available for definition. However,

```
new x = 0. do old x. A od
```

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

If a name is introduced by `new` outside all `do od` and `{ }` pairs, its scope ends only with an `old`. Its scope does not end with the end of a computing session, not even by switching off the power. Variables declared outside all parentheses serve as “files”. A predefined name cannot have its scope ended by `old`, but it can be obscured by a programmer's redefinition of the same name.

In a variable definition, the name being introduced cannot be used in the type and initialization; its scope begins after that.

In a data or program definition, the scope of the name being introduced starts immediately. This allows the definitions to be recursive. The forward definition allows mutual recursion by starting the scope of a data name or program name even before its definition. For example, in

```
new f = 3. do new f. new g = ···f···g···. new f = ···f···g···. B od
```

$f$ and $g$ are each defined in terms of both of them. Without the forward definition of $f, g$ would be defined in terms of the less local $f=3$.

A name can be introduced without the keyword `new`, as a procedure parameter or function parameter or `for` parameter, or `result` variable, or as the name of a named program. Any such name must be fresh within the most local scope, i.e. since the previous `do` or `{`, just like a name introduced with the keyword `new`. Its scope extends only through the program or data to which it is attached, not beyond. After that, it is again fresh and available for definition.

The opening and closing of dictionaries obey the same scope rules. In a program of the form

A. `do B od. C`

all names in all dictionaries, and which dictionaries are open, and the order in which they were opened, are the same at the start of $C$ as they were at the end of $A$, regardless of any local changes within $B$. However,

```
open d. do close d. A od
```

is not allowed; a dictionary cannot be closed in a subscope of the one in which it was opened.
Miscellaneous

The ProTem equivalent of enumerated type is shown here.

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

The ProTem equivalent of the record type is as follows.

```protem
new person = "name" → text | "age" → nat.
new p: person. p := "name" → "Josh" | "age" → 16.
```

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

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

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

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

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

```protem
new file: *person. file := nil.
and catenate new records onto its end.
file := file; p.
```

The efficiency of pointers is obtained through the use of three predefined names. The first is:

```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 number will be used only as an index into the list whose name is given by the text argument (and the implementation will check that this is so). For example,

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

We can still assign `first` to a natural number, for example

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

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

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

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

The other two predefined names that give pointer efficiency are

```protem
new path = text → * nat
new backup = ⟨list: [* nat] → ~ list [0;..#list–1]⟩
```

The use of `path` is a signal to the implementation that the string of natural numbers will be used only as a string of indexes into the structure whose name is given by the text argument (and the implementation will check that this is so). For example,

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

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

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

and similarly to move it down to the right. To move it up, we just remove its final item
Indexing $t$ with $p$ yields a subtree of $t$

$t @ p$

and we can replace this subtree with tree $s$ using the assignment

$t := p \rightarrow s | t$

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

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

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

$t := p; 1 \rightarrow 6 | t$

We obtain the performance benefit of having $p$ implemented as a string of addresses rather than as a string of natural numbers, without complicating the language.

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

```
new transformX:: \langle \text{magnification: num } \rightarrow \langle \text{translation: num } \rightarrow \\
x := \text{magnification} \times x + \text{translation} \rangle \rangle
```

Here is a procedure with one parameter

```
new translateX:: transformX 1
```

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.

```
new magnifyX:: \langle \text{magnification: num } \rightarrow \langle \text{transformX magnification 0} \rangle \rangle
```

We can now obtain a three-times magnification of $x$ in either of these ways.

```
magnifyX 3
transformX 3 0
```

The function of some other programming languages is a combination of naming, parameterizing, and programmed data. For example,

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

Exception handling is provided by bunch union or by the | operator. For example,

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

We can state the type of this function as

`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

```
new weekday = \langle d: (0,..7) \rightarrow 1 \leq d \leq 5 \rangle
```

Then in the expression

```
(weekday | all→“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.

```
inputchoice:: \quad \text{if } \sqrt{c} \text{ then } c?\text{int. } P \\
\text{else if } \sqrt{d} \text{ then } d?\text{int. } Q \\
\text{else inputchoice fi fi}
```
The effect of modules is partly obtained by \texttt{old} and partly by dictionaries. There is no direct counterpart to the import 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 generate such comments on request. It is also possible for programmers to make such comments in an agreed format so that an implementation can recognize them and check them. Here is a suggested standard.

\begin{itemize}
  \item \% input: on these channels.
  \item \% output: on these channels.
  \item \% need: the values of these variables.
  \item \% assign: these variables.
  \item \% use: these data names.
  \item \% call: these program names.
  \item \% refer: to these dictionaries.
\end{itemize}

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

A loophole that allows us to drop down into assembly language is provided by the predefined procedure \texttt{asm}, which has one text parameter. If the argument represents an assembly-language program, the execution is that of the represented assembly-language program. An implementation may provide procedures for a variety of languages; for example, it may provide a procedure named \texttt{Java}, with one text parameter, whose execution is that of the Java fragment represented by the argument.

