CSK SYSTEMS CORPORATION

VDMTools

VDM++ 言語マニュアル VICE編

ver.1.0 beta

How to contact CSK SYSTEMS CORPORATION:

http://www.csk.com/systems Web
@ VDM.SP@csk.com General information

VDM++ 言語マニュアル *VICE*編 *1.0 beta*
— Revised for VDMTools v8.2

目 次

1 導入

VDM++ は、技術分野 [FJ98] において特有の並列性、実時間をともなうオブジェクト指向システムを、記述することを意図した形式仕様記述言語である。この言語は VDM-SL [P. 96] を基にして、Smalltalk-80 や Java といった言語に現存するクラスやオブジェクトの概念を加えての拡張がなされてきた。この両者の結合により、オブジェクト指向形式仕様記述の発展が促されている。VICE は、「VDM++ In Constrained Environments」の略である。そして、この VDM の改良が適切なモデルとリアルタイム分散組込みシステムに使われる。 [?]

1.1 本書について

本書は VDM++の言語参照マニュアルである。VDM++言語構文の構成を文法法則を用いて定義している。各々の言語構造の意味はまず非形式な方法で説明され、次にいくつかの小さな例題が与えられる。「順読み」を想定するよりは「検索」利用を目的に記述されているため、チュートリアルではなくマニュアルである。読者には、オブジェクト指向プログラミング／デザインという概念に親しみ身近に感じられるようになられることを期待する。本書では Unicode 具象構文 (交換具象構文) を用いることとし、すべての予約語を特別なキーワード・フォントで示す。これは本書が、Unicode 記号を入力とする VDM++ Toolbox の言語マニュアルだからである。数学的な具象構文は、Toolbox を用いることで自動的に生成することができるので、更にみかけのよい構文をつくることが可能となる。

1.2 言語の歴史

VDM++は、1992 年以来現在に至るまでも未だ開発途上にある；その最初の記述については [Dür92] を参照。かつては AFRODITE[1] プロジェクトの一部として、飛躍的な発展をとげてきた。したがって、VDM++は AFRODITE プロジェクトの中での開発に基盤を置く。言語開発過程においては、数多くの大規模なケーススタディからのフィードバックおよび言語評価がなされてきている。その VDM++ 言語を支えるのが VDM++ Toolbox である。この Toolbox では、構文チェッカー、

[1] AFRODITE は欧州連合の支援のもとに行われた ESPRIT 計画に含まれる (EP6500).

静的意味チェッカー、インタープリタ[2]、C++コード生成、それに UML リンクの機能を持つ。一般的には ISO/VDM-SL は実行不可能な言語なので、インタープリタはこの言語の一部分をサポートしているに過ぎない。本書では特に、VDM-SL の意味とインタープリタにおいて用いられる意味との違いに焦点をあてる。そのため本書では、VDM++ Toolbox におけるインタープリタを引用する場合をすべて「インタープリタ」と記述する。

1.3 本書の構成

第 2 章では、本書に示された言語および関連する VDM++ Toolbox が、いかに VDM-SL 標準に準拠しているかを述べる。第 3 章では、構文構造の記述に用いられる BNF 記法を紹介する。VDM++ 表記法については、第 4 章から 第 16 章までで述べる。第 18 章では、ISO/VDM-SL と VDM++ との相違点をリストアップし、第 19 章では、VDM++ の静的意味について簡単に説明する。言語の全構文は 付録 A に、語彙の仕様は 付録 B に、演算子の優先順位は 付録 C に示す。付録 D では、数学構文と ASCII 具象構文の記号の違いをリスト (一覧表) に示す。標準ライブラリの詳細と使用法は、付録 E にて示す。最後には、本書中の全構文規則定義に対しての索引が与えられている。

2 準拠事項

標準規格である VDM-SL には、いくつかの準拠レベルを記載する準拠事項の節がある。最も低レベルでの準拠事項は構文一致である。VDM++ Toolbox では、標準のもの、例外は第 18 章にて記述される の構文記述に従った仕様記述を受け入れる。加えて、準拠条項に従えば排除されるべき多くの拡張記述 (第 18 章参照) についても受け入れる。

準拠事項レベル 1 では、恐らくの正しさに対する静的意味を扱う (第 19 章参照)。ここでは、恐らくは良形である標準記述を対象にし、他に多く存在するさまざまな記述は極力排除することとした[3]。

[2]加えて, 清書機能、デバッグ機能、テストカバレージサポートを提供するが、これらは基本構成要素である。

[3]例えば述語が存在する集合の理解において、標準記述では (恐らくは良形であることのチェックでは) 要素式に対する検査をまったく行わない。なぜなら、述語は false となる可能性がある (し

準拠事項レベル 2 およびこれ以降のレベル (最終レベル以外) では、絶対的な良形であることの静的意味チェックと、静的意味に加えられるいくつかのおこりうる拡張チェックについて扱う。絶対的に良形であることの検査機能は Toolbox が持っている。しかしながら、実際例においてはこれが最も価値あるものとは考えない。なぜなら「現実にある」例に対し、ほとんどすべての記述がこの検査をパスすることはないからである。

準拠最終レベルでは動的意味を扱う。ここで、標準の動的意味 (これは実行可能でない) からどのように逸脱しているかについては、添付書類を用いた詳細の提供が求められている。本書では、どのような構成要素が Toolbox にて翻訳されるか、ほんの少しの構成要素において逸脱するものが何であるかを説明し、この要求に事実上答える。このようにこの準拠レベルは、VDM++ Toolbox の存在で条件が満たされている。

まとめれば、 VDM++ はきわめて標準準拠に近いと言うことができるが、これを保証するに十分な時間は未だ費やされていない。

3 具象構文表記法

本書の中で、一部の言語構文については常に BNF 表記を用いる。使用される BNF 表記法には、以下に示すような特殊記号が用いられる:

たがって全式が空集合を表すことになる可能性がある) からである。読者はこの例を実際試すことにも興味をもつであろうと確信する。

,	連結記号
=	定義記号
|	定義分離記号 (選択枝)
[ ]	オプションの構文項目を囲む
{ }	0 回以上出現する構文項目を囲む
‘ ’	シングル引用リテラルは終端記号を囲むのに使用される
メタ識別子	非終端記号は小文字 (空白も含む) で記される
;	1 つの規則の終わりを表わす終了記号
( )	グループ化に用いられる、つまり “a, (b | c)” は “a, b | a, c” と等しい。
–	終端記号の集合からの減算を表す (つまり “character – (‘"’)” はダブル引用リテラルを除くすべての文字を表す。)

4 データ型定義

伝統的なプログラミング言語と同様に、VDM++ においてもデータ型を定義し適切な名称を与えることができる。例えば次のような等式が与えられたとする:

```
Amount = nat
```

ここでは “Amount(合計)” という名のデータ型を定義し、この型に属する値は自然数であると述べている (nat(自然数) は以下に記述される基本型の 1 つである)。VDM++ の型体系で全般に共通する 1 つは、今この点について述べることは重要だが、相等と不等とはどのような値間にも用いることができるということである。プログラミング言語においてはしばしば、演算対象が同じ型であることを要求される。VDM++ では合併型 (以下に示す) と呼ばれる構造があるので、これには当てはまらない。

この節では、データ型定義の構文について述べる。加えて、ある型に属する値はどのように構成され操作されうるのか (組込み演算子を用いて) について述べる。最初に基本データ型を示し、次に合成型へと進めよう。

4.1 基本データ型

以下にいくつかの基本型を提示する。その各々は次を含む:

- 構成の名称
- 構成の記号
- そのデータに属する特殊な値
- そのデータ型に属する値のための組込み演算子。
- 組込み演算子の意味定義。
- 組込み演算子の使用例[4]

組込み演算子の各々については、その意味定義の記述と共に、名称、記号、そして演算子の型が与えられる (ただし相等と不等の意味については、通常の意味に従うので、記述されていない。) 意味定義の記述において、識別子は例えば a, b, x, y 他 といったもので、対応する演算子型の定義で使用されるものを参照している。

基本型とは、言語により定義されていて、それ以上単純な値には分解することができない異なる値をもっている型とされる。主要な基本型として 5 つ：ブール型、数値型、文字型、トークン型、引用型 が挙げられる。以下にこの基本型について 1 つずつ説明していこう。

4.1.1 ブール型

一般的に VDM++ では、その中で計算が終了しなかったり結果を出せなかったりするかもしれないシステムを対象とすることも許されている。このような潜在的な未定義状態を取り扱うために、VDM++ では 3 値論理：値は「true(真)」、「false(偽)」、「bottom/undefined(未定義)」のいずれかであるとする、を取り入る。インタプリターの意味定義は、演算対象の順番に重きをおかない LPF (Logic of Partial Functions、部分関数の論理) の 3 値論理 ([Jon90] 参照) をもつものでは

[4] これらの例題中では、メタ記号 '≡' を用いて与えられた例題が何と同等であるかを示す。

ないという意味において、 VDM-SL のものとは異なる。それでも、論理積 and、論理和 or、それに含意演算子は、最初の演算対象のみで結果を決定するのに十分であるならば、次の演算対象をあえて評価しようとはしない、という条件つきの意味定義をもつ。ある意味で、インタプリターの論理の意味定義は 3 値であると、VDM-SL に関してはまだ考えることができるであろう。しかしながら、未定義値は無限大ループやランタイムエラーになる可能性がある。

名称: ブール

記号: bool

値: true, false

演算子: 下記の a と b は任意のブール式を表す:

演算子	名称	型
not b	否定	bool → bool
a and b	論理積	bool * bool → bool
a or b	論理和	bool * bool → bool
a => b	含意	bool * bool → bool
a <=> b	同値	bool * bool → bool
a = b	相等	bool * bool → bool
a <> b	不等	bool * bool → bool

演算子の意味定義: 意味定義では、ブール値を扱う場合の <=> と = は等しい。and、 or、および =>においては条件つきの意味定義がある。⊥ によって定義されていない項目 (たとえば定義域外のキーをもつ写像に適用される) を表示しよう。ブール演算子に対する真理値表は次のとおり[5]:

[5]標準 VDM-SL ではこれらの真理値表は (=>以外は) 対称性をもつことに注目しよう。

否定 not b

b	true	false	$\perp$
not b	false	true	$\perp$

論理積 a and b

$a \backslash b$	true	false	$\perp$
true	true	false	$\perp$
false	false	false	false
$\perp$	$\perp$	$\perp$	$\perp$

論理和 a or b

$a \backslash b$	true	false	$\perp$
true	true	true	true
false	true	false	$\perp$
$\perp$	$\perp$	$\perp$	$\perp$

含意 a => b

$a \backslash b$	true	false	$\perp$
true	true	false	$\perp$
false	true	true	true
$\perp$	$\perp$	$\perp$	$\perp$

同値 a <=> b

$a \backslash b$	true	false	$\perp$
true	true	false	$\perp$
false	false	true	$\perp$
$\perp$	$\perp$	$\perp$	$\perp$

例題: a = true で b = false と仮定すると次のとおり:

not a	≡	false
a and b	≡	false
b and ⊥	≡	false
a or b	≡	true
a or ⊥	≡	true
a => b	≡	false
b => b	≡	true
b => ⊥	≡	true
a <=> b	≡	false
a = b	≡	false
a <> b	≡	true
⊥ or not ⊥	≡	⊥
(b and ⊥) or (⊥ and false)	≡	⊥

4.1.2 数値型

数値型には5つの基本型：正の自然数、自然数、整数、有理数、そして実数がある。3つを除きどの数値演算子も、演算対象として5つの型の混在を許す。例外である3つとは、整数除算、法算、剰余算、である。

5つの数値型は階層構造をなし、実数 (real) が最も一般的な型で有理数 (rat)[6]、整数 (int)、自然数 (nat)、正の自然数 (nat1) と続く。

型	値
nat1	1, 2, 3, ...
nat	0, 1, 2, ...
int	..., -2, -1, 0, 1, ...
real	..., -12.78356, ..., 0, ..., 3, ..., 1726.34, ...

この表より、int ならばどのような数でも自動的に real であるが、nat であるとは限らないということがわかる。言い換えると、正の自然数は自然数の一部であり、その自然数は整数の、その整数は有理数の、有理数は最終的には実数の一部である、と表現することができる。次の表でいくつかの数が属する型を示す：

[6] VDM++ Toolbox の見地からすれば 実数 (real) と 有理数 (rat) は違いがない。コンピューター上では有理数しか表現できないからである。

数	型
3	real, rat, int, nat, nat1
3.0	real, rat, int, nat, nat1
0	real, rat, int, nat
-1	real, rat, int
3.1415	real, rat

すべての数が必然的に real 型 (そして rat 型) であることに注意。

名称: 実数, 有理数, 整数, 自然数、そして 正の自然数

記号: real, rat, int, nat, nat1

値: ..., -3.89, ..., -2, ..., 0, ..., 4, ..., 1074.345, ...

演算子: 以下における x と y は数式を表すとする。これらの型について仮定はなされない。

演算子	名称	型
-x	負符号	real → real
abs x	絶対値	real → real
floor x	底値	real → int
x + y	加算	real * real → real
x - y	減算	real * real → real
x * y	乗算	real * real → real
x / y	除算	real * real → real
x div y	整数除算	int * int → int
x rem y	剰余算	int * int → int
x mod y	法算	int * int → int
x**y	べき算	real * real → real
x < y	より小さい	real * real → bool
x > y	より大きい	real * real → bool
x <= y	より小さいか等しい	real * real → bool
x >= y	より大きいか等しい	real * real → bool
x = y	相等	real * real → bool
x <> y	不等	real * real → bool

演算対象として書かれた型は、許される限りでの最も広範な型である。例えば負符号は5つのすべての型 (nat1, nat, int rat そして real) を演算対象と

する、ことを示している。

演算子の意味: 演算子であるマイナス符号、総和、差、積、商、小さい、大きい、等しいか小さい、等しいか大きい、相等関係、不等関係はこのような演算の通常の意味をもつ。

演算子名称	意味記述
底値	x と等しいかより小さい整数のうちで最大のもの
絶対値	x の絶対値、つまり x >= 0 ならば x そのままで x < 0 ならば -x となる
冪	x を y 回乗じたもの

整数商、剰余、そして法　が負の数にどのように作用するかについては、しばしば混乱がおきる。事実 -14 div 3 に対して有効な答えが 2 つある: Toolbox においてと同様-4 (the intuitive) となるか、たとえば Standard ML [Pau91] においてと同様に-5 となるかである。したがってこれらの演算については詳細に説明しておくべきであろう。

整数除算は floor と実数除算を用いて定義される:

```
x/y <  0:   x div y = -floor(abs(-x/y))
x/y >= 0:   x div y =  floor(abs(x/y))
```

右辺の floor と abs の順により違いが生じ、その順を交換することで上記の例題は-5 となる。これは floor は常により小さい（か等しい）整数に従うからである、たとえば floor（14/3）は 4 である一方 floor（-14/3）は -5 である。

剰余 x rem y と　法 x mod y は、x と y の符号が同じであれば同じ値となるが、そうでない場合は異なる値となり、 rem は x の符号を mod は y の符号をとる。剰余と法の公式は次のとおり:

```
x rem y = x - y * (x div y)
x mod y = x - y * floor(x/y)
```

そのため, -14 rem 3 は -2 に等しく、 -14 mod 3 は 1 に等しい。実数軸をたどり、 -14 から進め 3 づつジャンプすることで、これらの結果を確認することができる。剰余はたどった負の数の最後の値であるが、それは x にあたる最初の引数が負であるからであり、一方の法はたどった正の数の最初の値であるが、それは y にあたる 2 番目の引数が正であるからである。

例題: a = 7, b = 3.5, c = 3.1415, d = -3, e = 2 とすると:

- a	≡	-7
abs a	≡	7
abs d	≡	3
floor a <= a	≡	true
a + d	≡	4
a * b	≡	24.5
a / b	≡	2
a div e	≡	3
a div d	≡	-2
a mod e	≡	1
a mod d	≡	-2
-a mod d	≡	-1
a rem e	≡	1
a rem d	≡	1
-a rem d	≡	-1
3**2 + 4**2 = 5**2	≡	true
b < c	≡	false
b > c	≡	true
a <= d	≡	false
b >= e	≡	true
a = e	≡	false
a = 7.0	≡	true
c <> d	≡	true
abs c < 0	≡	false
(a div e) * e	≡	6

4.1.3 文字型

文字型は、VDM 文字集合 (190 ページの表 12 を参照) 中の単一の文字すべてを含む。

名称: 文字

記号: char

値: 'a', 'b', ..., '1', '2', ... '+', '-' ...

演算子: 次の c1 と c2 は任意の文字を表す:

演算子	名称	型
c1 = c2	相等	char * char → bool
c1 <> c2	不等	char * char → bool

例題:

```
'a' = 'b'    ≡  false
'1' = 'c'    ≡  false
'd' <> '7'   ≡  true
'e' = 'e'    ≡  true
```

4.1.4 引用型

引用型は、パスカルのようなプログラミング言語においては列挙型に相当する。しかしながら VDM++ においては、中括弧の中に様々な引用リテラルを書く代わりに引用型というシングル引用リテラルからなるものを用いて、それらを合併型の一部をなすものとする。

名称: 引用

記号: たとえば <QuoteLit>

値: <RED>, <CAR>, <QuoteLit>, ...

演算子: 以下の q と r が、列挙型 T に属する任意の引用値を表していると仮定すると:

演算子	名称	型
q = r	相等	$T * T \to \text{bool}$
q <> r	不等	$T * T \to \text{bool}$

例題: T を次に定義された型とする:

```
T = <France> | <Denmark> | <SouthAfrica> | <SaudiArabia>
```

ここで a = <France>であるならば次のとおり:

```
<France> = <Denmark>                 ≡  false
<SaudiArabia> <> <SouthAfrica>       ≡  true
a <> <France>                        ≡  false
```

4.1.5 トークン型

トークン型は、トークンと呼ばれる異なる値の可算無限集合からなる。トークンに対して実行される操作は、相等と不等のみである。VDM++, におけるトークンは、mk_token を用いて任意の式を囲む記述ができるのにもかかわらず、単独に表現することはできない。これが、トークン型を含む仕様のテストを可能にする方法である。しかしながら VDM-SL 標準に似せるためには、これらのトークン値はどんなパターンマッチングによっても分解できず、相等または不等の比較以外どのような演算にも用いることはできない。

名称: トークン

記号: token

値: mk_token(5), mk_token({9, 3}), mk_token([true, {}]), ...

演算子: 以下の s と t は任意のトークン値を表す:

演算子	名称	型
s = t	相等	token * token → bool
s <> t	不等	token * token → bool

例題: 次においてたとえば s = mk_token(6) 、 t = mk_token(1) とすると:

```
s = t                ≡  false
s <> t               ≡  true
s = mk_token(6)      ≡  true
```

4.2 合成型

以下に合成型について記述する。各々は次を含む：

- 合成型定義の構文
- 構成要素をどのように用いるか示す等式
- この型に属する値をどのように構成するか示す例題ほとんどの場合に、基本構成子式の構文が与えられている前の節への参照が示される。
- この型に属する値に対する演算子 [7]
- 演算子の意味定義
- 演算子の使用例

演算子の各々に対し、名称、記号、演算子の型がその意味定義と共に与えられる (ただし相等と不等については、通常の意味に従うとして除かれる)。意味定義記述において、識別子はたとえば m, m1, s, s1 他 というような、対応する演算子型定義で用いられたものを参照する。

4.2.1 集合型

集合とは、値を順番をつけずに集めたものであり、それらはすべて同じ型のもので[8]、全体は1つとして扱われる。VDM++ におけるすべての集合は有限である、なぜならばもともと有限個の要素しか含められないからだ。集合型の要素は任意の合成型でありうるし、例えば集合自身の集合であってもよい。

[7] これらの演算子は、第 7.3 節で全演算子が与えられるなかの単項式か 2 項式に用いられている。

[8] ただし合併型を用いれば、2 つの値に共通な型を見つけ出すのは常に可能であることに注意 (第 4.2.6 節参照)。

以下の記述には次の合意を用いる：A は任意の型、 S は集合型、 s、 s1、 s2 は集合値、 ss は集合値の集合、 e、 e1、 e2、 en は集合の要素、 bd1, bd2、 ...、 bdm は集合または型を示す識別子を束ねたもの、そして P は論理述語である。

構文:

```
型 = 集合型
   | ... ;

集合型 = 'set of', 型 ;
```

等式: `S = set of A`

構成子:

集合列挙: `{e1, e2, ..., en}` は列挙された要素の集合を構成する。空集合は {} と表記される。

集合内包: `{e | bd1, bd2, ..., bdm & P}` は、述語 P が true となるすべての束縛について式 e を評価することにより集合を定義する。束縛は集合束縛と型束縛のどちらかとなる[9]。集合束縛 bdn は pat1, ..., patp in set s という形式をもつが、ここでの pati はパターン (通常は単純な識別子である) であり、 s は 1 つの式で構成される集合である。型束縛も、in set がコロンに換わり s が型式となるという意味において、同様のものである。

すべての集合式に対する構文と意味定義は、第 7.7 節に与えられる

演算子:

[9]型束縛は実行可能ではないので一般的にはインタープリタで実行されない (これについては第 9 節を参照)。

演算子	名称	型
e in set s1	帰属	$A *$ set of $A \to$ bool
e not in set s1	非帰属	$A *$ set of $A \to$ bool
s1 union s2	合併	set of $A *$ set of $A \to$ set of A
s1 inter s2	共通部分	set of $A *$ set of $A \to$ set of A
s1 \ s2	差	set of $A *$ set of $A \to$ set of A
s1 subset s2	包含	set of $A *$ set of $A \to$ bool
s1 psubset s2	真包含	set of $A *$ set of $A \to$ bool
s1 = s2	相等	set of $A *$ set of $A \to$ bool
s1 <> s2	不等	set of $A *$ set of $A \to$ bool
card s1	濃度	set of $A \to$ nat
dunion ss	分配的合併	set of set of $A \to$ set of A
dinter ss	分配的共通部分	set of set of $A \to$ set of A
power s1	有限べき集合	set of $A \to$ set of set of A

A，set of A 型と set of set of A 型は単に型の構造を表すだけではないことに注意。たとえば、任意の集合 s1 と s2 の合併を行った場合、結果の集合の型は 2 つの集合型の合併型とすることができる。これについての例は第 4.2.6 節に与えられる。

演算子の意味:

演算子名称	意味記述
帰属関係	e が集合 s1 の要素であるかどうか検査する
非帰属関係	e が集合 s1 の要素でないことを検査する
合併	集合 s1 と s2 の合併、つまり s1 と s2 の両方の要素をすべて含む集合である。
共通部分	集合 s1 と s2 の共通部分、つまり s1 と s2 の両方にある要素を含む集合である。
差	s2 に含まれていない s1 の要素をすべて含む集合。s2 は s1 の部分集合である必要はない。
包含関係	s1 が s2 の部分集合であるかどうかを検査する、つまり s1 のすべての要素が s2 の要素であるかどうかである。どの集合もそれ自身の部分集合であることには注意。
真包含関係	s1 が s2 の真部分集合であることを検査する、つまり 部分集合でありしかも s2\s1 が空集合でないことである。

演算子名称	意味記述
濃度	s1 の要素の数。
分配的合併	結果の集合は ss のすべての要素 (それら自身が集合である) の合併である、つまり ss のすべての要素／集合のすべての要素を含む。
分配的共通部分	結果の集合はすべての要素の共通部分であり、つまり ss のすべての要素／集合の中の要素を含むということ。 ss は空集合であってはならない。
有限べき集合	s1 のべき集合である、つまり s1 のすべての部分集合の集合である。

例題: s1 = {<France>,<Denmark>,<SouthAfrica>,<SaudiArabia>}、s2 = {2, 4, 6, 8, 11} 、 s3 = {} であるときには以下のとおり:

```
<England> in set s1                          ≡ false
10 not in set s2                             ≡ true
s2 union s3                                  ≡ {2, 4, 6, 8, 11}
s1 inter s3                                  ≡ {}
(s2 \ {2,4,8,10}) union {2,4,8,10} = s2      ≡ false
s1 subset s3                                 ≡ false
s3 subset s1                                 ≡ true
s2 psubset s2                                ≡ false
s2 <> s2 union {2, 4}                        ≡ false
card s2 union {2, 4}                         ≡ 5
dunion {s2, {2,4}, {4,5,6}, {0,12}}          ≡ {0,2,4,5,6,8,11,12}
dinter {s2, {2,4}, {4,5,6}}                  ≡ {4}
dunion power {2,4}                           ≡ {2,4}
dinter power {2,4}                           ≡ {}
```

4.2.2 列型

列値とは ある型の要素を順にならべた集まりで 1, 2, ..., n によって索引づけられるもの；ここでは n がこの列の長さとなる。列型とはある型の要素を有限個連続させた型であり、空列を含む場合 (空列を含む列型) と含まない場合 (空列を含まない列型) のいずれかとなる。列型の要素には任意の混在が許されている; た

とえばそれらが連続したものであればよいわけである。

以下はこの合意が用いられる: A は任意の型であり、L は列型であり、 S は集合型であり、 l, l1, l2 は列値であり、 ll は列値の列である。e1, e2 および en はこれらの列の要素、 i は自然数、 P は述語、 e は任意の式である。

構文:

型 = 列型
| ... ;

列型 = 空列を含む列型
| 空列を含まない列型 ;

空列を含む列型 = 'seq of', 型 ;

空列を含まない列型 = 'seq1 of', 型 ;

等式: `L = seq of A` または `L = seq1 of A`

構成子:

列列挙: `[e1, e2,..., en]` は、列挙された要素によって列を構成する。空列は `[]` と表現する。テキストリテラルは文字の列挙の簡約記法である (たとえば `"csk" = ['c','s','k']`)

列内包: `[e | id in set S & P]` は、述語 P が true となるようなすべての束縛に対して式 e を評価することで列を構成する。式 e は識別子 id を用いる。S は数の集合であり、 id は通常の順で数とマッチする (最小の数を最初として)

すべての列式の構文と意味定義については、第 7.8 節で述べる。

演算子:

演算子	名称	型
hd l	先頭	seq1 of $A \to A$
tl l	尾部	seq1 of $A \to$ seq of A
len l	長さ	seq of $A \to$ nat
elems l	要素集合	seq of $A \to$ set of A
inds l	索引	seq of $A \to$ set of nat1
l1 ^ l2	連結	(seq of A) $*$ (seq of A) $\to$ seq of A
conc ll	分配的連結	seq of seq of $A \to$ seq of A
l ++ m	列修正	seq of $A *$ map nat1 to $A \to$ seq of A
l(i)	列適用	seq of $A *$ nat1 $\to A$
l1 = l2	相等	(seq of A) $*$ (seq of A) $\to$ bool
l1 <> l2	不等	(seq of A) $*$ (seq of A) $\to$ bool

型 A は任意の型であって、連結や分配的連結の演算子に対する演算対象は、同じ型 (A) である必要はない。結果列の型は、複数の演算対象の型の合併型となる。第 4.2.6 節に例題が与えられている。

演算子の意味定義:

演算子名称	意味記述
先頭	l の最初の要素。 l は空列であってはならない。
尾部	l から最初の要素を取り除いた部分列。 l は空列であってはならない。
長さ	l の長さ。
要素集合	l の要素すべてを含む集合。
添字集合	l の索引の集合、つまり集合 {1,...,len l}。
連結	l1 と l2 の連結、つまり順に、 l1 の列要素のあとに l2 の列要素を続けた列。
分配的連結	l1 の列要素 (これら自体が列である) が連結された列: 最初と第 2 の列要素を連結し、次に第 3 の列要素を連結し、等々。
列修正	列索引が m の定義域にある l の列要素は、その索引が写像された先の値域値に修正される。 dom m は索引 l の部分集合でなければならない。
列適用	l からの索引の要素。 i は l の列索引になければならない。

例題: l1 = [3,1,4,1,5,9,2], l2 = [2,7,1,8],
l3 = [<England>, <Rumania>, <Colombia>, <Tunisia>] とすると以下のとおり：

len l1	≡	7
hd (l1^l2)	≡	3
tl (l1^l2)	≡	[1,4,1,5,9,2,2,7,1,8]
l3(len l3)	≡	<Tunisia>
"England"(2)	≡	'n'
conc [l1,l2] = l1^l2	≡	true
conc [l1,l1,l2] = l1^l2	≡	false
elems l3	≡	{ <England>, <Rumania>, <Colombia>,<Tunisia>}
(elems l1) inter (elems l2)	≡	{1,2}
inds l1	≡	{1,2,3,4,5,6,7}
(inds l1) inter (inds l2)	≡	{1,2,3,4}
l3 ++ {2 |-> <Germany>,4 |-> <Nigeria>}	≡	[<England>, <Germany>, <Colombia>, <Nigeria>]

4.2.3 写像型

A 型から B 型への写像型とは、 A (または A の部分集合) の要素各々を B の 1 つの要素と結合する型のことである。写像の値とは、この 2 つの要素の組を順不同で集めたものと考えることができる。各々の組の最初の要素をキーと呼ぶが、これは各組で最初の要素を用いて 2 番目の要素 (情報部分と呼ばれる) を得ることができるからである。よって 1 つの写像におけるキー要素は、すべて異なるものでなければならない。すべてのキー要素の集合をこの写像の定義域と呼び、一方すべての情報値の集合を値域と呼ぶ。VDM++ におけるすべての写像とは有限のものである。写像型の定義域と値域の要素には任意の合成が許されていて、たとえば要素を写像とすることもできる。

特別な写像としては 1 対 1 写像がある。1 対 1 写像とは、値域の要素で 2 つ以上の定義域の要素と結合するものはない写像のことである。この 1 対 1 写像では、写像を逆にすることが可能である。

以下では次のとおりに用いる: m, m1、および m2 は、任意の A 型からもう 1 つの任意の B 型への写像を表し、ms は写像値の集合であり。a, a1, a2、および an は A

から取り出した要素である一方、 b, b1, b2 および bn は B から取り出した要素である。P は論理述語である。e1、e2 は任意の式であり、 s は任意の集合である。

構文:

```
型 = 写像型
   | ... ;

写像型 = 一般写像型
       | 1 対 1 写像型 ;

一般写像型 = 'map', 型, 'to', 型 ;

1 対 1 写像型 = 'inmap', 型, 'to', 型 ;
```

等式: `M = map A to B` または `M = inmap A to B`

構成子:

写像列挙: {a1 |-> b1, a2 |-> b2, ..., an |-> bn} は、列挙された写からなる写像を構成する。空写像は {|->} と表す。

写像内包: {ed |-> er | bd1, ..., bdn & P} は、述語 P が true と判断するすべてのありうる束縛上で、式 ed と er を評価することによって写像を構成する。

すべての写像式の構文と意味定義については、第 7.9 節で述べる。

演算子:

演算子	名称	型
dom m	定義域	(map A to B) $\rightarrow$ set of A
rng m	値域	(map A to B) $\rightarrow$ set of B
m1 munion m2	併合	(map A to B) $*$ (map A to B) $\rightarrow$ map A to B
m1 ++ m2	上書	(map A to B) $*$ (map A to B) $\rightarrow$ map A to B
merge ms	分配的併合	set of (map A to B) $\rightarrow$ map A to B
s <: m	定義域限定	(set of A) $*$ (map A to B) $\rightarrow$ map A to B
s <-: m	定義域削減	(set of A) $*$ (map A to B) $\rightarrow$ map A to B
m :> s	値域限定	(map A to B) $*$ (set of B) $\rightarrow$ map A to B
m :-> s	値域削減	(map A to B) $*$ (set of B) $\rightarrow$ map A to B
m(d)	写像適用	(map A to B) $* A \rightarrow B$
m1 comp m2	写像合成	(map B to C) $*$ (map A to B) $\rightarrow$ map A to C
m ** n	写像反復	(map A to A) $*$ nat $\rightarrow$ map A to A
m1 = m2	相等	(map A to B) $*$ (map A to B) $\rightarrow$ bool
m1 <> m2	不等	(map A to B) $*$ (map A to B) $\rightarrow$ bool
inverse m	逆写像	inmap A to $B \rightarrow$ inmap B to A

演算子の意味定義: ２つの写像 m1 と m2 は、dom m1 と dom m2 に共通の要素が両写像により同じ値に写像されるならば、両立している。

演算子名称	意味記述
定義域	m の定義域 (キーの集合)。
値域	m の値域 (情報値の集合)。
併合	m1 と m2 が結合した写像で、結果の写像は m1 と同様に dom m1 の要素に、 また m2 と同様に dom m2 の要素に、写像を行う。２つの写像は両立していなければならない。
上書	m1 に m2 を上書または併合する、つまり m1 と m2 は必ずしも両立する必要はないということを除けば、併合と似ている。共通の要素はいずれも m2 によるものとして写像される (したがって m2 は m1 を上書する)。
分配的併合	ms に含まれるすべての写像を併合することにより構成される写像。 ms に含まれる写像は両立していなければならない。

演算子名称	意味記述
定義域限定	m の要素のうちでキーが s に含まれるもの、から構成される写像をつくりだす。s は dom m の部分集合である必要はない。
値域限定	m の要素のうちで情報値が s に含まれるもの、から構成される写像をつくりだす。 s は rng m の部分集合である必要はない。
写像の適用	キーが d である写像の情報値。 d は m の定義域に含まれていなければならない。
写像の合成	m2 の要素に m1 の要素を合成してつくった写像。結果は m2 と同じ定義域をもった 1 つの写像である。あるキーに対応する情報値は、最初に m2 をキーに適用しその後 m1 をその結果に適用することによって見つけられるものである。rng m2 は dom m1 の部分集合でなければならない。
写像の反復	m からそれ自体を n 回繰り返すことで構成された写像。 n = 0 は dom m の各々の要素がそれ自体への写像である同一写像； n = 1 は m 自体である。 n > 1 に対して、 m の値域は dom m の集合でなければならない。
逆写像	m の逆写像。 m は 1 対 1 写像でなければならない。

例題: 次を仮定すると

```
m1 = { <France> |-> 9, <Denmark> |-> 4,
       <SouthAfrica> |-> 2, <SaudiArabia> |-> 1},
m2 = { 1 |-> 2, 2 |-> 3, 3 |-> 4, 4 |-> 1 },
Europe = { <France>, <England>, <Denmark>, <Spain> }
```

以下のとおり：

```
dom m1  ≡ {<France>, <Denmark>,
           <SouthAfrica>,
           <SaudiArabia>}

rng m1  ≡ {1,2,4,9}
```

```
m1 munion {<England> |-> 3}          ≡  {<France> |-> 9,
                                         <Denmark> |-> 4,
                                         <England> |-> 3,
                                         <SaudiArabia> |-> 1,
                                         <SouthAfrica> |-> 2}

m1 ++ {<France> |-> 8,               ≡  {<France> |-> 8,
       <England> |-> 4}                  <Denmark> |-> 4,
                                         <SouthAfrica> |-> 2,
                                         <SaudiArabia> |-> 1,
                                         <England> |-> 4}

merge{ {<France> |-> 9,              ≡  {<France> |-> 9,
        <Spain> |-> 4}                   <England> |-> 3,
       {<France> |-> 9,                  <Spain> |-> 4,
        <England> |-> 3,                 <UnitedStates> |-> 1}
        <UnitedStates> |-> 1}}


Europe <:  m1                        ≡  {<France> |-> 9,
                                         <Denmark> |-> 4}

Europe <-:  m1                       ≡  {<SouthAfrica> |-> 2,
                                         <SaudiArabia> |-> 1}

m1 :> {2,...,10}                     ≡  {<France> |-> 9,
                                         <Denmark> |-> 4,
                                         <SouthAfrica> |-> 2}

m1 :-> {2,...,10}                    ≡  {<SaudiArabia> |-> 1}

m1 comp ({"France" |-> <France>})    ≡  {"France" |-> 9}

m2 ** 3                              ≡  {1 |-> 4, 2 |-> 1,
                                         3 |-> 2, 4 |-> 3 }
```

```
inverse m2                    ≡ {2 |-> 1, 3 |-> 2,
                                 4 |-> 3, 1 |-> 4 }

m2 comp (inverse m2)          ≡ {1 |-> 1, 2 |-> 2,
                                 3 |-> 3, 4 |-> 4 }
```

4.2.4 組型

組型の値を組と呼ぶ。組とは固定長のリストであり、組の i 番目の要素は組型の i 番目の要素に属さなければならない。

構文: 型 = 組型
| ... ;

組型 = 型, '*', 型, { '*', 型 } ;

組型は少なくとも 2 つの部分型から構成される。

等式： `T = A1 * A2 * ... * An`

構成子： 組構成子： `mk_(a1, a2, ..., an)`

組構成子についての構文と意味定義は第 7.10 節で述べられる。

演算子:

演算子	名称	型
`t.#n`	選択	$T * \mathsf{nat} \to Ti$
`t1 = t2`	相等	$T * T \to \mathsf{bool}$
`t1 <> t2`	不等	$T * T \to \mathsf{bool}$

組に対して有効な演算子は、構成要素選択、相等、不等、のみである。組構成要素は、選択演算子を用いたり組パターンとマッチングさせることで、アクセスすることもできる。組選択演算子についての意味定義の詳細および使用例は、第 7.12 節に述べる。

例題: `a = mk_(1, 4, 8), b = mk_(2, 4, 8)` とすると以下のとおり:

```
a = b          ≡ false
a <> b         ≡ true
a = mk_(2,4)   ≡ false
```

4.2.5 レコード型

レコード型は、プログラミング言語においての構造体に相当する。したがってこの型の要素は、前述の組型の節で述べられた組にいくぶんか似ている。レコード型と組型の違いは、レコードの異なる構成要素は相応の選択関数を用いることで、直接選択することができることである。さらに加えて、レコードは操作するとき用いられるべき識別子によってタグ付けされる。一般的な使い方として、タグを与えるためにはただ 1 つの項目からなるレコードも定義される。組とのもうひとつの違いとなるが、組は少なくとも 2 つの実体をもつ必要があるが、レコードは空でもよい。

VDM++, is_ は名称に対する予約接頭辞であって *is* 式の中で使用される。これは、あるレコード値がどのレコード型に属するのか決定するために用いられる、組込演算子である。しばしば合併型の部分型同士を区別することに用いられるため、更なる説明が第 4.2.6 節になされている。is_演算子は、レコード型を決定するのに加え、ある値が基本型のひとつであるかどうかの決定も行うことができる。

以下では次の約束に従う： `A` はレコード型、 `A1, ..., Am` は任意の型、 `r, r1, r2` はレコード値、 `i1, ..., im` はレコード値 `r` からの選択子、 `e1, ..., em` は任意の式である。

構文:

型 = レコード型
| ... ;

レコード型 = 'compose', 識別子, 'of', 項目リスト, 'end' ;

項目リスト = { 項目 } ;

項目 = [識別子, ':'], 型
| [識別子, ':-'], 型 ;

または省略型表記法で

レコード型 = 識別子, '::', 項目リスト ;