\section*{Other Issues}

\subsection*{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, and should be done whenever it is helpful. 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, they can be defined as items in a list. Or, if you prefer, they can be instantiated by re-invoking the program that defines one of them.

\subsection*{Documents}

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

\begin{verbatim}
  new p: pic.
\end{verbatim}

The name \texttt{pic} is defined as \([x*[y*(0.,z)])\) where \(x\) is the number of screen 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 \(p_{34}\).

Another predefined name is \texttt{movie}, defined as \([*pic]\). The operations on movies are just those of lists, 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.

WE NEED a sound (noise) data type. WE ALSO NEED a way to combine all of these types in one document. WE ALSO NEED to be able to define regions of documents to be clickable links.
Editing

THIS SECTION IS NOT YET THOUGHT OUT  The command control-e (hold down the control key and type an e) invokes an editor for creating or modifying any definition (variable, data name, program name, channel, or dictionary name). When a program name is defined, the defined program is not immediately compiled; it is compiled when it is first invoked. When its definition is modified, the old executable form is thrown away; the new definition is not compiled until it is invoked. It may also be necessary to throw away the executable form of all programs that depend directly on the redefined name.

Session

When the computer is turned on, a session begins. When control-q is typed, a session ends and a new one begins. When a number of idle minutes pass (the number 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 screen is clear and is divided into two regions; one region shows what is input on channel key, and the other is the output from the computer on channel screen. Input and output on separate channels are not mixed. Also at the start of a session, only the root dictionary is open and all passwords are required. A password will not be requested twice within the same session for the same dictionary.

Sessions do not define the lifetime of definitions (variables, data, programs, dictionaries). A definition that is outside all do od 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, and whose values outlast a session, to be saved in permanent memory.

Sessions are defined for each user of a multiuser computer, and are for security and error recovery.

Security

Any dictionary may contain a variable definition such as

```
new password: nat. password:= encode "my mother's maiden name"
```

If a dictionary contains a variable named password, the text whose encoding is its value will be requested when an attempt is made to open the dictionary or to refer to its contents. Passwords belong to dictionaries, not to people. For example

```
new open readBarrier.
new password: nat. password:= encode "read code".
new open writeBarrier.
new password: nat. password:= encode "write code".
new it: real. it:= 17.2.
close writeBarrier.
new readonlyit = writeBarrier_it.
close readBarrier.
```

To use data name readonlyit, either by opening dictionary readBarrier or as readBarrier_readonlyit, you must know the password “read code”. This enables you to know the
value of variable \textit{it}, but not to change it. To change it, you must know a second password, “write code”.

\textbf{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. To do so, type control-u (for “undo”). The undo command not only aborts execution, but also returns to the state 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. In that case it acts 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 \textit{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).  

\begin{verbatim}
  new copy: text. copy := session.
\end{verbatim}

One then edits the keystroke file, perhaps using the text editor, and then executes the result.  

\begin{verbatim}
  exec copy.
\end{verbatim}

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

\textbf{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:

\begin{itemize}
  \item control-e: enter editor
  \item control-q: quit session
  \item control-u: undo program
  \item control-s undo session
\end{itemize}

\textbf{Implementation Philosophy}

No general-purpose programming language has ever been, nor 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 may give the programmer 3 options: change the program to live within the limitation; change the compiler 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 declaration, the type must be one of

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

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, and so allow an implementer to invent ways to implement programs that previous implementations could not accommodate.

Predefined Names

\( \text{abs: com} \rightarrow \text{real} \). Absolute value. For complex \( x \),
\[ \text{abs} \ x = \sqrt{\text{re} \ x \uparrow 2 + \text{im} \ x \uparrow 2} \].
\( \text{all} \). All ProTem items.
\( \text{asm} \). A machine-dependent program with one text parameter. If the argument represents an assembly-language program, the execution is that of the represented assembly-language program.
\( \text{await} \). A program with one parameter of type \( 5*\text{nat}; \text{real} \). Its execution does nothing but takes time until the instant given by the argument. See \( \text{time} \) and \( \text{wait} \).
\( \text{backspace: char} \).
\( \text{backup: } [\text{nat}] \rightarrow \text{nat} \). \( \text{backup} \ [s; i] = s \). For use with \( \text{path} \).
\( \text{bin} = \text{true}, \text{false} \).
\( \text{calculus} \). A dictionary containing the following names.
\[ e = 2.718281828459045 \) (approx). An approximation to the base of the natural logarithms.
\( \text{exp: real} \rightarrow \text{real} \). An approximation to \( e^{x} \). (The domain and range should probably include complex numbers, but I have forgotten my complex analysis.)
**lb**: $\text{\texttt{\$}}(r: \text{real} \to r>0) \to \text{real}$. An approximation to the binary logarithm (base 2).