この識別子が表すものは型名かタグ名である。

等式:

```
A :: selfirst : A1
     selsec   : A2
```

または

```
A :: selfirst :  A1
     selsec   :- A2
```

または

```
A :: A1 A2
```

2 番目の表記では、 比較対象外 項目 が第 2 項 selsec に対し用いられる。この負符号は、等号演算子を使ってレコード比較を行うときにこの項が無視されることを指定している。最後の表記法では A の項目はひとつひとつに名称が付けられていないため、パターンマッチングによってのみ (組についてそうだったように) アクセスを行うことができる。

省略型表記である :: は前の 2 例でも使われ、タグ名が型名と等しいというものだが、この表記法は最もよく用いられている。より一般的である compose 表記法は、次のようにレコード型がそれより複雑な型の構成要素として直接記述されなければならない場合に、典型的に用いられる:

```
T = map S to compose A of A1 A2 end
```

しかしながら、レコード型は型定義においてのみ用いることができるもので、例えば関数や操作に対するシグネチャにおいてではないことは明記しておくべきであろう。

レコード型は、合併型定義における代案 (4.2.6 を参照) として、典型的に用いられる:

```
MasterA = A | B | ...
```

ここで A と B は、自身がレコード型として定義されている。この状態で、is_ 前置詞を代案と区別するために用いることができる。

構成子: レコード構成子: mk_A(a, b) において、 a は型 A1 に属し b は型 A2 に属す。

すべてのレコード式に対する構文と意味定義は第 7.11 節で与えられる。

演算子:

演算子	名称	型
r.i	項目選択	$A * Id \to Ai$
r1 = r2	相等	$A * A \to$ bool
r1 <> r2	不等	$A * A \to$ bool
is_A(r1)	Ｉｓ	$Id * MasterA \to$ bool

演算子の意味定義:

演算子名称	意味記述
項目選択	レコード値 r の中で項目名が i である項目の値。r は i という名の項目をもっていなければならない。

例題: Score は以下のように定義される

```
Score :: team : Team
         won : nat
         drawn : nat
         lost : nat
         points : nat;
Team = <Brazil> | <France> | ...
```

さらに次の通りとする

```
sc1 = mk_Score (<France>, 3, 0, 0, 9),
sc2 = mk_Score (<Denmark>, 1, 1, 1, 4),
sc3 = mk_Score (<SouthAfrica>, 0, 2, 1, 2) そして
sc4 = mk_Score (<SaudiArabia>, 0, 1, 2, 1)
```

このとき

```
sc1.team                    ≡  <France>
sc4.points                  ≡  1
sc2.points > sc3.points     ≡  true
is_Score(sc4)               ≡  true
is_bool(sc3)                ≡  false
is_int(sc1.won)             ≡  true
sc4 = sc1                   ≡  false
sc4 <> sc2                  ≡  true
```

':' の代わりに ':-' を用いて記述する比較対象外項目は、たとえばプログラム言語の抽象構文における低水準モデルにおいて役立つことがある。例としては、識別子の一意性に影響を与えることなく、それらの識別子の型に位置情報項目を加えたい場合などである。

```
Id :: name :  seq of char
      pos  :- nat
```

この効果は pos 項が相等比較において無視されることにあり、たとえば次の例は true と評価されるであろう：

```
mk_Id("x",7) = mk_Id("x",9)
```

特にこのことは、以下の形の写像の典型的な環境において検索を行う場合に役に立つはずである:

```
Env = map Id to Val
```

このような写像は指定の識別子に対し最大 1 つの索引を含み、写像検索は pos 項目から独立したものとなる。

そのうえ、比較対象外項目は集合式に影響を与える。たとえば、

```
{mk_Id("x",7),mk_Id("y",8),mk_Id("x",9)}
```

は次と等しくなる

```
{mk_Id("x",?),mk_Id("y",8)}
```

ここにおける疑問符は 7 から 9 までを表している。

最後に比較対象外項目に対する有効なパターンとしては、don't care あるいは識別子パターンに限定されていることには注意しよう。比較対象外項目は 2 つの値を比較するときに無視されるものであり、それ以上複雑なパターンを用いることに対しては意味をなさないからである。

4.2.6 合併型と選択型

合併型は集合論理における和に相当する、つまり合併型として定義される型はその合併型の構成要素各々からすべての要素を含むことになる。合併型の中で互いに素であるとはいえない複数の型を用いることは、あまりよくない使用法だが可能ではある。しかし通常は、属する型として可能な複数の型から 1 つを考える場合には合併型が用いられる。合併型を構成する型としてしばしばレコード型がある。is_演算子を用いることで、合併型のある値がこういった型のいずれに属するものであるのかを決定することが可能である。

選択型 [T] とは合併型 T | nil に対してのいわゆる省略であり、この nil は値が存在しないことを表記するために用いられるものである。ただし集合 {nil} をひとつの型として用いることはできないので、nil を含む型のみが選択型となりうる。

構文:

型 = 合併型
| 選択型
| ... ;

合併型 = 型, '|', 型, { '|', 型 } ;

選択型 = '[', 型, ']' ;

等式: `B = A1 | A2 | ... | An`

構成子: なし

演算子:

演算子	名称	型
`t1 = t2`	相等	$A * A \to$ bool
`t1 <> t2`	不等	$A * A \to$ bool

例題: この例題中で Const, Var, Infix および Cond は省略 :: 記法を用いて定義されたレコード型であることから、Expr は合併型である。

```
Expr  = Const | Var | Infix | Cond;
Const :: nat | bool;
Var   :: id:Id
         tp: [<Bool> | <Nat>];
Infix :: Expr * Op * Expr;
Cond  :: test : Expr
         cons : Expr
         altn : Expr
```

また expr = mk_Cond(mk_Var("b",<Bool>),mk_Const(3), mk_Var("v",nil)) とすると:

```
is_Cond(expr)        ≡  true
is_Const(expr.cons)  ≡  true
is_Var(expr.altn)    ≡  true
is_Infix(expr.test)  ≡  false
```

合併型を用いることで、今までで定義してきた演算子の使用を拡張することができる。たとえば =を bool | nat 上でのテストと解釈することで次を得る。

```
1 = false  ≡  false
```

同様に、集合の合併や列の連結の代わりに合併型を用いることができる:

```
{1,2} union {false,true}  ≡  {1,2, false,true}
['a','b']^[<c>,<d>]       ≡  ['a','b', <c>,<d>]
```

集合合併においては、 nat | bool 型の集合上での合併を考える；一方列連結に対しては、 char | <c> | <d>型の列を操作している。

4.2.7 オブジェクト参照型

オブジェクト参照型が標準 VDM-SL の型に加えられた。したがって純粋なオブジェクト指向原則に従わせようとすれば、オブジェクト参照型 (およびそのオブジェクト) の使用を制限する直接的な方法は存在しない；クラスを超えたさらな

る構造化機能はいまだ予見すらなされていない。これらの原則から考えれば、型構成子 (レコード、写像、集合、等々) と結合されるオブジェクト参照型の使用には十分な注意を払うべきであるといえる。

オブジェクト参照型の値はオブジェクトへの**参照**とみなすことができる。たとえばもし、あるインスタンス変数 (第 11 節参照) がオブジェクト参照型として定義されるならば、このインスタンス変数が定義されているクラスは、オブジェクト参照型の中のクラスの「クライアント」となる；つまり**クライアント関係** がこの 2 つのクラス間に確立する。

オブジェクト参照型はクラス名によって表示される。オブジェクト参照型に含まれるクラス名は、その仕様の中で定義された 1 つのクラスの名称でなければならない。

この型の値に対して定義された演算子は、相等 (‘=’) と不等 (‘<>’) のみである。相等は、値ではなく参照に基づくものとなる。このことは、もし o1 と o2 が 2 つの異なるオブジェクトであるならば、たまたま同じ内容であったとしても、o1 = o2 は false となるということである。

構成子 オブジェクト参照は new 式 (第 7.13 節参照) を用いて構成される。

演算子

演算子	名称	型
t1 = t2	相等	$A * A \to$ bool
t1 <> t2	不等	$A * A \to$ bool

例題 オブジェクト参照の使用例として二分木のクラス定義である:

```
class Tree

  types

    protected tree = <Empty> | node;

    public node :: lt: Tree
                   nval : int
                   rt : Tree
```

```
 instance variables
    protected root: tree := <Empty>;
end Tree
```

ここでは node 型を定義するが、これは node 値で構成されていて、lt,rt オブジェクトを参照するものである。アクセス指定子についての詳細は第 14.4 節に述べられている。

4.2.8 関数型

VDM++ では関数型もまた型定義に用いることができる。型 A (実際は型のリスト) から型 B への関数型というのは、型 A の各々の要素に対して B の要素を結びつける型である。関数の値は、プログラム言語においての関数と同じもので他に副作用をおよぼすことのない (つまりグローバル変数を使用していない) ものとして考えることができる。

このような用い方は、関数が値として用いられるという意味で上級向けの使用法と考えることができる (したがって初読ではこの節はとばしていただいてもよい)。関数値は、ラムダ式 (以下を参照) によって生成されることもあるし、第 6 節に述べる関数定義による場合もある。関数値は、関数を引数としたりまた戻り値にすることができるという意味で、高階なものとなり得る。この方法を用いれば、最初のパラメーターの組が与えられると新しい関数が 1 つ返されるというように、関数はカリー化されることが可能である (次の例題を参照)。

構文:

型 = 関数型
  | ... ;

関数型 = 部分関数型
  | 全関数型 ;

部分関数型 = 任意の型, '->', 型 ;

全関数型 = 任意の型, '+>', 型 ;

任意の型 = 型 | '(',')' ;

等式: `F = A +> B`[10] または `F = A -> B`

構成子: 伝統的な関数定義に加えて、関数を構成する唯一の方法がラムダ式によるものである: `lambda pat1 : T1, ..., patn : Tn & body` ここにおける `patj` はパターン、 `Tj` は型式、そして `body` は本体式で全パターンよりパターン識別子を用いることが許されている。

ラムダ式に対する構文や意味定義は、第 7.16 節にある。

演算子:

演算子	名称	型
`f(a1,...,an)`	関数適用	$A1 * \cdots * An \to B$
`f1 comp f2`	関数合成	$(B \to C) * (A \to B) \to (A \to C)$
`f ** n`	関数反復	$(A \to A) * \mathsf{nat} \to (A \to A)$
`t1 = t2`	相等	$A * A \to \mathsf{bool}$
`t1 <> t2`	不等	$A * A \to \mathsf{bool}$

型値間での相等と不等については、最大の注意を払うべきである。VDM++においてこれは、数学上の相等 (または不等) に相等するが、一般関数と同様に無限値に対して計算不能となる。このように、インタプリターでの相等は関数値の抽象構文上のものである (以下の `inc1` と `inc2` を参照)。

演算子の意味定義:

演算子名称	意味記述
関数適用	関数 `f` を $\mathtt{a}_j$ の値に適用した結果。第 7.12 章の適用式の定義を参照のこと。
関数合成	最初に `f2` を適用して次はその結果に `f1` を適用することと同等な関数。`f1` はカリー化されてもよいが，`f2` はいけない。
関数繰り返し	`f` を `n` 回適用することと同等な関数。`n = 0` の場合はそのパラメーター値をそのまま返す恒等関数となる。 `n = 1` の場合はその関数自身となる。 `n > 1` の場合、 `f` の戻り値はそれ自身のパラメーター型に含まれるものでなければならない。

例題: 以下に関数の値を定義してみよう:

[10] 全関数矢印は全定義関数のシグネチャにおいてのみ用いることができ、型定義においては用いることはできないことに注意したい。

```
f1 = lambda x : nat & lambda y : nat & x + y
f2 = lambda x : nat & x + 2
inc1 = lambda x : nat & x + 1
inc2 = lambda y : nat & y + 1
```

ここで次のことが導かれる:

```
f1(5)          ≡  lambda y :nat & 5 + y
f2(4)          ≡  6
f1 comp f2     ≡  lambda x :nat & lambda y :nat & (x + 2) + y
f2 ** 4        ≡  lambda x :nat & x + 8
inc1 = inc2    ≡  false
```

相等判定は、VDM++ の意味定義に基づいての期待される結果に従うものではないことに注意したい。このように、関数といった無限値に対する相等の使用には**十分**注意深くなる必要がある。

4.3 不変条件

もし先に述べた等式によって指定されたデータ型が許されるべきでない値を含むような場合、それは 1 つの不変条件により 1 つの型の値に制限することができる。結果として、その型はもともとの値の部分集合に制限されるということである。このように、述語の手段によって、定義された型の条件にかなう値はこの式が true となる値に制限されるのである。

不変条件の使用についての一般的構成は次の通り:

```
Id = Type
inv pat == expr
```

ここで pat は Id 型に属する値にマッチングさせるパターンであり、expr は true となる式であり、パターン pat から識別子のいくつかまたはすべてを含んでいる。

ある不変条件が定義された場合、1 つの新しい (全) 関数がシグネチャと共に暗黙に生成される:

```
inv_Id : Type +> bool
```

この関数は、他の不変条件、関数、あるいは操作の定義中で用いることも可能である。

たとえば、28 ページ上に定義されたレコード型 Score を思い返してみよう。不変条件を用いることで、得点数は勝つか引き分けたゲームの数と一致する、ということが保障できる:

```
Score :: team : Team
         won : nat
         drawn : nat
         lost : nat
         points : nat
inv sc == sc.points = 3 * sc.won + sc.drawn;
```

この型に対して暗黙に作成される不変条件関数は次の通り:

```
inv_Score : Score +> bool
inv_Score (sc) ==
  sc.points = 3 * sc.won + sc.drawn;
```

5 アルゴリズム定義

VDM++ では、アルゴリズムが関数と操作の両方により定義できる。しかしながら、伝統的なプログラム言語における関数にただちに相当するというものではない。VDM++ において関数と操作を区別するものは、ローカルおよびグローバル変数の使用である。操作は、グローバル変数といくらかのローカル変数の両方を扱うことができる。ローカル変数とグローバル変数の両者については後に述べられる。関数は、グローバル変数にアクセスすることはできないしローカル変数を定義することも許されていないという意味で、純粋なものである。このように、操作が命令的なものである一方で、関数は純粋に作用的なものである。

関数と操作は、陽に (明確なアルゴリズム定義によって) あるいは陰に (事前条件または事後条件によって)、両方法で定義することができる。関数に対する明示的

なアルゴリズム定義を式と呼ぶ一方、操作に対するそれは文と呼ぶ。事前条件は、関数や操作が評価される前に何を保持していなくてはならないかを指定する true の値をとる式である。事前条件は、パラメーター値と (操作の場合は) グローバル変数のみを参照することができる。事後条件もまた、関数や操作が評価された後に何が保持されなければならないかを指定する true の値をとる式である。事後条件は、結果識別子、パラメーター値、グローバル変数の現在値、そしてグローバル変数の旧値、を参照することができる。グローバル変数の旧値とは、操作が評価される前の変数の値のことである。関数ではグローバル変数の変更は許されていないが、操作だけはグローバル変数の旧値を参照することができる。

しかしながら、インタープリタにより関数と操作の両方の実行を可能にするためには、それらは明示的に定義されていなければならない[11]。VDM++ では、陽関数および操作定義に対して追加の事前または事後条件を指定することもできる。陽関数および操作定義の事後条件において、結果の値は予約語 RESULT によって参照されなければならない。

6 関数定義

VDM++ では、1 階関数と高階関数を定義することができる。高階関数とは、カリー化関数 (結果として関数を返す関数) かまたは関数を引数にとる関数である。さらには、1 階のものも高階のものもいずれも多相であることが可能である。一般的に、ある関数を定義するための構文は次の通り:

```
関数定義 = 'functions', [ アクセス関数定義,
           { ';', アクセス関数定義 }, [ ';' ] ] ;

アクセス関数定義 = ([ アクセス ], [ 'static' ]) | ([ 'static' ], [ アクセス ]),
                   関数定義 ;

アクセス = 'public'
         | 'private'
         | 'protected' ;
```

[11] 暗黙に指定された関数と演算は一般的に実行できない、というのもそれらの事後条件は出力を入力に明白に関係づける必要がないからである。出力が満たさなくてはならないプロパティを指定することで、しばしば済む。

関数定義 = 陽関数定義
| 陰関数定義
| 拡張陽関数定義 ;

陽関数定義 = 識別子,
[型変数リスト], ':', 関数型,
識別子, パラメーターリスト, '==',
関数本体,
['pre', 式],
['post', 式],
['measure', 名称] ;

陰関数定義 = 識別子, [型変数リスト],
パラメーター型, 識別子型ペアリスト,
['pre', 式],
'post', 式 ;

拡張陽関数定義 = 識別子, [型変数リスト],
パラメーター型,
識別子型ペアリスト,
'==', 関数本体,
['pre', 式],
['post', 式] ;

型変数リスト = '[', 型変数識別子,
{ ',', 型変数識別子 }, ']' ;

識別子型ペアリスト = 識別子, ':', 型,
{ ',', 識別子, ':', 型 } ;

パラメーター型 = '(', [パターン型ペアリスト], ')' ;

パターン型ペアリスト = パターンリスト, ':', 型,
{ ',', パターンリスト,':', 型 } ;

関数型 = 部分関数型
| 全関数型 ;

部分関数型 = 任意の型, '->', 型 ;

全関数型 = 任意の型, '+>', 型 ;

任意の型 = 型 | '(',')' ;

パラメーター群 = '(', [パターンリスト], ')' ;

パターンリスト = パターン,{ ',', パターン } ;

関数本体 = 式
| 'is not yet specified'
| 'is subclass responsibility' ;

ここで、あるモデルが発展過程にある間は is not yet specified の指定が関数本体として用いられることが許されている; is subclass responsibility の指定はこの関数本体の実行にはどのようなサブクラスでも責任を負わなければならないことを示す。

アクセスおよび static 指定子の詳細は、第 14.4 節に記述がある。静的関数は静的でない操作や関数を呼び出すことは許されていない、また静的関数の定義において自身の式を用いることはできない、ということは注意しておこう。

陽関数定義の簡単な例は関数 map_inter であり、これは自然数上の 2 つの両立する写像をもってきて、両者に共通する写を返すものである

```
map_inter: (map nat to nat) * (map nat to nat) -> map nat to nat
map_inter (m1,m2) ==
  (dom m1 inter dom m2) <: m1
pre  forall d in set dom m1 inter dom m2 & m1(d) = m2(d)
```

関数結果についての主張を許すために選択事後条件をさらにまた用いることができることにも注意しよう:

```
map_inter: (map nat to nat) * (map nat to nat) -> map nat to nat
map_inter (m1,m2) ==
  (dom m1 inter dom m2) <: m1
pre  forall d in set dom m1 inter dom m2 & m1(d) = m2(d)
post  dom RESULT = dom m1 inter dom m2
```

同じ関数が暗黙的にまた定義されることも可能である:

```
map_inter2 (m1,m2: map nat to nat) m: map nat to nat
pre  forall d in set dom m1 inter dom m2 & m1(d) = m2(d)
post  dom m = dom m1 inter dom m2 and
      forall d in set dom m & m(d) = m1(d);
```

拡張陽関数定義 (標準ではない) の簡単な例は関数 map_disj で、これは自然数上で 2 つの両立する写像を持ってきて、それらのどちらかの写像に対して唯一の写からなる写像を返す:

```
map_disj (m1:map nat to nat,m2:map nat to nat) res : map nat to nat ==
  (dom m1 inter dom m2) <-: m1 munion
  (dom m1 inter dom m2) <-: m2
pre  forall d in set dom m1 inter dom m2 & m1(d) = m2(d)
post  dom res = (dom m1 union dom m2) \ (dom m1 inter dom m2)
      and
      forall d in set dom res & res(d) = m1(d) or res(d) = m2(d)
```