**ln**: $\text{\texttt{\$}}(r: \text{real} \to r>0) \to \text{real}$. An approximation to the natural logarithm (base $e$).

**log**: $\text{\texttt{\$}}(r: \text{real} \to r>0) \to \text{real}$. An approximation to the decimal (common) logarithm (base 10).

**ceil**: real $\to$ int. $r \leq \text{ceil} r < r+1$

**char**. The characters.

**charint**: char $\to$ int. A one-to-one function with inverse **intchar**.

**com**. The complex numbers.

**complex**. A dictionary containing the following names.

**arc**: com $\to$ $\text{\texttt{\$}}(r: \text{real} \to 0 \leq r < 2\pi i)$. An approximation to the angle or arc of a complex number.

**i** = $\text{\texttt{sqrt}}((–1))$. The imaginary unit.

**im**: com $\to$ int. The imaginary part of a complex number.

**re**: com $\to$ real. The real part of a complex number.

**context**: com $\to$ text. A textual representation of a complex number.

**cursor!** [nat, nat]. An input channel.

**dictionary**: text. A readable summary of the content of the open dictionary that was opened last.

**div**: real $\to$ $\text{\texttt{\$}}(r: \text{real} \to r>0) \to$ int. div $a d$ is the integer quotient when $a$ is divided by $d$.

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

**encode**: text $\to$ nat. A not easily invertible function. SHOULD IT BE text $\to$ text.

**end**: char. The end-of-file character. It is greater than all letters, digits, punctuation marks, space, tab, and return.

**eval**: text $\to$ all. If the argument represents a ProTem data expression, the evaluation is that of the represented data. It “unquotes” its argument. IN **eval** “x” WHAT x ARE WE TALKING ABOUT?

**even**: int $\to$ bin.

**exec**. A program with one text parameter. If the argument represents a ProTem program, the execution is that of the represented program. It “unquotes” its argument. IN **exec** “x:= x +1” WHAT x ARE WE TALKING ABOUT?

**false**: bin. screen! false prints false

**find**: all $\to$ [*all] $\to$ nat. If $i$ is an item in $L$, then find $i L$ is the index of its first occurrence; if not, then find $i L = \#L$.

**fit**: text $\to$ int $\to$ text. If $i \geq 0$ then fit $t i$ 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 $t i$ 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 $\to$ int. floor $r \leq r < 1 + \text{floor} r$

**form**: real $\to$ nat $\to$ nat $\to$ (nat+1) $\to$ text. Format a real number. form $r$ $d$ $e$ $w$ 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^↑0” 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 $\pi$ 4 1 12 = “ 3.1416×10^↑0”. form $(–\pi)$ 2 0 6 = “–3.14”.

form $5$ 0 $0$ 3 = “ 5”. form $(–5)$ 0 $0$ 3 = “–5”. form $123$ 0 $0$ 2 = “***”.

**hyperbolic**. A dictionary containing the following names. (The domains and ranges should probably include complex numbers, but I have forgotten my complex analysis.)

**cosh**: real $\to$ real. An approximation to a hyperbolic function.

**sinh**: real $\to$ real. An approximation to a hyperbolic function.
tanh: real→real. An approximation to a hyperbolic function.

index = text→nat. A signal to the implementation that the natural number will be used only as an
index to the indicated list.

int. The integers.

intchar: charint char → char. A one-to-one function with inverse charint .

key!. An input channel.

line! text. An input channel giving the same input as key except that the characters are gathered
into texts, each text extending from one return character to the next, not including the
return characters, and corrected according to the use of backspace characters.

mail. A CHANNEL, PERHAPS?

match: *all→*all→nat. 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. The maximum representable integer (machine dependant).

maxnat: nat. The maximum representable natural (machine dependant).

minint: int. The minimum representable integer (machine dependant).

mod: real → §(r: real → r>0) → real. mod a d is the remainder when a is divided by d .