(ここにおいて事後条件をインタープリタに通す試みは、もしかすると実行時エラーを引き起こすかもしれない、というのは m1(d) と m2(d) は同時に両者が定義される必要はないからなのである。)

関数 map_inter と map_disj はインタプリターにより評価することが可能であるが、暗黙的関数である map_inter2 は評価することができない。しかしながら、これら 3 つの場合における事前条件と事後条件は他の関数のなかで使用することが可能である; たとえば map_inter2 の定義から、関数 pre_map_inter2 と post_map_inter2 を以下のシグネチャで得る:

```
pre_map_inter2 : (map nat to nat) * (map nat to nat) +> bool
```

```
post_map_inter2 : (map nat to nat) * (map nat to nat) *
                  (map nat to nat) +> bool
```

これらの種類の関数は自動的にインタープリタで作成され、他の定義においても用いることができる (この技術は引用とよばれる)。一般的に、次のシグネチャをもつ関数 f に対して

```
f : T1 * ... * Tn -> Tr
```

関数に対する事前条件を定義することで、次のシグネチャの関数 pre_f が生成される。

```
pre_f : T1 * ... * Tn +> bool
```

そして関数に対する事後条件を定義することで、次のシグネチャの関数 post_f が生成される。

```
post_f : T1 * ... * Tn * Tr +> bool
```

関数は再帰 (自分自身の呼び出し) を使って定義することもできる。これがなされた場合、'measure' 関数を追加することが推奨される。これはモデルから生成される証明課題で、終了証明を実行できるようにするために利用される。シンプルな階乗関数の例を以下に定義する:

```
functions

fac: nat +> nat
fac(n) ==
  if n = 0
  then 1
  else n * fac(n - 1)
measure id
```

ここで、 id は以下のように定義されている:

```
id: nat +> nat
id(n) == n
```

6.1 多相関数

関数はまた多相であることが可能である。これは、複数の異なる型の値のもとに使用可能な包括的な関数を生成することができるということを意味する。この目的のために、型引数 (または接頭辞@記号をおき通常の識別子と同様に記述された型変数) が用いられる。空のバッグをつくりだすための多相関数を考える: [12]

```
empty_bag[@elem] : () +> (map @elem to nat1)
empty_bag() ==
  { |-> }
```

上記の関数が使用できる以前のこととして、関数 empty_bag の、たとえば整数といったある型のインスタンス生成を行わなくてはならない:

```
emptyInt = empty_bag[int]
```

さぁこれで整数をいれるための新しいバッグをつくるために、関数 emptyInt を使用することができる。更なる多相関数の例としては:

```
num_bag[@elem] : @elem * (map @elem to nat1) +> nat
num_bag(e, m) ==
  if e in set dom m
  then m(e)
  else 0;

plus_bag[@elem] : @elem * (map @elem to nat1) +> (map @elem to nat1)
plus_bag(e, m) ==
  m ++ { e |-> num_bag[@elem](e, m) + 1 }
```

もし事前条件や事後条件が多相関数に対して定義された場合は、対応する述語関数もまた多相である。たとえばもし num_bag が下記のように定義されていたとすると

[12] 多相関数の例は [Daw91] から引用する。バッグというのは、バッグの中での要素からその要素の重複度への写像をモデル化したものである。ここでの重複度は少なくも 1 以上であり、つまり要素がないならこの写像の役目は負えないので、0 に写像されるものではない。

```
num_bag[@elem] : @elem * (map @elem to nat1) +> nat
num_bag(e, m) ==
  m(e)
pre  e in set dom m
```

事前条件は次のようになるであろう

```
pre_num_bag[@elem] :@elem * (map @elem to nat1) +> bool
```

また、measure は機能が多相的に定義された時に使用されるべきです。

6.2 高階関数

関数は他の関数を引数として受け取ることが許される。この簡単な例は、自然数の列となる関数 nat_filter であり、1 つの述語をもち、この述語を満足させる部分列を返すものである:

```
nat_filter : (nat -> bool) * seq of nat -> seq of nat
nat_filter (p,ns) ==
  [ns(i) | i in set inds ns & p(ns(i))];
```

このとき nat_filter (lambda x:nat & x mod 2 = 0, [1,2,3,4,5]) ≡ [2,4].
実際、このアルゴリズムは自然数に限ったものではない、したがってこの関数の多相版を定義してもよいであろう:

```
filter[@elem]: (@elem -> bool) * seq of @elem -> seq of @elem
filter (p,l) ==
  [l(i) | i in set inds l & p(l(i))];
```

so filter[real](lambda x:real & floor x = x, [2.3,0.7,-2.1,3]) ≡ [3].

関数はまた結果として関数を返してもよい。これの例は関数 fmap である:

```
fmap[@elem]: (@elem -> @elem) -> seq of @elem -> seq of @elem
```

```
fmap (f)(l) ==
  if l = []
  then []
  else [f(hd l)]^(fmap[@elem] (f)(tl l));
```

よって fmap[nat](lambda x:nat & x * x)([1,2,3,4,5]) ≡ [1,4,9,16,25]

7 式

この中の節では異なる種類の式の 1 つ 1 つについて述べていこう。各々を次の方法で記述する:

- BNF 構文記法
- 非公式な意味定義記述
- 使用の記述例

7.1 let 式

構文:

式 = let 式
  | let be 式
  | ... ;

let 式 = 'let', ローカル定義 { ',', ローカル定義 },
  'in', 式 ;

let be 式 = 'let', 束縛, ['be', 'st', 式], 'in',
  式 ;

ローカル定義 = 値定義
  | 関数定義 ;

値定義 = パターン, [':', 型], '=', 式 ;

ここでの構成要素である “関数定義” は第 6 節で述べられている。

意味定義: 単純な *let* 式 は次の形式をもつ:

```
let p1 = e1, ..., pn = en in e
```

ここで、 p1, ..., pn はパターン、 e1, ..., en はそれぞれの対応パターン pi にマッチさせる式であって、 e は任意の型でよいが p1, ..., pn の中のパターン識別子を含む式である。これは、パターン p1,..., pn が対応する式 e1, ..., en とマッチさせられる文脈中での、式 e の値を示している。

ローカル関数定義を用いることで、より発展した形の let 式をつくることもできる。そのようなことを行う意味は単に、このようなローカル定義関数のスコープは let 式の本体に制限されているということにある。

標準の VDM-SL においては、定義の収集が相互に再帰するものとなる可能性がある。しかしながら VDM++ においては、このようなものがインタープリタでサポートされることはない。さらに、すべての構成子が使用される前に定義されているように、定義に順番付けがされていなければならない。

let-be-such-that 式は次の形式をもつ:

```
let b be st e1 in e2
```

ここでは、 b は集合値 (または型) に対する束縛で、 e1 は ブール式、 e2 は式だが何の型であってもよく、b におけるパターンのパターン識別子を含むものである。be st e1 部分はオプション。この式は、b のパターンが b の集合要素かまたは b の中の型の値とマッチさせる文脈中での式 e2 の値を示す[13]。 st e1 式がある場合は、マッチングの文脈中で e1 が true となる束縛のみが用いられる。

例題: *let* 式 は読みやすさの改善に役立つ、特に何回も使われる複雑な式は縮めることで改善される。たとえば 40 ページの関数 map_disj を改善することができる:

[13] 集合束縛のみはインタープリタによって実行できることを思い出そう。

```
map_disj : (map nat to nat) * (map nat to nat) -> map nat to nat
map_disj (m1,m2) ==
  let inter_dom = dom m1 inter dom m2
  in
    inter_dom <-: m1 munion
    inter_dom <-: m2
pre  forall d in set dom m1 inter dom m2 & m1(d) = m2(d)
```

また複雑な構造体を構成要素に分解する上でも便利である。たとえば、前に定義したレコード型 Score (28 ページ) を使用することで、あるスコアがもうひとつより大きいかどうかをテストすることができる:

```
let mk_Score(-,w1,-,-,p1) = sc1,
    mk_Score(-,w2,-,-,p2) = sc2
in (p1 > p2) or (p1 = p2 and w1 > w2)
```

この特別な例では、2 つのスコアから 2 番目と 5 番目の構成要素を抽出している。don't care パターン (79 ページ) が、この式本体で行われた処理と残りの構成要素が無関係であることを示すために用いられていることに注目しよう。*let-be-such-that* 式 は、1 つの集合から 1 つの要素を選ぶ意味のない選択を減らすために、特に集合上での再帰定義の形式化において用いられる。これについての例は、列の filter 関数 (43 ページ) を集合上で考えたものである:

```
set_filter[@elem] : (@elem -> bool) -> (set of @elem) ->
                    (set of @elem)
set_filter(p)(s) ==
  if s = {}
  then {}
  else let x in set s
       in (if p(x) then {x} else {}) union
          set_filter[@elem](p)(s \ {x});
```

別の方法として、この関数を集合内包 (第 7.7 節参照) を用いて定義することもできるであろう:

```
set_filter[@elem] : (@elem -> bool) -> (set of @elem) ->
                    (set of @elem)
set_filter(p)(s) ==
  { x | x in set s & p(x)};
```

最後の例はオプションである “be such that” 部分をどのように用いることができるかを示す。いくつかのプロパティをもつある要素が存在することはわかっているがその要素に対する明示的な式がわからないまたは記述することが難しい場合に、この部分は特に役に立つ。たとえばこの式を選択ソートアルゴリズムを書くために活用することができる:

```
remove : nat * seq of nat -> seq of nat
remove (x,l) ==
  let i in set inds l be st l(i) = x
  in l(1,...,i-1)^l(i+1,...,len l)
pre  x in set elems l;

selection_sort : seq of nat -> seq of nat
selection_sort (l) ==
  if l = []
  then []
  else let m in set elems l be st
       forall x in set elems l & m <= x
       in [m]^(selection_sort (remove(m,l)))
```

ここでは、最初の関数は与えられたリストから与えられた要素を取り除く；2 番目の関数は並び替えされていないリスト部分から最も小さい要素を繰り返し取り除き、並び替えされた部分の頭に置く。

7.2 def 式

この式は、第 12 節で述べられる操作の内部でのみ用いることができる。式の部分でグローバル変数を取り扱うために、操作の内部で特別な式 (すなわち def 式) が許されている。

構文:

```
式 = ...
   | def式
   | ... ;

def式 = 'def', パターン束縛, '=', 式,
        { ';', パターン束縛, '=', 式 }, [ ';' ],
        'in', 式 ;
```

意味定義: *def*式 は次の形式をもつ:

```
def pb1 = e1;
    ...
    pbn = en
in
  e
```

*def*式 は、右辺の式がローカル変数やグローバル変数の値に従属する可能性はあるが相互に再帰するものではない、といったことを除けば、let 式に相等する。これは、パターン (または束縛)pb1，...，pbn が対応する式 e1，...，en とマッチする文脈中で、式 e の値を示す[14]。

例題: 式の値はグローバル変数に従属するという事実に気づいてもらえるよう、*def*式 が合理的な方法で用いられる。

これは小さな例で説明することができる:

```
def user = lib(copy) in
  if user = <OUT>
  then true
  else false
```

copy が文脈中に定義されている場所で、lib はグローバル変数である (このように lib(copy) は変数の一部の内容検索と考えることができる)。

第 13.1 節の操作 GroupRunnerUp_expl でもまた def 式の例が与えられている。

[14]束縛が用いられている場合は、簡単に言えばパターンと一致した値はさらに第 8 章で述べられる型式または集合式によって制限を受けるということを意味する。

7.3 単項式または 2 項式

構文:

式 = ...
| 単項式
| 2 項式
| ... ;

単項式 = 接頭辞式
| 逆写像 ;

接頭辞式 = 単項演算子, 式 ;

単項演算子 = '+' | '-' | 'abs' | 'floor' | 'not'
| 'card' | 'power' | 'dunion' | 'dinter'
| 'hd' | 'tl' | 'len' | 'elems' | 'inds' | 'conc'
| 'dom' | 'rng' | 'merge' ;

逆写像 = 'inverse', 式 ;

2 項式 = 式, 2 項演算子, 式 ;

2 項演算子 = '+' | '-' | '*' | '/'
| 'rem' | 'div' | 'mod' | '**'
| 'union' | 'inter' | '\' | 'subset'
| 'psubset' | 'in set' | 'not in set'
| '^'
| '++' | 'munion' | '<:' | '<-:' | ':>' | ':->'
| 'and' | 'or'
| '=>' | '<=>' | '=' | '<>'
| '<' | '<=' | '>' | '>='
| 'comp' ;

意味定義: 単項式と 2 項式は、特定の型の値を記述する演算子と演算対象の結合である。これらすべての演算子のシグネチャについては、すでに第 4 節で述べてあるのでそれ以上の説明はここでは行わない。逆写像単項演算子は、数学的構文における接尾辞記号で記述されるため、別に取り扱う。

例題: これらの演算子を用いた例題は第 4 節で与えられるため、ここでは触れない。

7.4 条件式

構文:

式 = ...
| if式
| cases式
| ... ;

if式 = 'if', 式, 'then', 式,
{ elseif式 }, 'else', 式 ;

elseif式 = 'elseif', 式, 'then', 式 ;

cases式 = 'cases', 式, ':',
cases式選択肢群,
[',', others式], 'end' ;

cases式選択肢群 = cases式選択肢,
{ ',', cases式選択肢 } ;

cases式選択肢 = パターンリスト, '->', 式 ;

others式 = 'others', '->', 式 ;

意味定義: *if*式 と *cases*式は、1 つの特定の式の値を基に、複数の中から 1 つの式を選ぶことを可能にする。

*if*式 は次の形式をもつ:

```
if e1
then e2
else e3
```

ここで e1 はブール式であり、一方 e2 と e3 はどのような型であってもよい。もし e1 が与えられた文脈中で true であるならば、 if式は与えられた文脈中で評価された e2 の値を表す。そうでなければ、if式は与えられた文脈上で e3 の値を表す。elseif 式の使用は、ある式の else 部分においてネストされた if-then-else 式を単に省略したものである。

*cases*式 は次の形式をもつ

```
cases e :
  p11, p12, ..., p1n -> e1,
  ...                -> ...,
  pm1, pm2, ..., pmk -> em,
  others             -> emplus1
end
```

ここで e は 1 つの任意の型の式であり、pij で表すすべては 1 つ 1 つが式 e にマッチするパターンである。ei で表すのは任意の型の式であり、キーワードの others とそれに対応する式 emplus1 とはオプションとなる。cases 式では、 pij パターンの 1 つが e にマッチした文脈中で評価された ei 式の値を示す。選択された ei は、パターンの 1 つを式 e とマッチさせることができた最初の入口である。もしパターンのうちのどれも e にマッチしない場合には、 others 節がなくてはならないし、そこで cases 式は与えられた文脈中で評価される emplus1 の値を示す。

例題: VDM++ における if 式は、大部分のプログラム言語において用いられているものに相等するが、その一方 VDM++ における cases 式は、大部分のプログラム言語よりもより一般的なものとなる。このことは実際にパターンマッチングがおきる事例から見て取れるであろうが、しかしまた大部分のプログラム言語におけるようなパターンが定数である必要がないためでもある。条件式の使用例はマージソートアルゴリズムの記述により提供される:

```
lmerge : seq of nat * seq of nat -> seq of nat
lmerge (s1,s2) ==
  if s1 = [] then s2
  elseif s2 = [] then s1
  elseif (hd s1) < (hd s2)
  then [hd s1]^(lmerge (tl s1, s2))
  else [hd s2]^(lmerge (s1, tl s2));

mergesort : seq of nat -> seq of nat
mergesort (l) ==
  cases l:
    [] -> [],
```

```
    [x] -> [x],
    l1^l2 -> lmerge (mergesort(l1), mergesort(l2))
  end
```

cases 式によって提供されたパターンマッチングは、型の合併を扱うことに役立つ。たとえば、31 ページからの型定義 Expr を用いることで次を得る:

```
print_Expr : Expr -> seq1 of char
print_Expr (e) ==
  cases e:
    mk_Const(-) -> "Const of"^(print_Const(e)),
    mk_Var(id,-) -> "Var of"^id,
    mk_Infix(mk_(e1,op,e2)) -> "Infix of"^print_Expr(e1)^","
                                         ^print_Op(op)^","
                                         ^print_Expr(e2),
    mk_Cond(t,c,a) -> "Cond of"^print_Expr(t)^","
                               ^print_Expr(c)^","
                               ^print_Expr(a)
  end;

print_Const : Const -> seq1 of char
print_Const(mk_Const(c)) ==
  if is_nat(c)
  then "nat"
  else -- must be bool
       "bool";
```

関数 print_Op は同様に定義されるであろう。

7.5 限量式

構文: 式 = ...
| 限量式
| ... ;

限量式 = 全称限量式
| 存在限量式
| 1 存在限量式 ;

全称限量式 = 'forall', 束縛リスト, '&', 式 ;

存在限量式 = 'exists', 束縛リスト, '&', 式 ;

束縛リスト = 多重束縛, { ',', 多重束縛 } ;

1 存在限量式 = 'exists1', 束縛, '&', 式 ;

意味定義: 限量式には 3 つの形式がある: 全称 (forall と記述される), 存在 (exists と記述される), そして *1* 存在 (exists1 と記述される) である。以下に述べられるように、各々はブール値である true または false の値をとる。

全称限量式 は次の形式をもつ:

```
forall mbd1, mbd2, ..., mbdn & e
```

ここで各々の mbdi は多重束縛 pi in set s (あるいは型束縛であるならば pi : 型) であり、 e は mbdi のパターン識別子を含むブール式である。この値は、e を mbd1, mbd2, ..., mbdn における束縛のすべてにおいて文脈上で評価して、true であるならば true となりそうでない場合は false となる。

存在限量式 は次の形式をもつ:

```
exists mbd1, mbd2, ..., mbdn & e
```

ここで mbdi および e は、全称限量式におけるものと同じである。ここで mbd1, mbd2, ..., mbdn における束縛の少なくとも 1 つを選択した文脈上で評価した場合に e が true であったならば、この値は true となりそうでない場合は false となる。

1 存在限量式 は次の形式をもつ:

```
exists1 bd & e
```

ここで bd は 集合束縛か型束縛であり、 e は bd のパターン識別子を含むブール式である。束縛のうちのちょうど 1 つを選択した文脈上で評価して e が true であるならば、この値は true となりそうでない場合は false となる。

すべての限量式は、可能な優先度の中で最も低い優先度を持つ。これは、可能な限り長い構成式が使われることを意味する。式は、構文的に可能な限りの右側へ続く。

例題: 存在限量の例は以下の QualificationOk で提示される関数で与えられる。この関数は、[FJ98] における化学プラント警報システムの仕様書からとってきたものであるが、ある専門家の集団が要求された資質を満たすか否かを照合するものである。

```
types

ExpertId = token;
Expert :: expertid : ExpertId
          quali : set of Qualification
inv ex == ex.quali <> ;
Qualification = <Elec> | <Mech> | <Bio> | <Chem>

functions

QualificationOK: set of Expert * Qualification -> bool
QualificationOK(exs,reqquali) ==
    exists ex in set exs & reqquali in set ex.quali
```

この関数 min は全称限量の例を示す:

```
min(s:set of nat) x:nat
pre  s <> {}
post  x in set s and
      forall y in set s \ {x} & y < x
```

1 存在限量は、すべての写像 m が満足する関数プロパティを述べるために用いることができる:

```
forall d in set dom m &
  exists1 r in set rng m & m(d) = r
```

7.6 iota 式

構文:

式 = ...
| iota 式
| ... ;

iota 式 = 'iota', 束縛, '&', 式 ;

意味定義: *iota* 式は次の形式をもつ:

```
iota bd & e
```

ここで bd は集合束縛かまたは型束縛であり、 e は bd のパターン識別子を含むブール式である。束縛に一致して本体式 e を true とする唯一の値が存在するならば、iota 演算子を唯一用いることができる (i.e. exists1 bd & e は true でなくてはならない)。iota 式の意味定義は、本体式 (e) を満たす唯一の値を返すということである。

例題: 次に定義された値 sc1,...,sc4 を用いる

```
sc1 = mk_Score (<France>, 3, 0, 0, 9);
sc2 = mk_Score (<Denmark>, 1, 1, 1, 4);
sc3 = mk_Score (<SouthAfrica>, 0, 2, 1, 2);
sc4 = mk_Score (<SaudiArabia>, 0, 1, 2, 1);
```

これより

```
iota x in set {sc1,sc2,sc3,sc4} & x.team = <France>  ≡  sc1
iota x in set {sc1,sc2,sc3,sc4} & x.points > 3       ≡  ⊥
iota x :  Score & x.points < x.won                   ≡  ⊥
```

最後の例は実行不可能であり、加えて最後の 2 式は未定義となることに注意しよう奸酎 O 者は式を満たす値が多くなるからであり、後者は式を満たす値がないからである。

7.7 集合式

構文:

式 = ...
| 集合列挙
| 集合内包
| 集合範囲式
| ... ;

集合列挙 = '{', [式リスト], '}' ;

式リスト = 式, { ',', 式 } ;

集合内包 = '{', 式, '|', 束縛リスト,
['&', 式], '}' ;

集合範囲式 = '{', 式, ',', '...', ',',
式, '}' ;

意味定義: 集合列挙は次の形式をもつ:

```
{e1, e2, e3, ..., en}
```

ここで e1 から en までは一般の式である。列挙された式の値の集合を構成する。空集合は {} と書かれなければならない。

集合内包式は次の形式をもつ:

```
{e | mbd1, mbd2, ..., mbdn & P}
```

述語 P が true と評価される束縛すべてのもとで、式 e を評価することで 1 つの集合が構成される。多重束縛には集合束縛と型束縛の両方を含めることができる。したがって mbdn は pat1 in set s1, pat2 : tp1, ...in set s2 というようになるであろうが、ここにおける pati はパターンであり (通常は単なる識別子である)、 s1 や s2 は式で構成される集合である (これに対して tp1 は、型束縛もまた用いることができることを示すために使われている)。ただし型束縛はインタープリタでは実行できないので注意したい。

集合範囲式 は集合内包の特別な場合である。これは次の形式をもつ

```
{e1, ..., e2}
```

ここでの e1 と e2 は数式である。この集合範囲式は e1 から e2 までに含まれる整数の集合を表記する。e2 が e1 よりも小さい場合には、集合範囲式は空集合を表す。

例題: Europe={<France>,<England>,<Denmark>,<Spain>} および GroupC = {sc1,sc2,sc3,sc4} (ここでの sc1,...,sc4 は前述の例にて定義されたもの) の値を用いて次を得る

```
{<France>, <Spain>} subset Europe          ≡ true
{<Brazil>, <Chile>, <England>}             ≡ false
      subset Europe
{<France>, <Spain>, "France"}              ≡ false
      subset Europe
{sc.team | sc in set GroupC                ≡ {<France>,
      & sc.points > 2}                       <Denmark>}
{sc.team | sc in set GroupC                ≡ {<SouthAfrica>,
      & sc.lost > sc.won }                   <SaudiArabia>}
{2.718,...,3.141}                          ≡ {3}
{3.141,...,2.718}                          ≡ {}
{1,...,5}                                  ≡ {1,2,3,4,5}
{ x | x:nat & x < 10 and x mod 2 = 0}       ≡ {0,2,4,6,8}
```

7.8 列式

構文:

```
式 = ...
   | 列列挙
   | 列内包
   | 部分列
   | ... ;

列列挙 = '[', [ 式リスト ], ']' ;

列内包 = '[', 式, '|', 集合束縛,
         [ '&', 式 ], ']' ;
```

部分列 = 式,
'(', 式, ',', '...', ',',
式, ')' ;

意味定義: 列列挙は次の形式をもつ:

```
[e1, e2, ..., en]
```

ここでの e1 から en は一般の式である。これは列挙された要素の列を構成する。空列は [] と書かれなければならない。

列内包 は次の形式をもつ:

```
[e | pat in set S & P]
```

ここでの式 e は、パターン pat からもってきた識別子を用いることになる (通常このパターンは単なる識別子となるが、唯一実際上の必要条件としては、ちょうど 1 つのパターン識別子のみがパターン中に存在するということである)。S は値 (通常は自然数) の集合である。このパターン識別子の束縛は何らかの種類の数値に対するものでなければならず、これにより結果列における要素の順を指示するために用いられる。述語 P が true と評価されるすべての束縛上で式 e を評価することにより、列を構成する。

列 l の部分列 というのは l の連続する要素からなる列; 索引 n1 以上 n2 以下のもの、である。次の形式をもつ:

```
l(n1, ..., n2)
```

ここでの n1 と n2 は正の整数式である。下限の n1(空でない列での最初の索引) が 1 より小さい場合は、列式は列の最初の要素から始まることとなる。上限の n2(空でない列で索引中最大のもの) が列の長さよりも大きい場合は、列式は列の最後の要素で終わることとなる。

例題: GroupA が次の列に等しい場合

```
[ mk_Score(<Brazil>,2,0,1,6),
  mk_Score(<Norway>,1,2,0,5),
  mk_Score(<Morocco>,1,1,1,4),
  mk_Score(<Scotland>,0,1,2,1) ]
```

以下が導かれる:

```
[GroupA(i).team                  ≡  [<Brazil>,
| i in set inds GroupA                <Norway>,
   & GroupA(i).won <> 0]              <Morocco>]
[GroupA(i)                       ≡  [mk_Score(<Scotland>,0,1,2,1)]
| i in set inds GroupA
   & GroupA(i).won = 0]
GroupA(1,...,2)                  ≡  [mk_Score(<Brazil>,2,0,1,6),
                                     mk_Score(<Norway>,1,2,0,5)]
[GroupA(i)                       ≡  []
| i in set inds GroupA
   & GroupA(i).points = 9]
```

7.9 写像式

構文:

式 = ...
| 写像列挙
| 写像内包
| ... ;

写像列挙 = '{', 写, { ',', 写 }, '}'
| '{', '|->', '}' ;

写 = 式, '|->', 式 ;

写像内包 = '{', 写, '|', 束縛リスト, ['&', 式], '}' ;

意味定義: 写像列挙 は次の形式をもつ:

```
{d1 |-> r1, d2 |-> r2, ..., dn |-> rn}
```

ここですべての定義域式 di と値域式 ri は一般の式である。空写像は {|->} と書かれなければならない。

写像内包 は次の形式をもつ:

```
{ed |-> er | mbd1, ..., mbdn & P}
```

ここでの構成 mbd1, ..., mbdn は、式 ed および er から集合 (または型) をきめる変数の多重束縛である。写像内包 は、述語 P を true と評価するすべての可能なかぎりの束縛上で、式 ed および er を評価することにより写像を構成する。

例題: GroupG は次の写像と等しいと仮定する

```
{ <Romania> |-> mk_(2,1,0), <England> |-> mk_(2,0,1),
  <Colombia> |-> mk_(1,0,2), <Tunisia> |-> mk_(0,1,2) }
```

この場合に次が成り立つ:

```
{ t |-> let mk_(w,d,-) = GroupG(t)          ≡  {<Romania> |-> 7,
        in w * 3 + d                            <England> |-> 6,
| t in set dom GroupG}                          <Colombia> |-> 3,
                                                <Tunisia> |-> 1}
{ t |-> w * 3 + d                           ≡  {<Romania> |-> 7,
| t in set dom GroupG, w,d,l:nat                 <England> |-> 6}
 & mk_(w,d,l) = GroupG(t)
 and w > l}
```

7.10 組構成子式

構文:

式 = ...
| 組構成子
| ... ;

組構成子 = 'mk_', '(', 式, ',', 式リスト, ')' ;

意味定義: 組構成子式 は次の形式をとる:

```
mk_(e1, e2, ..., en)
```

ここで ei は一般の式である。相等および不等演算子のみが使用できる。

例題: 前述の例で定義された写像 GroupG を用いて、次が得られる:

```
mk_(2,1,0) in set rng GroupG                          ≡ true
mk_("Romania",2,1,0) not in set rng GroupG            ≡ true
mk_(<Romania>,2,1,0) <> mk_("Romania",2,1,0)          ≡ true
```

7.11 レコード式

構文:

式 = ...
| レコード構成子
| レコード修正子
| ... ;

レコード構成子 = 'mk_', 名称, '(', [式リスト], ')' ;

レコード修正子 = 'mu', '(', 式, ',', レコード修正,
{ ',', レコード修正 }')' ;

レコード修正 = 識別子, '|->', 式 ;

意味定義: レコード構成子は次の形式をもつ:

```
mk_T(e1, e2, ..., en)
```

ここでの式 (e1, e2, ..., en) の型は、レコード型 T にある対応する入り口の型に一致する。

レコード修正 は次の形式をとる:

```
mu (e, id1 |-> e1, id2 |-> e2, ..., idn |-> en)
```

ここで式 e の評価として、修正されるべきレコード値を返す。識別子 idi は、e のレコード型の中ですべて異なる名称をもつ入り口でなければならない。

例題: sc が値 mk_Score(<France>,3,0,0,9) であるならば

```
mu(sc, drawn |-> sc.drawn + 1, points |-> sc.points + 1)
≡ mk_Score(<France>,3,1,0,10)
```

さらなる例題として関数 win の説明を行う。この関数は 2 つのチームと 1 つのスコアをもつ。スコアの集合から与えられているチームに相当するスコア (勝ったチームには wsc、負けたチームには lsc) を各々割り当て、mu 演算子を用いてこれらを更新する。チームの集合はここで、新しいスコアをもとのものと置き換えることで更新される。

```
win : Team * Team * set of Score -> set of Score
win (wt,lt,gp) ==
  let wsc = iota sc in set gp & sc.team = wt,
      lsc = iota sc in set gp & sc.team = lt
  in let new_wsc = mu(wsc, won |-> wsc.won + 1,
                           points |-> wsc.points + 3),
         new_lsc = mu(lsc, lost |-> lsc.lost + 1)
     in (gp \ {wsc,lsc}) union {new_wsc, new_lsc}
pre  forall sc1, sc2 in set gp &
          sc1 <> sc2 <=> sc1.team <> sc2.team
          and {wt,lt} subset {sc.team | sc in set gp}
```

7.12 適用式

構文:

```
式 = ...
   | 適用
   | 項目選択
   | 組選択
   | 関数型インスタンス化
   | ... ;
```

適用 = 式, '(', [式リスト], ')' ;

項目選択 = 式, '.', 識別子 ;

組選択 = 式, '.#', 数値 ;

関数型インスタンス化 = 名称, '[', 型, { ',', 型 }, ']' ;

意味定義: 項目選択式 はレコードに対して用いることができるが、第 4.2.5 節ですでに説明したのでここではそれ以上の説明は行わない。適用 は、ある写像において検索を行い、列に索引をし、最後に関数を呼び出すために用いられる。第 4.2.3 節で、写像において検索を行うとはどういうことかはすでに述べてある。同様に第 4.2.2 節では、列に索引をするとはどのように行うのかが説明されている。

VDM++ においては、ここで更に 1 つの操作を呼び出すことが可能である。これは標準 VDM-SL においては許されていないことであり、この種の操作呼び出しは状態を変更してしまう可能性があるので、混合式においては慎重に使用されるべきである。このような操作呼び出しで例外を起こすことが許されてはいないことに注意したい。

このような操作呼出しでは評価の順が重要となる可能性がある。したがって型検査では、式の中でユーザーが操作呼出しを有効化や無効化することを許す。

組選択式は、組から特別な構成要素を抽出するために用いられる。式の意味は、 もし e がいくつかの組 mk_(v1,...,vN) であると評価され、 M が範囲 {1,...,N} 内の 1 つの整数であるならば、 e.#M は vM となるということである。M が {1,...,N} からはずれているならば、この式は未定義である。

関数型インスタンス化 は、適当な型をもつ多相関数のインスタンス生成に用いられる。これは次の形式をもつ:

```
pf [ t1, ..., tn ]
```

ここで pf は多相関数の名称であり、 t1, ..., tn は型である。結果の関数は、関数定義で与えられた変数型の名称の代わりに、型 t1, ..., tn を用いる。

例題: GroupA は 1 つの列 (59 ページ)、 GroupG は 1 つの写像 (60 ページ)、そして selection_sort は 1 つの関数 (47 ページ) であったことを思い起こそう:

```
GroupA(1)                          ≡  mk_Score(<Brazil>,2,0,1,6)
GroupG(<Romania>)                  ≡  mk_(2,1,0)
GroupG(<Romania>).#2               ≡  1
selection_sort([3,2,9,1,3])        ≡  [1,2,3,3,9]
```

多相関数使用と関数型インスタンス化の 1 つの例として、第 6 節から例題の関数を用いる:

```
let emptyInt = empty_bag[int] in
  plus_bag[int](-1, emptyInt())

≡

{ -1 |-> 1 }
```

7.13 new 式

構文:

式 = ...
| new 式 ;

new 式 = 'new', 名称, '(', [式リスト], ')' ;

意味定義: *new* 式は次の形式をもつ:

```
new classname(e1, e2, ..., en)
```

new 式を用いることで、クラス記述からオブジェクトを生成すること (これはまた**インスタンス生成**とも呼ばれる) が可能である。*new* 式による効果は、classname クラスに記述された他と識別できる新しいオブジェクトが生成されることである。*new* 式 の値は、新しいオブジェクトへの参照である。

new 式 がパラメーターなしで呼び出された場合は、中のすべてのインスタンス変数は “既定” 値 (i.e. それらの初期化条件で定義された値) をとった 1 つのオブジェクトが生成される。パラメーターありの場合には *new* 式 は **構成子** (第 12.1 を参照) に相当し、カスタマイズされたインスタンスを生成する (つまり ここでのインスタンス変数は既定値とは異なる値をとることも許される)。

例題: Queue という 1 つのクラスを仮定し、この既定インスタンスは空であるとする。またこのクラスは 1 つの構成子 (これもまた Queue と呼ばれる) を含み、これは単一のパラメーターをとりこれが任意のスタートキューを表す値のリストであるとする。このように仮定すると Queue の既定インスタンスを生成することができ、実際のキューは次の式を用いて空である

```
new Queue()
```

そして次の式を用いることで Queue の 1 つのインスタンスを生成することができるが、 ここにおいて実際のキューはたとえば e1, e2, e3 となる

```
new Queue([e1, e2, e3])
```

32 ページで定義されたクラス Tree を用いることで、 nodes を構成する新しい Tree インスタンスを生成する:

```
mk_node(new Tree(), x, new Tree())
```

7.14 self 式

構文:

式 = ...
| self 式 ;

self 式 = 'self' ;

意味定義: *self* 式は次の形式をもつ:

```
self
```

self 式は現在実行中のオブジェクトへの参照を返す。継承の連鎖における名前空間を単一化するために、用いることができる。

例題: 32 ページで定義された Tree クラス を用いることで、B 木検索アプローチを用いてデータを保存する BST と呼ばれるサブクラスを記述することができる。これにより、B 木検索挿入を実行する操作を指定することができる:

```
Insert : int ==> ()
Insert (x) ==
  (dcl curr_node : Tree := self;

   while not curr_node.isEmpty() do
     if curr_node.rootval() < x
     then curr_node := curr_node.rightBranch()
     else curr_node := curr_node.leftBranch();
   curr_node.addRoot(x);
   )
```

この操作は、挿入に先立ちそこから行き来するルートを見つけるため、self 式を用いる。更なる例題が第 13.9 に示される。

7.15 スレッド ID 式

構文:

式 = ...
| スレッド ID 式 ;

スレッド ID 式 = 'threadid' ;

意味定義: スレッド *ID* 式は次の形式をもつ:

```
threadid
```

スレッド ID 式は、その式が実行されているスレッドを一意に識別する自然数を返す。周期的なスレッドはそれぞれの周期の状態における新しいスレッド ID を得ることに注意する。

例題: スレッド ID を用いることで、許可述語を使って、VDM++に JAVA スタイルの wait-notify を実装する VDM++基本クラスを提供することが可能となる。この wait-notify 手法で利用できるオブジェクトはすべて、この基本クラスから派生するものでなければならない。

```
class WaitNotify

  instance variables
    waitset : set of nat := {};

  operations
    protected wait: () ==> ()
    wait() ==
      let p = threadid
      in (
        AddToWaitSet( p );
        Awake();
       );

    AddToWaitSet : nat ==> ()
    AddToWaitSet( p ) ==
      waitset := waitset union { p };

    Awake: () ==> ()
    Awake() ==
      skip;

    protected notify: () ==> ()
    notify() ==
        if waitset <> {} then
          let arbitrary_process in set waitset
          in  waitset := waitset \ {arbitrary_process};

    protected notifyAll: () ==> ()
    notifyAll() ==
         waitset := {};
```

```
  sync
    mutex(notifyAll, AddToWaitSet, notify);
    per Awake => threadid not in set waitset;

end WaitNotify
```

この例ではスレッド ID 式が 2 箇所で用いられている:

- スレッドに対する Wait 操作中に、このオブジェクトへの関心を記録するため。
- Awake に対する 許可述語中。関与するスレッドは、Wait を用いた記録を行った後に Awake を呼ぶべきである。そしてこのスレッドは、notify に対するもうひとつのスレッド呼出しの後、待ち集合からスレッド ID が取り除かれるまでブロックされる。

周期的なスレッドを持っているときは、wait-notify 構造の使用について注意する必要がある。(なぜなら、それぞれの新しい周期にたいしてスレッド ID が変化するからである)

7.16 ラムダ式

構文:

式 = ...
| ラムダ式
| ... ;

ラムダ式 = 'lambda', 型束縛リスト, '&', 式 ;

型束縛リスト = 型束縛, { ',', 型束縛 } ;

型束縛 = パターン, ':', 型 ;

意味定義: ラムダ式 は次の形式をもつ:

```
lambda pat1 : T1, ..., patn : Tn & e
```

ここで pati はパターン、Ti は型式、そして e は本体式である。パターン pati におけるパターン識別子のスコープが本体式である。ラムダ式は多相ではありえないが、それとは別に、意味定義においては第 6 節に説明される陽関数定義に相当する。ラムダ式によって定義される関数は、入れ子になった本体中で新しいラムダ式を用いることでカリー化することが可能となる。ラムダ式が 1 つの識別子と結びついたとき、再帰関数を定義することもまた可能である。

例題: 以下のようにラムダ式を用いて、増加関数を定義することができる:

```
Inc = lambda n : nat & n + 1
```

さらに加算関数はカリー化できる:

```
Add = lambda a : nat & lambda b : nat & a + b
```

もしこれが唯一の引数に適用された場合には、新しいラムダ式が返される:

```
Add(5) ≡ lambda b : nat & 5 + b
```

ラムダ式は、高階関数との関連で用いられる場合に役立つ。たとえば 46 ページに定義される関数 set_filter を用いてみると:

```
set_filter[nat](lambda n:nat & n mod 2 = 0)({1,...,10})
≡ {2,4,6,8,10}
```

7.17 is 式

構文:

式 = ...
| 一般 is 式
| ... ;