(0 ≤ mod a d < d) ∧ (a = div a d × d + mod a d)

movie = [*pic].

nat. The natural numbers.

nil. The empty string.

null. The empty bunch.

numtext: com→text. A text representing the argument.

odd: int→bin.

ok. A program whose execution does nothing.

openlist: text. The names of the open dictionaries in the order they were opened.

path = text→*nat. A signal to the implementation that the string will be used only as an index to the
indicated list.

pi = 3.141592653589793 (approx). An approximation to the ratio of a circle's circumference to its
diameter.

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

pre: char→char. The predecessor function.

printer!. An output channel.

random. A dictionary containing the following three names.

init. A program with one real parameter. Its execution assigns a hidden variable to a value.

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

value: real→real→real. A reasonably uniform function of the hidden variable over the
interval between the arguments.

real. The real numbers.

realtext: real→text A textual representation of a real number. MAYBE erealtext and frealtext
return: char. The return or newline character.

round: real→int. r–0.5 ≤ round r < r+0.5

screen!. An output channel.

session: text. A text expression giving all keystrokes on channel key since the start of a session.

sign: real → (−1, 0, 1).

sort: *ord→*ord where ord = real, char, [*ord].


stop: wait (∞;∞;∞;∞;∞).
subst: \texttt{all} \rightarrow \texttt{all} \rightarrow \texttt{all}. subst \texttt{x y s} is a string formed from \texttt{s} by replacing all occurrences of \texttt{y} with \texttt{x}. Substitute \texttt{x} for \texttt{y} in \texttt{s}.

suc: char \rightarrow char. The successor function.

tab: char.
text = *char.
textcom: text \rightarrow com. If the argument represents a complex number, the result is the represented number.
textint: text \rightarrow int. If the argument represents an integer, the result is the represented number.
textreal: text \rightarrow real. If the argument represents a real number, the result is the represented number.
time!: An input channel that gives the time as a string of six numbers. For example, 1947; 9; 16; 14; 24; 30.095 is the time 1947 September 16 at 2:24 pm and 30.095 seconds.
timetext: (5\*nat; real) \rightarrow text. A readable form of the time. For example, timetext (1947; 9; 16; 14; 24; 30.095) = “1947 Sep 16 at 2:24 pm”

trig. A dictionary containing the following names. (The domains and ranges should probably include complex numbers, but I have forgotten my complex analysis.)

\texttt{arccos}: \$\langle r: \text{real} \rightarrow -1 \leq r \leq +1 \rangle \rightarrow \$\langle r: \text{real} \rightarrow 0 < r < \pi/2 \rangle$. An approximation to a trigonometric function.

\texttt{arcsin}: \$\langle r: \text{real} \rightarrow -1 \leq r \leq +1 \rangle \rightarrow \$\langle r: \text{real} \rightarrow 0 < r < \pi/2 \rangle$. An approximation to a trigonometric function.

\texttt{arctan}: real \rightarrow \$\langle r: \text{real} \rightarrow 0 < r < \pi/2 \rangle$. An approximation to a trigonometric function.

\texttt{cos}: real \rightarrow \$\langle r: \text{real} \rightarrow -1 \leq r \leq +1 \rangle$. An approximation to a trigonometric function.

\texttt{sin}: real \rightarrow \$\langle r: \text{real} \rightarrow -1 \leq r \leq +1 \rangle$. An approximation to a trigonometric function.

\texttt{tan}: (\$r: \text{real} \cdot \neg \exists i: \text{int} \cdot (r = (2 \times i + 1) \times \pi)) \rightarrow \text{real}$. An approximation to a trigonometric function.

trim: text \rightarrow text. A text formed from the argument by removing all leading and trailing space, tab, and return characters.

true: bin. screen! true prints true

wait. A program with one parameter of type \texttt{5*nat; real}. Its execution does nothing but take the length of time given by the argument. See \texttt{await} and \texttt{time}.

\textbf{Grammar LL(1/2)}

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 why I call it LL(1/2).
modifier _ identifier modifier
empty

phrase after newname : data
= data
:: phrase
!
== name
open name
equal

phrase after name := data
! data
? data
:: phrase
argument
data
comparand after comparand
comparand
element after element
element
item after item
term after term
term
factor after factor
factor
# factor
– factor
~ factor
+ factor
~ factor
√ factor
□ factor
* factor
primary factor after primary

primary
number
text
if data then data else data fi argument
result name : data do program od argument
{ data }
[ data ] argument
( data ) argument
〈 name : primary → data 〉 argument
name argument

argument
number argument
text argument
if data then data else data fi argument
result name : data do program od argument
{ data } argument
[ data ] argument
( data ) argument
〈 name : primary → data 〉 argument
identifier modifier argument
equal