一般 is 式 = is 式
| 型判定 ;

```
is式 = 'is_', 名称, '(', 式, ')'
     | is基本型, '(', 式, ')' ;

is基本型 = 'is_', ( 'bool' | 'nat' | 'nat1' | 'int'
                  | 'rat' | 'real'
                  | 'char' | 'token' ) ;

型判定 = 'is_', '(', 式, ',', 型, ')' ;
```

意味定義: *is* 式 は基本値かまたはレコード値 (なにかのレコード型に属するタグ付けされた値) とともに用いられる。この is 式は、与えられた値が指定された基本型に属する場合、または値が指定されたタグを持つ場合に、true となる。他の場合は false となる。

型判定は、型が静的には決定されえない式に対して用いることができることから、より一般的な形式である。式 is_(e,t) は、 e が t 型 でありその場合にのみ、true となる。

例題: 28 ページに定義されたレコード型 Score を用いて次を得る:

```
is_Score(mk_Score(<France>,3,0,0,9))  ≡  true
is_bool(mk_Score(<France>,3,0,0,9))   ≡  false
is_real(0)                            ≡  true
is_nat1(0)                            ≡  false
```

型判定の例は以下のとおり:

```
Domain : map nat to nat | seq of (nat*nat) -> set of nat
Domain(m) ==
  if is_(m, map nat to nat)
  then dom m
  else {d | mk_(d,-) in set elems m}
```

加えて 31 にも例題が載せられている。

7.18 基底クラス構成要素

構文: 式 = ...

| isofbaseclass 式
| ... ;

isofbaseclass 式 = 'isofbaseclass', '(', 名称, 式, ')' ;

意味定義: isofbaseclass 関数がオブジェクト参照である式やクラス名である名称に適用されるときは、 式によって参照されるオブジェクトの継承連鎖において名称 が ルートスーパークラスで、かつその場合にのみブール値 true をとりその他の場合は false となる。

例題: BinarySearchTree が Tree のサブクラスであると仮定すると、Tree は他のクラスのサブクラスにはならないし、 Queue が Tree や BinarySearchTree に継承によって関係付けられることもない。t を Tree のインスタンス、 b を BinarySearchTree のインスタンス、 q を Queue のインスタンス、とすると次の通り:

```
isofbaseclass(Tree, t)              ≡ true
isofbaseclass(BinarySearchTree, b)  ≡ false
isofbaseclass(Queue, q)             ≡ true
isofbaseclass(Tree, b)              ≡ true
isofbaseclass(Tree, q)              ≡ false
```

7.19 クラス構成要素

構文

式 = ...
| isofclass 式
| ... ;

isofclass 式 = 'isofclass', '(', 名称, 式, ')' ;

意味定義: あるオブジェクト参照 式とクラス名 名称に適用された関数 isofclass は、式が 名称 クラスのオブジェクトまたは 名称クラスのいくつかのサブクラスのうちの 1 つのオブジェクトを参照しかつその場合にのみブール値 true をとり、それ以外の場合には false となる。

例題: 前の例と同様に、Tree,BinarySearchTree, Queue のクラスと、識別子 t,b, q を仮定する:

```
isofclass(Tree,t)                ≡ true
isofclass(Tree,b)                ≡ true
isofclass(Tree,q)                ≡ false
isofclass(Queue,q)               ≡ true
isofclass(BinarySearchTree,t)    ≡ false
isofclass(BinarySearchTree,b)    ≡ true
```

7.20 同基底クラス構成要素

構文:

```
式 = ...
   | samebaseclass 式
   | ... ;

samebaseclass 式 = 'samebaseclass',
                   '(', 式, 式, ')' ;
```

意味定義: オブジェクト参照 expression1 と expression2 に適用された関数 samebaseclass は、 expression1 と expression2 によって記述されたオブジェクトが同じルートスーパークラスから派生し得たクラスのインスタンスでありかつその場合にのみにブール値 true をとり、それ以外の場合は false となる。

例題: 前に述べた例題と同様に、クラス Tree、BinarySearchTree, Queue, および識別子 t,b, q を仮定し、AVLTree を Tree のもうひとつのサブクラス、BalancedBST を BinarySearchTree のサブクラス、 a を AVLTree のインスタンス、そして bb を BalancedBST のインスタンスとする:

```
samebaseclass(a,b)    ≡ true
samebaseclass(a,bb)   ≡ true
samebaseclass(b,bb)   ≡ true
samebaseclass(t,bb)   ≡ false
samebaseclass(q,a)    ≡ false
```

7.21 同クラス構成要素

構文:

```
式 = ...
   | sameclass 式
```

| ... ;

sameclass 式 = 'sameclass',
'(', 式, 式, ')' ;

意味定義: オブジェクト参照 expression1 と expression2 に適用される関数 sameclass は、expression1 と expression2 により記述されたオブジェクトが同じクラスのインスタンスとなりかつその場合にのみブール値 true をとり、それ以外の場合は false となる。

例題: 第 7.18 節においてのクラス Tree、BinarySearchTree、 Queue、そして識別子 t、b、 q を仮定し、さらに b' が BinarySearchTree のもうひとつのインスタンスであると仮定した場合、次が得られる:

```
sameclass(b,t)    ≡ false
sameclass(b,b')   ≡ true
sameclass(q,t)    ≡ false
```

7.22 履歴式

構文:

式 = ...
| act 式
| fin 式
| active 式
| req 式
| waiting 式
| ... ;

act 式 = '#act', '(', 名称, ')'
| '#act', '(', 名称リスト, ')' ;

fin 式 = '#fin', '(', 名称, ')'
| '#fin', '(', 名称リスト, ')' ;

active 式 = '#active', '(', 名称, ')'
| '#active', '(', 名称リスト, ')' ;

req 式 = '#req', '(', 名称, ')'
| '#req', '(', 名称リスト, ')' ;

waiting 式 = '#waiting', '(', 名称, ')'
| '#waiting', '(', 名称リスト, ')' ;

意味定義: 履歴式は許可述語においてのみ用いられる (第 15.1 節参照)。履歴式は以下の式を 1 つ以上含むことが許される:

- `#act` (**操作名**) **操作名** 操作が起動された回数。
- `#fin`(**操作名**) **操作名**操作が完了した回数。
- `#active`(**操作名**) 現在起動中である**操作名**操作の数。このとき: `#active`(**操作名**) = `#act`(**操作名**) - `#fin`(**操作名**)
- `#req`(**操作名**) **操作名** 操作に対して発生した要求の数。
- `#waiting`(**操作名**) **操作名**操作に対する未解決の要求の数。このとき: `#waiting`(**操作名**) = `#req`(**操作名**) - `#act`(**操作名**)

これらすべての演算子に対して、名前リスト版である#*history op(op1,...,opN)* は #*history op(op1)* + ··· +#*history op(opN)* に対する簡易な省略形である。

例題: 3 つの操作 A, B そして C が実行されるある特別なスレッドの実行における 1 時点を想定しよう。要求、起動、完了、の列がこのスレッド中で起こる。このことは図 1 において視覚的にみてとれる。

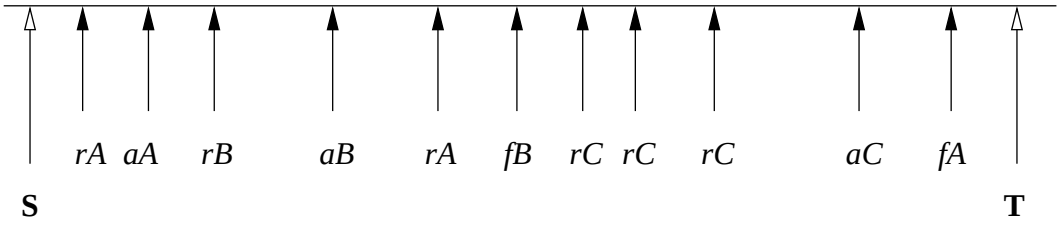

図 1: **履歴式**

ここに記号 *rA* を操作 A の実行要求を示すものとして用い、 *aA* は A の起動を示すもの、 *fA* は操作 A の実行の完了を示すものとし、そして同様のことを操作 B と C に対しても用いる。各々の履歴式は、 時間間隔 [**S**,**T**] に対するものとしての以下の値をとる:

```
#act(A) = 1      #act(B) = 1      #act(C) = 1      #act(A,B,C) = 3
#fin(A) = 1      #fin(B) = 1      #fin(C) = 0      #fin(A,B,C) = 2
#active(A) = 0   #active(B) = 0   #active(C) = 1   #active(A,B,C) = 1
#req(A) = 2      #req(B) = 1      #req(C) = 3      #req(A,B,C) = 6
#waiting(A) = 1  #waiting(B) = 0  #waiting(C) = 2  #waiting(A,B,C) = 3
```

7.23 time 式

構文: time 式 = 'time' ;

意味定義: これは単純に、与えられた CPU 上の現在の時間を問い合わせるものである。時間は自然数で提供されます。

例: たとえば、確実にある操作が実行されたことをログ（記録）に取りたい場合、logEnvToSys のようにして操作を作成することができる。

```
public logEnvToSys: nat ==> ()

logEnvToSys (pev) == e2s := e2s munion {pev |-> time};
```

7.24 リテラルと名称

構文:

式 = ...
| 名称
| 旧名称
| 記号リテラル
| ... ;

名称 = 識別子, ['‘', 識別子] ;

名称リスト = 名称, { ',', 名称 } ;

旧名称 = 識別子, '~' ;

意味定義: 名称 と 旧名称 は、関数、操作、値、状態構成要素の定義にアクセスするためによく用いられる。名称 は次の形式をもつ:

```
id1‘id2
```

ここで id1 と id2 は単なる識別子である。名称が唯一の識別子で構成される場合は、その識別子はスコープ内で定義されている。つまり、ローカルにパターン識別子かパターン変数として定義されているか、あるいはグローバルに現モジュール内で関数、操作、値、またはグローバル変数として定義されているか、いずれかである。そうでない場合は、識別子 id1 がコンストラクタが定義されている場所のクラス名を示している (第 14.2 節および付録 B も参照)。旧名称 は、操作定義の事後条件 (第 12 節参照) および仕様文の事後条件 (第 13.15 節参照) において、グローバル変数の旧値にアクセスするためによく用いられる。これは次の形式をもつ:

```
id~
```

ここで id は状態構成要素である。

記号リテラル はいくつかの基本型における定数値である。

例題: 名称 と 記号リテラル はこの本の中ですべての例題を通して用いられている (付録 B.2 参照)。

旧名称の使用例として、以下のように定義されたインスタンス変数を考えてみよう:

```
instance variables
  numbers: seq of nat := [];
  index  : nat := 1;
inv  index not in set elems numbers;
```

変数 index を増加させる陰操作を定義することができる:

```
IncIndex()
ext wr index : nat
post index = index~ + 1
```

操作 IncIndex は、ext wr 節に示されるように、変数 index を操作する。事後条件の中で、 index の新しい値は index の旧値に 1 を足したものと等しい。(これ以上は第 12 節の操作についてを参照)。

クラス名の簡単な例としては、以下のように、 build_rel という関数が CGRel というクラスにおいて定義された (そしてエクスポートされた) と仮定する:

```
types

  Cg = <A> | <B> | <C> | <D> | <E> | <F> |
       <G> | <H> | <J> | <K> | <L> | <S>;
  CompatRel = map Cg to set of Cg

functions

  build_rel : set of (Cg * Cg) -> CompatRel
  build_rel (s) == {|->}
```

別のクラスにおいては、それから、以下の呼出しを行なうことでこの関数をアクセスすることができる

```
CGRel`build_rel(mk_(<A>, <B>))
```

7.25 未定義式

構文: 式 = ...
| 未定義式 ;

未定義式 = 'undefined' ;

意味定義: 未定義式 は、ある式の結果が定義されないことを明白に述べるために用いられる。たとえばこれは、if-then-else 式で else 分岐を評価した結果をどうすべきかが決定されていない場合などに、用いることができるであろう。未定義式 が評価される場合、インタプリタは実行を終了し未定義式が評価されたと記録する。

実用において、未定義式の使用は事前条件のとは異なる: 事前条件の使用とは、関数が呼ばれたときに事前条件が満たされることを保障するのは呼び出す側の責任であることを意味する; 未定義式の使用であれば、エラー処理を行うのは呼び出された関数の責任となる。

例題: Score 値の build の前に、型の不変条件が保たれるかをチェックすることができる:

```
build_score : Team * nat * nat * nat * nat -> Score
build_score (t,w,d,l,p) ==
  if 3 * w + d = p
  then mk_Score(t,w,d,l,p)
  else undefined
```

7.26 事前条件式

構文:

式 = ...
| 事前条件式 ;

事前条件式 = 'pre_', '(', 式,
[{ ',', 式 }], ')' ;

意味定義: e が関数型であると仮定すると、 式 pre_(e,e1,...,en) は、e の事前条件が引数 e1,...,em に対して true でありかつその場合にのみ true となるが、ここで m は e の事前条件の arity(引数の数) である。e が関数でなかったり、 m > n であったりした場合は、結果は true となる。e が事前条件をもたない場合は、式は true と等しい。

例題: 以下のように定義された関数 f と g を考えよう

```
f : nat * nat -> nat
f(m,n) == m div n
pre n <> 0;

g (n: nat) sqrt:nat
pre n >= 0
```

```
post sqrt * sqrt <= n and
     (sqrt+1) * (sqrt+1) > n
```

この場合、次の式は

```
pre_(let h in set {f,g, lambda mk_(x,y):nat * nat & x div y}
     in h, 1,0,-1)
```

以下と等しくなる

- h が f に束縛されている場合は pre_f(1,0) と等しいと考えられるため、false となる;
- h が g に束縛されている場合は pre_g(1) と等しいと考えられるため、true となる;
- h が lambda mk_(x,y):nat * nat & x div y に束縛されている場合はこの関数に対して定義された事前条件がないため、 true となる。

h がいかに束縛されていたとしても、最後の引数 (-1) は決して使われないことに注意しよう。

8 パターン

構文: パターン束縛 = パターン | 束縛 ;

パターン = パターン識別子
| 一致値
| 集合列挙パターン
| 集合合併パターン
| 列列挙パターン
| 列連結パターン
| 組パターン
| レコードパターン ;

パターン識別子 = 識別子 | '-' ;

一致値 = 記号リテラル
| '(', 式, ')' ;

集合列挙パターン = '{', [パターンリスト], '}' ;

集合合併パターン = パターン, 'union', パターン ;

列列挙パターン = '[', [パターンリスト], ']' ;

列連結パターン = パターン, '^', パターン ;

組パターン = 'mk_(', パターン, ',', パターンリスト, ')' ;

レコードパターン = 'mk_', 名称, '(', [パターンリスト], ')' ;

パターンリスト = パターン, { ',', パターン } ;

意味定義: パターンは常に文脈中で用いられ、1 つの特定の型の 1 つの値に一致する。マッチングでは、あるパターンがある値と一致する可能性があるかの照合を行い、そしてパターン中のパターン識別子に対応する値を結びつけ、識別子がそのスコープ内で、これらの値を意味するようにする。パターンを用いることのできるいくつかの場合においては、束縛も同様に用いることができる (次節を参照)。もし束縛が用いられていたら、それは単純に言って、与えられたパターンに一致する可能性のある値を束縛することに更なる情報 (型式または集合式) が用いられていることを意味する。

マッチングは次のように定義される

1. パターン識別子 はどんな型にも合致するしどんな値にも一致し得る。それが識別子であるならば、その識別子はその値に束縛される; それが don't-care 記号 '-' であるならば、どのような束縛も起こらない。
2. 一致値 はそれ自身の値に対してのみ一致し得る; どのような束縛もなされない。一致値がたとえば 7 とか <RED>とかのようにリテラルでない場合は、パターン識別子に対してこれを区別するために、括弧にかこまれた式でなければならない。
3. 集合列挙パターン は集合値のみと適合する。1 つ 1 つのパターンは 1 つの集合の異なる要素と一致させられ; すべての要素が一致しなければならない。

4. 集合合併パターン は集合値のみと適合する。1 つの集合における区分けされた 2 つの部分集合に対しては、2 つのパターンが一致する。Toolbox 中では、2 つの部分集合は常に双方とも空でなく、互いに素であるであるように選択されるであろう。
5. 列列挙パターン は唯一列値にのみ合致する。各々のパターンは列値中の対応する要素に対して一致させられる; 列長とパターン数は等しくなければならない。
6. 列連結パターン は唯一列値とのみ合致する。2 つのパターンは、共に連結するともとの列値をつくることができる 2 つの部分列に対して、一致させるものである。Toolbox においては、2 つの部分列は常に空ではないように選ばれるであろう。
7. 組パターン は同じ要素数をもつ組にのみ合致する。パターンの各々は、組値の中で対応する要素に対して一致させられる。
8. レコードパターン は同じタグをもつレコード値にのみ適合する。パターンの各々は、レコード値の項目に対して一致させられる。レコードのすべての項目が一致させられなくてはならない。

例題: 最も単純なパターンはパターン識別子である。この例は次に述べる let 式で与えられる:

```
let top = GroupA(1)
in top.sc
```

ここで識別子 top は列 GroupA の先頭と結びつき、したがって識別子は let 式の本体で用いられることが許される。

以下の例では一致値を用いる:

```
let a = <France>
in cases GroupA(1).team:
            <Brazil> -> "Brazil are winners",
            (a)      -> "France are winners",
            others   -> "Neither France nor Brazil are winners"
   end;
```

一致値は唯一それ自身の値と一致させることが可能なので、ここで GroupA の先頭のチームが <Brazil> であるならば最初の節で一致する; もし GroupA

の先頭のチームが<France> であるなら 2 番目の節で一致する。これら以外は others が一致する。ここで a を囲んだ括弧の使用が、a を一致値とみなすよう強要していることに留意しよう。

集合列挙は、パターンを 1 つの集合の要素と一致させる。たとえば次において

```
let {sc1, sc2, sc3, sc4} = elems GroupA
in sc1.points + sc2.points + sc3.points + sc4.points;
```

識別子 sc1, sc2, sc3 および sc4 は GroupA の 4 つの要素と結び付けられる。束縛の選択はゆるいものであることに注目しよう - たとえば sc1 は elemsGroupA の [どのような] 要素と結び付いてもよい。この場合、もし elems GroupA がちょうど 4 つの要素を含んでいるわけではなかったら、この式は良形とはいえない。

集合合併パターンは、集合を再帰関数呼出しに分解させるために用いることができる。この 1 つの例は集合を (任意の順での) 列に変換する関数 set2seq である:

```
set2seq[@elem] : set of @elem -> seq of @elem
set2seq(s) ==
  cases s:
    {} -> [],
    {x} -> [x],
    s1 union s2 -> (set2seq[@elem](s1))^(set2seq[@elem](s2))
  end
```

case の 3 番目の選択肢で、集合合併パターンを使用しているのがわかる。これは s1 と s2 を s の任意の部分集合に束縛し、それによって s を区分けする。Toolbox インタープリタは常に互いに素の区分けを実現する。

列列挙パターンは、1 つの列から指定された要素を抽出するために用いることができる。この 1 つの例として関数 promoted があり、これはスコアの列の最初から 2 つの要素を抽出し、チームの中の対応する 2 つを返す:

```
promoted : seq of Score -> Team * Team
promoted([sc1,sc2]^-) == mk_(sc1.team,sc2.team);
```

ここで sc1 は引数列の先頭と結びつき、sc2 は列の 2 番目の要素と結びつく。もし promoted が要素数が 2 つない列で呼び出されるなら、ランタイムエラーが起きる。リストの残りの要素には興味を持たないので、それら残りに対して don't care パターンを用いていることに注目したい。