after comparand := comparand after comparand
< comparand after comparand
> comparand after comparand
\[ \leq \text{comparand aftercomparand} \]
\[ \geq \text{comparand aftercomparand} \]
\[ + \text{comparand aftercomparand} \]
\[ \text{empty} \]
\[ \text{afterelement , aftercomma afterelement} \]
\[ \text{l element afterelement} \]
\[ \text{data} \llparenthesis \text{element} \rrparenthesis \text{afterelement} \]
\[ \text{empty} \]
\[ \text{aftercomma . . element} \]
\[ \text{element} \]
\[ \text{afteritem ; aftersemicolon afteritem} \]
\[ \text{‘ item afteritem} \]
\[ \text{empty} \]
\[ \text{aftersemicolon . . item} \]
\[ \text{item} \]
\[ \text{afterterm + term afterterm} \]
\[ \text{– term afterterm} \]
\[ + \text{term afterterm} \]
\[ \cup \text{term afterterm} \]
\[ \text{empty} \]
\[ \text{afterfactor } \times \text{factor afterfactor} \]
\[ / \text{factor afterfactor} \]
\[ \cap \text{factor afterfactor} \]
\[ \wedge \text{factor afterfactor} \]
\[ \lor \text{factor afterfactor} \]
\[ \Delta \text{factor afterfactor} \]
\[ \nabla \text{factor afterfactor} \]
\[ @ \text{factor afterfactor} \]
\[ \text{empty} \]
\[ \text{factoryafterprimary} \uparrow \text{factor} \]
\[ \downarrow \text{factor} \]
\[ \rightarrow \text{factor} \]
\[ * \text{factor} \]
\[ \text{argument} \]

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 name data comparand element item term.

**Grammar LR(1/2)**

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 is essentially “looking at” an input symbol. So I'll compromise and call it LR(1/2).

```
program                  phrase
program . phrase
program || phrase
phrase                new name : data
```
new name = data
new name :: phrase
new name !
new name == data
new name
old name
open name
new open name
close name
name ::= data
name ! data
name ? data
name !
name ?
name :: phrase
text ::= phrase
if data then program else program fi
for name : data do program od
do program od
procedure
(procedure ( program )
( name : primary → program )
procedure argument
name
data
data = comparand
data + comparand
data < comparand
data > comparand
data ≤ comparand
data ≥ comparand
comparand
comparand , element
comparand , . . element
comparand | element
comparand <| data >| element
element
element ; item
element ; . . item
element ‘ item
item
item + term
item – term
item * term
item \ term
term
term × factor
term / factor
term ∧ factor
term v factor
term $\Delta$ factor
term $\nabla$ factor
term $\cap$ factor
factor

+ factor
$-$ factor
$\#$ factor
$\sim$ factor
$\sim$ factor
$\sqrt{}$ factor
$\Box$ factor
* factor
primary * factor
primary $\rightarrow$ factor
primary $\uparrow$ factor
primary $\downarrow$ factor
primary

primary

primary argument
primary $\rightarrow$ argument
argument

number
text
[ data ]
{ data }
( data )
\langle name : primary $\rightarrow$ data \rangle
if data then data else data fi
result name : data do program od
name

name

identifier
ame _ identifier

Problems and Concerns

Do we need channel parameters?

Should there be interactive variables? The syntactic cost is one symbol and one production.
new name =: data

The following is not a semantic problem, but it is an implementation problem.
screen! $-3$ should print $-3$, and similarly
screen! 1/0 should print 1/0
screen! [0; 1; 2] 3 should print [0; 1; 2] 3
screen! $\langle r: \text{rat} \rightarrow 5 \rangle$ (1/0) should print 5
screen! 1/0 = 1/0 should print true
screen! [0; 1; 2] 3 = [0; 1; 2] 3 should print true

To execute a program stored on someone else's computer, I just invoke that remote program using its full address (computer address + program address within the computer). For efficiency, it might be
best to compile that remote program for my own computer and run it locally. The question is how to get that program to read from my local keyboard and write to my local screen. We could add

! data
? data
? √

with no channel name to mean the local screen and keyboard, but what about the local cursor and speakers? Should we treat channel names dynamically? Do channel parameters solve the problem?

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.

variable definition with initialization

new x: nat := 3

one-tailed if

if a=0 then x:= b fi

list item assignment

A 3:= 5

definition grouping

new x, y: int
old x, y
open this, that
new here, there!
(a, b: nat → a+b)
(a, b: nat → x:= a+b)

name and use data

1 + (fact:=: (n: nat → if n=0 then 1 else n×fact(n−1) fi)) 9 × 2

result r: nat
do new fact = (n: nat → if n=0 then 1 else n×fact(n−1) fi).

r:= 1 + fact 9 × 2  od