前に述べた例でも、列連結パターンの使用を行っている。もうひとつの例として関数 quicksort があるが、これは標準のクイックソートアルゴリズムを実装している:

```
quicksort : seq of nat -> seq of nat
quicksort (l) ==
  cases l:
    [] -> [],
    [x] -> [x],
    [x,y] -> if x < y then [x,y] else [y,x],
    -^[x]^- -> quicksort ([y | y in set elems l & y < x]) ^
               [x] ^ quicksort ([y | y in set elems l & y > x])
  end
```

ここで、 第 2 のケース節で列連結パターンは l をある任意のピボット (かなめ) 要素と 2 つの部分列に分解するのに用いられている。ピボットはリストをピボットより小さい値と大きい値に区分けるために用いられ、2 つの区分けされた部分は再帰的にソートされる。

組パターンは、組構成要素を識別子と結びつけるために用いることができる。たとえば上で定義された関数 promoted は 2 つを返すので、以下の値定義では GroupA の勝ったチームの方を識別子 Awinner に結びつける:

```
values

  mk_(Awinner,-) = promoted(GroupA);
```

レコードパターンはレコードのいくつかの項目が同じ式で用いられるときに役立つ。たとえば次に述べる式は、チーム名から点数スコアへの写像を構成する:

```
{ t |-> w * 3 + l | mk_Score(t,w,l,-,-) in set elems GroupA}
```

52 ページの関数 print_Expr もまた、レコードパターンのいくつかの例を与えてくれる。

9 束縛

構文: 束縛 = 集合束縛 | 型束縛 ;

集合束縛 = パターン, 'in set', 式 ;

型束縛 = パターン, ':', 型 ;

束縛リスト = 多重束縛, { ',', 多重束縛 } ;

多重束縛 = 多重集合束縛
| 多重型束縛 ;

多重集合束縛 = パターンリスト, 'in set', 式 ;

多重型束縛 = パターンリスト, ':', 型 ;

意味定義: 束縛は、あるパターンをある値に一致させる。集合束縛 において、値は束縛の集合式によって定義された集合から選ばれる。型束縛 において、値は型式で定義された型から選ばれる。多重束縛は、いくつかのパターンが同じ集合または型に束縛されることを除けば 束縛 と同じである。型束縛はインタープリタで実行させることは **できない** ことに注意しよう。これは、インタープリタに自然数というような無限の定義域の検索を要求するということであるからだ。

例題: 束縛は主に、これらの例にみられるように限量式や内包で用いられる:

```
forall i, j in set inds list & i < j => list(i) <= list(j)

{ y | y in set S & y > 2 }

{ y | y: nat & y > 3 }

occurs : seq1 of char * seq1 of char -> bool
occurs (substr,str) ==
  exists i,j in set inds str & substr = str(i,...,j);
```

10 値 (定数) 定義

VDM++ では定数値の定義をサポートする。値定義については、伝統的プログラム言語における定数定義に相当する。

構文: 値定義群 = 'value', [アクセス値定義,
{ ';', アクセス値定義 }, [';']] ;

アクセス値定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
値定義 ;

値定義 = パターン, [':', 型], '=', 式 ;

意味定義: 値定義は次の形式をもつ:

```
values
  access pat1 = e1;
  ...
  access patn = en
```

グローバル値 (値定義で定義された) は、 VDM++ 記述の全水準で参照が可能である。しかしながら、1 つの記述が実行可能であるためには、値定義の列に用いられる前段階でそれらの値は定義されていなければならない。この "使用前の宣言" 原則は、インタープリタが値定義にのみ使う。このことはたとえば、関数などは宣言される前に用いられることが可能なのである。標準 VDM-SL では、定義の順番における制限はいっさい存在しない。同様に型制限を提供することが可能であるから、このことでより正確な型情報を得るのに役立てることができる。

アクセスおよび static 記述子の詳細は、第 14.4 節で述べられる。

例題: 以下の例は [FJ98] からとったものであるが、識別子 `p1` と `eid2` にトークン値を与え、`e3` に `Expert` レコード値を与え、そして `a1` に `Alarm` レコード値を与える。

```
types
```

```
Period = token;
ExpertId = token;
Expert :: expertid : ExpertId
          quali : set of Qualification
inv ex == ex.quali <> {};
Qualification = <Elec> | <Mech> | <Bio> | <Chem>;
Alarm :: alarmtext : seq of char
         quali : Qualification

values

public p1: Period = mk_token("Monday day");
private eid2 : ExpertId = mk_token(145);
protected e3 : Expert = mk_Expert(eid2,  <Mech>, <Chem> );
 a1 : Alarm = mk_Alarm("CO2 detected", <Chem>)
```

この例が示すように、ある値はそれ自身が定義される前に定義された他の値に依存できる。

11 インスタンス変数

クラス定義からインスタンス化されたオブジェクトとそのクラス自身の両者で、1つの内部状態を持つことができ、それはまたオブジェクトまたはクラスの **インスタンス変数** と呼ばれる。オブジェクトの場合には、この状態をまたオブジェクトのグローバル状態として参照する。

構文:

インスタンス変数定義群 = 'instance', 'variables',
[インスタンス変数定義,
{ ';', インスタンス変数定義 }] ;

インスタンス変数定義 = アクセス指定定義
| 不変条件定義 ;

アクセス指定定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
指定定義 ;

指定定義 = 識別子, ':', 型, [':=', 式] ;

不変条件定義 = 'inv', 式 ;

意味定義: 内部状態の記述する節に先立ち、 `instance variables` というキーワードが必要である。インスタンス変数定義と不変条件定義のリストは以下にある。各々のインスタンス変数定義は、対応する型指定をともなうインスタンス変数名からなり、そこには初期値とアクセスおよび static 指定子を含めることもある。アクセスおよび static 指定子についての詳細は、第 14.4 節にみることができる。

不変条件定義の方法により、インスタンス変数の値を制限することが可能である。各々の不変条件定義は、1 つ以上のインスタンス変数を含み、クラスオブジェクトのインスタンス変数の値上で定義される可能性もある。スーパークラスから継承されるものを含むクラスにあるすべてのインスタンス変数は、不変条件式で使用することができる。各不変条件定義は、式が true となるようにインスタンス変数の値を制限するブール式でなければならない。すべての不変条件式は、そのクラスの各々のオブジェクトの全存在期間で true となる必要がある。

あるクラスの全てにわたる不変条件式というのは、そのクラスおよびその複数のスーパークラスの不変条件定義のすべてが、まずは 1) 複数のスーパークラス、次は 2) そのクラス自身、の中で定義された順に論理 and で結合されたものである。

この操作はプライベートのものであり、パラメーターはもたず、不変条件式の実行に対応し 1 つのブール値を返す。

例題: 以下の例はインスタンス変数定義を示している。このクラスでは 1 つのインスタンス変数が詳しく述べられる:

```
class GroupPhase

types

  GroupName = <A> | <B> | <C> | <D> | <E> | <F> | <G> | <H>;
  Team = ... -- as on page 28
  Score::team : Team
         won : nat
         drawn : nat
```

```
            lost : nat
            points : nat;


instance variables
  gps : map GroupName to set of Score;
inv forall gp in set rng gps &
       (card gp = 4 and
        forall sc in set gp & sc.won + sc.lost + sc.drawn <= 3)

end GroupPhase
```

12 操作定義

操作については第 5 節にすでに述べてきた。一般的な形式はすぐ次に述べるが、クラスのインスタンス構成に用いられる**構成子** と呼ばれる特別な操作については 第 12.1 節に記述する。

構文:

操作定義群 = 'operations', [アクセス操作定義,
{ ';', アクセス操作定義 }, [';']] ;

アクセス操作定義 = (['async'] [アクセス], ['static'])
| (['async'] ['static'], [アクセス]),
操作定義 ;

操作定義 = 陽操作定義
| 陰操作定義
| 拡張陽操作定義 ;

陽操作定義 = 識別子, ':', 操作型,
識別子, パラメーター群,
'==',
操作本体,
['pre', 式],
['post', 式] ;

陰操作定義 = 識別子, パラメーター型,
[識別子型ペアリスト],
陰操作本体 ;

陰操作本体 = [外部節],
['pre', 式],
'post', 式,
[例外] ;

拡張陽操作定義 = 識別子,
パラメーター型,
[識別子型ペアリスト],
'==', 操作本体,
[外部節],
['pre', 式],
['post', 式],
[例外] ;

操作型 = 任意の型, '==>', 任意の型 ;

任意の型 = 型 | '()' ;

パラメーター群 = '(', [パターンリスト], ')' ;

パターンリスト = パターン, { ',', パターン } ;

操作本体 = 文
| 'is not yet specified'
| 'is subclass responsibility' ;

外部節 = 'ext', var 情報, { var 情報 } ;

var 情報 = モード, 名称リスト, [':', 型] ;

モード = 'rd' | 'wr' ;

名称リスト = 識別子, { ',', 識別子 } ;

例外 = 'errs', エラーリスト ;

エラーリスト = エラー, { エラー } ;

エラー = 識別子, ':', 式, '->', 式 ;

意味定義: VDM での操作はデフォルトの同期単位であるが、キーワード "async" が操作定義の前で使用されると、それは、操作が非同期操作として扱われることを意味する。これは、非同期操作の呼び出しを要求をされた後に、操作が戻り型を持つことが出来ず、非同期操作と呼ばれるスレッドが自身の実行を続けることを意味する。

※コンストラクタを非同期であると宣言できないことに注意してください。

アクセスと static 指定子の詳細については、第 14.4 節に求められる。静的操作では静的でない操作や関数を呼ぶことは許されていないし、self 式を静的操作の定義に用いることはできない、ということは注意しよう。

陽操作の以下の例は、1 つのチームがもうひとつを打ち負かす場合に GroupPhase クラスのインスタンス変数を更新する。

```
Win : Team * Team ==> ()
Win (wt,lt) ==
  let gp in set dom gps be st
        {wt,lt} subset {sc.team | sc in set gps(gp)}
  in gps := gps ++ { gp |->
                        {if sc.team = wt
                         then mu(sc, won |-> sc.won + 1,
                                     points |-> sc.points + 3)
                         else if sc.team = lt
                         then mu(sc, lost |-> sc.lost + 1)
                         else sc
                    | sc in set gps(gp)}}
  pre  exists gp in set dom gps &
         {wt,lt} subset {sc.team | sc in set gps(gp)};
```

1 つの陽操作は 1 つの文 (あるいは 1 つのブロック文を用いてまとめられたいくつかの文) からなるが、これについては第 13 節で述べられている。文は、必要とするどのようなインスタンス変数に対しても、適当と判断したときに読込みや書出しを行いアクセスすることが許されている。

陰操作は、オプションである事前条件、または必要不可欠な事後条件を用いて指定される。たとえば、ここに暗黙に陰操作 Win を指定できる:

```
Win (wt,lt: Team)
ext wr  gps : map GroupName to set of Score
pre  exists gp in set dom gps &
        {wt,lt} subset {sc.team | sc in set gps(gp)}
post  exists gp in set dom gps &
       {wt,lt} subset {sc.team | sc in set gps(gp)}
       and gps = gps~ ++
                    { gp |->
                      {if sc.team = wt
                       then mu(sc, won |-> sc.won + 1,
                                   points |-> sc.points + 3)
                       else if sc.team = lt
                       then mu(sc, lost |-> sc.lost + 1)
                       else sc
                  | sc in set gps(gp)}};
```

外部節の項目は、操作が扱うはずのインスタンス変数をリストする。予約語である rd の後にリストされたインスタンス変数は読み取りのみができるが、その一方 wr の後にリストされた変数は読みとり書きだしの両方行うことができる。

例外節は、ある操作がエラー状態にどのように対処するかを記述をすることに用いることができる。理論的根拠を持つための例外節は、正常なケースと例外ケースを切り離す分離することを可能にする。例外を用いた記述では、どのように例外を起こすかについて言及はしていないが、どのような環境でエラー状態が起こり得るか、また操作を呼び出した結果どのような影響が起きるかについて示す手段が与えられる。

例外節は次の形式をもつ:

```
errs COND1: c1 -> r1
     ...
     CONDn: cn -> rn
```

条件名 COND1, . . . , CONDn は識別子で、起きる可能性があるエラーの種類を記述する[15]。条件式 c1, . . . , cn は、異なる種類のエラーに対する事前条件と考えることができる。このようにこれらの式においては、引数リストか

[15] これらの名前は単に記憶を助けてくれる値であり、つまり意味定義上は重要でない。

ら識別子をまた外部節リストからは変数を用いることができる (それらは事前条件と同じスコープをもつ)。結果の式である r1,. . . , rn は相対的にみれば、異なる種類のエラーに対する事後条件と同じと考えられる。これらの式においては、結果の識別子とグローバル変数 (書き込みのできる) の旧値もまた用いることができる。このように、ここでのスコープは事後条件のスコープに相当する。

表面的には、ここでの例外と事前条件との間にはいくらか重複があるようにみえる。しかしながらこれらの間には、どちらをいつ用いるべきか指し示す概念的な違いが存在する。事前条件は、その操作の呼び出しが正しく行なわれるためにどんなことを保証しなければならないかを指定する; 例外節は、例外条件が満たされたときに記述された操作がエラー処理の責任をとることを示す。したがって通常は、例外節と事前条件は重複しない。

次のある操作例では、後に続くインスタンス変数定義を用いる:

```
instance variables
  q : Queue
end
```

この例では、陰操作の例外がどのように用いられるか示される:

```
DEQUEUE() e: [Elem]
ext wr q : Queue
post q~ = [e] ^ q
errs QUEUE_EMPTY: q = [] -> q = q~ and e = nil
```

これはデキュー操作であって、 型 Queue の グローバル変数 q を用いて、キューから型 Elem の 要素 e をとりのぞく。ここでの例外としては、その中で例外節が操作がどのように行われるかを指定するキューが、空である場合がある。

12.1 構成子

構成子は操作であって、それ自身が中で定義されたクラスと同じ名前をもち、このクラスの新しいインスタンスをつくるものである。このため戻り値の型は、そ

の同じクラス名でなければならず、戻り値が指定されるならば self となるべきであるが、これはオプションで省略可能である。

第 14.2 節で述べられるが、オーバーロードする操作を用いた単一クラスで、多重構成子の定義が可能である。

13 文

この章では、異なる種類の文を 1 種類ごとに記述する。各々は、次の方法で記述されていく:

- BNF 構文記法。
- 形式的でない意味定義記述。
- 使用例を 1 つ。

13.1 let 文

構文:

```
文 = let 文
  | let be 文
  | ... ;

let 文 = 'let', ローカル定義, { ',', ローカル定義 },
         'in', 文 ;

let be 文 = 'let', 束縛, [ 'be', 'st', 式 ], 'in',
            文 ;

ローカル定義 = 値定義
             | 関数定義 ;

値定義 = パターン, [ ':', 型 ], '=', 式 ;
```

ここでの構成要素である “関数定義” は第 6 節に記述されている。

意味定義: *let*文 と *let-be-such-that*文 は、*in*の部分が式であるかわりに文であることを除けば、各々がそれぞれ *let* と *let-be-such-that*式 に対応し似ている。これは以下のように説明することができる:

単純な *let*文 は次の形式をもつ:

```
let p1 = e1, ..., pn = en in s
```

ここで p1, ..., pn はパターン、e1, ..., en は対応するパターンである pi に一致する式、そして s は任意の型の文であるが p1, ..., pn というパターン識別子を含む。これは、パターン p1, ..., pn が式 e1, ..., en に対して一致する文脈中での、文 s の評価を示す。

ローカル関数定義を用いることで、より高度な let 文をつくることもできる。これを行う意味定義は単純で、このようなローカルに定義された関数のスコープは let 文の本体に制限される。

*let-be-such-that*文は次の形式をもつ

```
let b be st e in s
```

ここで b は束縛であって集合値 (または型) に対するパターンからなり、 e はブール式、 そして s は文であって b におけるパターンのパターン識別子を含むものである。be st e の部分はオプションである。この式は、b からの集合 (または型) の要素に対し b からのパターンが一致する文脈中での、文 s の評価を示すものである[16]。be st 式である e が存在するとき、唯一このような束縛が、一致させる文脈中で e が真と評価される場所で用いられる。

例題: let be st 文の 1 つの例は、クラス GroupPhase の操作 GroupWinner 中にあり、あるグループ内での勝チームを返してくれるものである:

```
GroupWinner : GroupName ==> Team
GroupWinner (gp) ==
  let sc in set gps(gp) be st
     forall sc' in set gps(gp) \ {sc} &
        (sc.points > sc'.points) or
```

[16]集合束縛のみがインタープリタで実行できるということを思い出そう。

```
        (sc.points = sc'.points and sc.won > sc'.won)
  in return sc.team
```

仲間の操作である GroupRunnerUp もまた同様に、簡単な let 文の例を与えてくれる:

```
GroupRunnerUp_expl : GroupName ==> Team
GroupRunnerUp_expl (gp) ==
  def t = GroupWinner(gp)
  in let sct = iota sc in set gps(gp) & sc.team = t
    in
      let sc in set gps(gp) \ {sct} be st
        forall sc' in set gps(gp) \ {sc,sct} &
          (sc.points > sc'.points) or
          (sc.points = sc'.points and sc.won > sc'.won)
      in return sc.team
```

ここにおける def 文 (第 13.2 節参照) の使用に注意; 右辺が操作呼出しであるために let 文ではなくこれを用いるが、したがってこれは式ではない。

13.2 def文

構文:

文 = ...
| def文
| ... ;

def文 = 'def', 相等定義,
{ ';', 相等定義 },[';'], 'in',
文 ;

相等定義 = パターン束縛, '=', 式 ;

意味定義: *def*文 は次の形式をもつ:

```
def  pb1 = e1;
     ...
     pbn = en
in
  s
```

def 文 は、 右辺において操作呼出しを用いることが許される点を除けば *def* 式に相当するものである。このような、状態を変化させる操作もここで用いることができ、またもし複数の定義がなされている場合には、出現した順に評価が行われる。このことは、パターン (または束縛)pb1, ..., pbn が対応する式や演算呼出し e1, ..., en によって返される値と一致する文脈中の文 s の評価の外延を表す[17]。

例題: 以下の列が与えられている:

```
secondRoundWinners = [<A>,<B>,<C>,<D>,<E>,<F>,<G>,<H>];
secondRoundRunnersUp = [<B>,<A>,<D>,<C>,<F>,<E>,<H>,<G>]
```

GroupPhase クラスからの操作 SecondRound は組の列を返し、第 2 ラウンドゲームが def 文の例を与えていることを表わす:

```
SecondRound : () ==> seq of (Team * Team)
SecondRound () ==
def winners = { gp |-> GroupWinner(gp) | gp in set dom gps };
    runners_up = { gp |-> GroupRunnerUp(gp) | gp in set dom gps}
in return ([mk_(winners(secondRoundWinners(i)),
                runners_up(secondRoundRunnersUp(i)))
          | i in set {1,...,8}])
```

13.3 ブロック文

構文: 文 = ...

[17]束縛が用いられるのであれば第 8 節で説明されるように、パターンと一致し得る値はさらに型や集合式により束縛がなされることを単純に意味する。

```
    |   ブロック文
    |   ... ;

ブロック文 = '(', { dcl 文 },
             文, { ';', 文 }, [ ';' ], ')' ;

dcl 文 = 'dcl', 代入定義,
         { ',', 代入定義 }, ';' ;

代入定義 = 識別子, ':', 型, [ ':=', 式 ] ;
```

意味定義: ブロック文は、伝統的な高水準プログラム言語におけるブロック文に相当する。ブロック文を用いることで、(宣言文を使用して) ブロック文の本体内での変更が許されたローカル定義変数の使用が可能となる。これは単に、個々の文が規定することを順に実行することを示すものである。文の列において 1 つの値を返す最初の文により、文の列を終了させるための評価がひき起こされる。この値はブロック文の値として返される。ブロック内のどの文も値を返さない場合には、ブロック文の評価はブロック内の最後の文が評価されたときに終了する。ブロック文が中止された場合には、ローカル変数の値は開放される。このように、これら変数のスコープは単純にブロック文の内部である。

例題: 次のようなインスタンス変数

```
instance variables
  x:nat;
  y:nat;
  l:seq1 of nat;
```

に関連したものとしてここに述べる Swap 操作は、変数 x と y の値交換を行うためにブロック文を用いる:

```
Swap : () ==> ()
Swap () ==
  (dcl temp: nat := x;
   x := y;
   y := temp
  )
```

13.4 代入文

構文:

文 = ...
| 一般代入文
| ... ;

一般代入文 = 代入文
| 多重代入文 ;

代入文 = 状態指示子, ':=', 式 ;

状態指示子 = 名称
| 項目参照
| 写像参照または列参照 ;

項目参照 = 状態指示子, '.', 識別子 ;

写像参照または列参照 = 状態指示子, '(', 式, ')' ;

多重代入文 = 'atomic', '(' 代入文, ';',
代入文,
{ ';', 代入文 }')' ;

意味定義: 代入文 は、伝統的な高水準プログラム言語における代入文を一般化したものに相当する。これを用いてグローバル状態またはローカル状態の値を変更する。したがって代入文は、状態を変える副作用を起こす。しかしながら、単純にある状態の一部を変更することができるように、代入文の左辺を状態指定子とすることができる。状態指定子とは、単純なグローバル変数の名前、変数項目への参照、変数の写像参照、または変数の列参照、である。この方法で、ある状態の小さな構成子の値を変更することが可能だ。たとえば、もし状態構成要素が写像であったならば、写像のひとつの要素を変更することが可能である。

代入文は次の形式をもつ:

```
sd := ec
```

ここで sd は状態指定子であり、 ec は式または操作呼出しである。代入文は、(式または操作呼出しの) 右辺に記述された既に与えられている状態構成要素への変更を示す。もし右辺が操作変更の状態であるならば、その操作は代入が行われる前に (それ相当の副作用を伴い) 実行される。

多重代入もまた可能である。これは次の形式をもつ：

```
atomic (sd1 := ec1;
        ...;
        sdN := ecN
        )
```

右辺の式または操作呼出しはすべて、実行されるかあるいは評価され、その結果は相当の状態指定子に結び付けられる。右辺は、不変条件評価に関しては原子的に実行される。しかし多重スレッド併発モデルの場合、タスク切替に関して、実行は必ずしも原子的ではない。

例題: 前に述べた例 (Swap) における操作は、通常の代入を表していた。次の Win_sd 操作は、90 ページの Win を手直ししたものであり、特定の写像キーに代入をおこなう状態指示子の仕様記述を行っている:

```
Win_sd : Team * Team ==> ()
Win_sd (wt,lt) ==
  let gp in set dom gps be st
      {wt,lt} subset {sc.team | sc in set gps(gp)}
  in gps(gp) := { if sc.team = wt
                  then mu(sc, won |-> sc.won + 1,
                              points |-> sc.points + 3)
                  else if sc.team = lt
                  then mu(sc, lost |-> sc.lost + 1)
                  else sc
                | sc in set gps(gp)}
  pre  exists gp in set dom gps &
                {wt,lt} subset {sc.team | sc in set gps(gp)}
```

SelectionSort 操作 は 47 ページにおける selection_sort 関数の状態使用版である。これは、 97 ページに定義されたインスタンス変数を用いて、特定の列索引の内容を変更するための状態指示子の使用を述べている。

```
functions

min_index : seq1 of nat -> nat
min_index(l) ==
if len l = 1 then 1
else let mi = min_index(tl l)
   in if l(mi+1) < hd l
     then mi+1
     else 1

operations

SelectionSort : nat ==> ()
SelectionSort (i) ==
  if i < len l
  then (dcl temp: nat;
        dcl mi : nat := min_index(l(i,...,len l)) + i - 1;
        temp := l(mi);
        l(mi) := l(i);
        l(i) := temp;
        SelectionSort(i+1)
       );
```

以下に述べる例では多重代入を描く。

```
class C

  instance variables
    size : nat;
    l : seq of nat;
  inv size = len l

  operations
    add1 : nat ==> ()
    add1 (x) ==
       ( l := [x] ^ l;
```

```
            size := size + 1);

    add2 : nat ==> ()
    add2 (x) ==
       atomic (l := [x] ^ l;
               size := size + 1)

end C
```

ここでは、add1 の中でこのクラスのインスタンス変数における不変条件はこわされるが、一方の add2 の中では多重代入を用いることで不変条件は保持される。

13.5 条件文

構文:

文 = ...
| if 文
| cases 文
| ... ;

if 文 = 'if', 式, 'then', 文,
{ elseif 文 }, ['else', 文] ;

elseif 文 = 'elseif', 式, 'then', 文 ;

cases 文 = 'cases', 式, ':',
cases 文選択肢群,
[',', others 文], 'end' ;

cases 式選択肢群 = cases 文選択肢,
{ ',', cases 文選択肢 } ;

cases 文選択肢 = パターンリスト, '->', 文 ;

others 文 = 'others', '->', 文 ;

意味定義: *if* 文の意味定義は、文に代わることを除けば (また else 部分がオプションであることも除けば)、第 7.4 節に述べられた *if* 式 に相当する[18]。

cases 文 に対する意味定義は、文に代わることを除けば、第 7.4 節に述べられた *cases* 式 に相当する。

例題: 以下のシグネチャをもつ、関数 clear_winner と winner_by_more_wins そして演算 RandomElement を仮定する:

```
clear_winner : set of Score -> bool
winner_by_more_wins : set of Score -> bool
RandomElement : set of Team ==> Team
```

その後、操作 GroupWinner_if ではネストした if 文使用の実例が挙げられている (iota 式については 55 ページで紹介されている):

```
GroupWinner_if : GroupName ==> Team
GroupWinner_if (gp) ==
  if clear_winner(gps(gp))
   -- 他のどのスコアより点数が多い gps(gp) の
   -- 唯一のスコアを返す
  then return ((iota sc in set gps(gp) &
                  forall sc' in set gps(gp) \ {sc} &
                    sc.points > sc'.points).team)
  else if winner_by_more_wins(gps(gp))
   -- 最大の点数であり最大点数の他のスコアより多く勝っている
   -- gps(gp) における唯一のスコアを返す
  then return ((iota sc in set gps(gp) &
              forall sc' in set gps(gp) f {sc} &
                (sc.points > sc'.points) or
                (sc.points = sc'.points and
                 sc.won > sc'.won)).team)
   -- まったくの勝者はなく、よって最高スコアの中から
   -- 無作為にスコアを選ぶ
  else RandomElement ( {sc.team | sc in set gps(gp) &
                                  forall sc' in set gps(gp) &
```

[18] else 部分が省略される場合は、意味定義上は else skip を用いるのと同じである。

```
                                    sc'.points <= sc.points} );
```

代わりとして、この操作に対しては一致値パターンをもつ cases 文を用いることができるだろう:

```
GroupWinner_cases : GroupName ==> Team
GroupWinner_cases (gp) ==
  cases true:
    (clear_winner(gps(gp))) ->
         return ((iota sc in set gps(gp) &
                       forall sc' in set gps(gp) \ {sc} &
                        sc.points > sc'.points).team),

    (winner_by_more_wins(gps(gp))) ->
         return ((iota sc in set gps(gp) &
                       forall sc' in set gps(gp) \ {sc} &
                         (sc.points > sc'.points) or
                         (sc.points = sc'.points and
                            sc.won > sc'.won)).team),

    others -> RandomElement ( {sc.team | sc in set gps(gp) &
                                    forall sc' in set gps(gp) &
                                     sc'.points <= sc.points} )
  end
```

13.6 for ループ文

構文:

文 = ...
| 列 for ループ
| 集合 for ループ
| 索引 for ループ
| ... ;

列 for ループ = 'for', パターン束縛, 'in', ['reverse'], 式,
'do', 文 ;

集合 for ループ = 'for', 'all', パターン, 'in set', 式,
'do', 文 ;

索引 for ループ = 'for', 識別子, '=', 式, 'to', 式,
['by', 式], 'do', 文 ;

意味定義: *for* ループ文には 3 種類ある。索引を用いる for ループはほとんどの高水準プログラム言語において知られているものである。さらに、集合や列を用いる 2 つの for ループがある。これらは特に、集合 (または列) のすべての要素に対するアクセスが 1 つ 1 つ必要とされる場合に役立つ。

索引 *for* ループ文 は次の形式をもつ:

```
for id = e1 to e2 by e3 do
s
```

ここにおいて id は識別子、e1 と e2 はループの下限と上限を示す整数式、e3 はステップ幅を示す整数式、そして s は文でここで識別子 id を用いることができる。これは連続する文としての文 s の評価を表すが、現文脈は id の束縛により拡張されたものである。このように、最初に s が評価されるとき、 id は下限 e1 などの評価から戻ってきた値に束縛され、これは上限に達するまでつまり、 s > e2 となるまで同様に繰り返される。e1, e2 および e3 はループに入る前に評価されることに、注意したい。

集合 *for* ループ文 は次の形式をもつ:

```
for all e in set S do
s
```

ここで S は集合式である。文 s は、集合 S から e の束縛で拡張され部分列の値となった現環境において評価される。

列 *for* ループ文 は次の形式をもつ:

```
for e in l do
s
```

ここで l は列式である。文 s は、列 l から e の束縛と共に拡張され部分列値となった現環境で、評価される。キーワード reverse が用いられる場合は、列 l の要素は逆順にとられる。

例題: 操作 Remove は、数の列から与えられた 1 つの数のすべての出現を削除するための、 列 *for* ループの使用について説明している:

```
Remove : (seq of nat) * nat ==> seq of nat
Remove (k,z) ==
(dcl nk : seq of nat := [];
 for elem in k do
   if elem <> z
   then nk := nk^[elem];
 return nk
);
```

集合 *for* ループは、全グループの勝者集合を戻すように開発されることも可能である:

```
GroupWinners: () ==> set of Team
GroupWinners () ==
(dcl winners : set of Team := {};
 for all gp in set dom gps do
   (dcl winner: Team := GroupWinner(gp);
    winners := winners union {winner}
   );
 return winners
 );
```

次の 索引 *for* ループの例は、古典的なバブルソートアルゴリズムである:

```
BubbleSort : seq of nat ==> seq of nat
BubbleSort (k) ==
  (dcl sorted_list : seq of nat := k;
   for i = len k to 1 by -1 do
     for j = 1 to i-1 do
```

```
        if sorted_list(j) > sorted_list(j+1)
        then (dcl temp:nat := sorted_list(j);
              sorted_list(j) := sorted_list(j+1);
              sorted_list(j+1) := temp
             );
    return sorted_list
    )
```

13.7 while ループ文

構文:

文 = ...
| while ループ
| ... ;

while ループ = 'while', 式, 'do', 文 ;

意味定義: *while* 文 に対する意味定義は、伝統的なプログラム言語からもってきた while 文 に対応する。*while* ループ の形式は次のとおり:

```
while e do
  s
```

ここで、 e はブール式、 s は文である。式 e が true と評価される限りは、本体文 s が評価される。

例題: *while* ループについては、相対誤差 e 内で実数 r の平方根を近似するニュートン法を用いた以下の例により、説明できる。

```
SquareRoot : real * real ==> real
SquareRoot (r,e) ==
  (dcl x:real := 1,
       nextx:real := r;
   while abs (x - nextx) >= e * x do
     ( x := nextx;
       nextx := ((r / x) + x) / 2;
     );
```

```
 return nextx
);
```

13.8 非決定文

構文:

```
文 = ...
   | 非決定文
   | ... ;

非決定文 = '||', '(', 文,
           { ',', 文 }, ')' ;
```

意味定義: 非決定文 は次の形式をもつ:

```
|| (stmt1, stmt2, ..., stmtn)
```

またこれは文構成要素 `stmti` の任意の (非決定) 順の実行を表すものである。しかしながら、文構成要素は同時に実行されるものではないことを書き留めておくべきであろう。インタープリタは、たとえその構成要素が非決定文と呼ばれたとしても、不十分決定の[19]意味定義を用いるということには注意しよう。

例題: 次のインスタンス変数

```
instance variables
  x:nat;
  y:nat;
  l:seq1 of nat;
```

を用いてバブルソートを行うために非決定文が使用できる:

[19] インタープリタの使用者がこれらの文要素が実行される順は知らないとしても、「プロジェクトオプション」の「乱数発生初期値」が用いられない限りは常に同じ順で実行される。

```
Sort: () ==> ()
Sort () ==
  while x < y do
    ||(BubbleMin(), BubbleMax());
```

ここで BubbleMin は、部分列 l(x,...,y) 内の最小値を “bubbles” した後に列の先頭にもってくる、また BubbleMax は、部分列 l(x,...,y) 内の最大値を “bubbles” した後に列の最終索引におく。BubbleMin は最小値の索引を見つけるために、最初に部分列を通して行う繰り返しにおいて働く。この索引の内容はその後、列 l(x) の先頭の内容と交換される。

```
BubbleMin : () ==> ()
BubbleMin () ==
  (dcl z:nat := x;
   dcl m:nat := l(z);
   -- find min val in l(x..y)
   for i = x to y do
     if l(i) < m
     then ( m := l(i);
            z := i);
   -- move min val to index x
   (dcl temp:nat;
    temp := l(x);
    l(x) := l(z);
    l(z) := temp;
    x := x+1));
```

BubbleMax もまた同様に操作する。こちらは最大値の索引を見つけるために、部分列を通して反復を行い、その後この索引の内容を部分列の最後の要素の内容と交換する。

```
BubbleMax : () ==> ()
BubbleMax () ==
  (dcl z:nat := x;
   dcl m:nat := l(z);
   -- find max val in l(x..y)
```

```
for i = x to y do
  if l(i) > m
  then ( m := l(i);
         z := i);
-- move max val to index y
(dcl temp:nat;
 temp := l(y);
 l(y) := l(z);
 l(z) := temp;
 y := y-1));
```

13.9 call 文

構文:

文 = ...
| call 文
| ... ;

call 文 = [オブジェクト指定子, '.'], name,
'(', [式リスト], ')', ;

オブジェクト指定子 = 名称
| self 式
| new 式
| オブジェクト項目参照
| オブジェクト適用 ;

オブジェクト項目参照 = オブジェクト指定子, '.', 識別子 ;

オブジェクト適用 = オブジェクト指定子, '(', [式リスト], ')' ;

意味定義: *call* 文は次の形式をもつ:

```
object.opname(param1, param2, ..., paramn)
```

*call*文 は操作 opname を呼び、 式というオブジェクト中で、その操作を評価した結果を返す。操作はグローバル変数を扱うことができるので、 *call* 文 は関数呼出しがそうするように必ずしも値を戻す必要はない。

オブジェクト指定子 が指定される場合、それは操作 opname が定義されているクラスのオブジェクトに対するオブジェクト参照に従わなければならない、そして操作は public に指定されなければならない。オブジェクト指定子が指定されていないのであれば、その操作は現オブジェクトにおいて呼ばれるものである。操作がスーパークラスで定義されているのであれば、それは public か protected かで定義されていなければならない。

例題:

以下に述べる Stack の単純な記述について考えよう:

```
class Stack

instance variables
  stack: seq of Elem := [];

operations

  public Reset: () ==> ()
  Reset() ==
    stack := [];

  public Pop: () ==> Elem
  Pop() ==
    def res = hd stack in
     (stack := tl stack;
      return res)
  pre stack <> []
  post stack~ = [RESULT] ^ stack

end Stack
```

例の中で操作 Reset はパラメーターをもたないし、操作 Pop がスタックの

一番上の要素を戻すのに反し値も戻さない。スタックは以下のように用いることができる:

```
( dcl stack := new Stack();
  stack.Reset();
  ....
  top := stack.Pop();
)
```

以下に示すように、Stack クラス内で操作を呼び出すことができる:

```
Reset();
....
top := Pop();
```

あるいは self 参照を用いれば以下の様になる:

```
self.Reset();
top := self.Pop();
```

13.10 return 文

構文:

```
文 = ...
   | return 文
   | ... ;

return 文 = 'return', [ 式 ] ;
```

意味定義: *return* 文 は操作内の式の値を戻す。値は与えられた文脈中で評価される。もし操作が値を返さないならば、式は省かれなければならない。*return* 文は次の形式をもつ:

```
return e
```

または

```
return
```

ここで式 e は操作の戻り値である。

例題: FunCall が関数呼出しであるの対し、以下に述べる例題 OpCall は操作呼出しである。*if* 文が 2 つに枝分かれした文だけを受け入れるため、 FunCall は *return* 文を用いることで文に “変換されて” いる。

```
if test
then  OpCall()
else  return FunCall()
```

たとえば、前節における stack クラスを、スタックの先頭を検査する操作を用い拡張することが可能である：

```
public Top : () ==> Elem
Top() ==
  return (hd stack);
```

13.11 例外処理文

構文:

文 = ...
| always 文
| trap 文
| 再帰 trap 文
| exit 文
| ... ;

always 文 = 'always', 文, 'in', 文 ;

trap 文 = 'trap', パターン束縛, 'with', 文, 'in',
文 ;

再帰 trap 文 = 'tixe', trap 群, 'in', 文 ;

trap 群 = '{', パターン束縛, '|->', 文,
{ ',', パターン束縛, '|->', 文 }, '}' ;

exit 文 = 'exit', [式] ;

意味定義: 例外処理文は、仕様記述のなかで例外エラーを制御するために用いられる。このことは、仕様記述内で例外信号を送ることができなければならないことを意味する。これは *exit* 文を用いて行うことができ、次の形式をもつ:

```
exit e
```

または

```
exit
```

ここにおいて e はオプションの式である。式 e はどのような種類の例外が起きたのかを知らせるために用いられる。

always 文 は次の形式をもつ:

```
always s1 in
s2
```

ここで s1 と s2 は文である。最初に文 s2 が評価され、さらに例外が起きたかどうかにかかわらず文 s1 も評価される。*always* 文全体の結果値は、文 s1 の評価により決定される: もしここで例外を起こせばこの値が戻される、それ以外は文 s2 の評価の結果が返される。

trap 文 は、ある一定の条件が満たされたときに、処理文 s1 を評価する唯一のものである。これは次の形式をもつ:

```
trap pat with s1 in s2
```

ここで pat はある一定の例外を選択するために用いられるパターンまたは束縛であり、 s1 と s2 は文である。最初に文 s2 を評価するが、もし例外が発生しなければ s2 の評価結果が、 *trap* 文全体の結果値となる。例外が起きた場合には、 s2 の値はパターン pat と一致するか調べる。そこで一致するものがない場合、例外が *trap* 文全体の結果値として戻され、そうでない場合は文 s1 が評価され、この評価の結果がまた *trap* 文全体の結果値となる。

再帰 *trap* 文 は次の形式をもつ:

```
tixe {
  pat1 |-> s1,
  ...
  patn |-> sn
} in s
```

ここで pat1, ..., patn はパターンまたは束縛であり、s, s1, ..., sn は文である。最初に文 s が評価され、もし例外が起きなければ、その結果が完全な 再帰 *trap* 文の結果として戻される。そうでない場合、値はパターン pati の各々に順に一致させられる。一致するものが見つからなかった場合、 再帰 *trap* 文の結果として例外が戻される。一致するものが見つかれば、対応する文 si が評価される。これが例外を起こさない場合には、 si の評価の結果値は 再帰 *trap* 文の結果として戻される。それ以外の場合は、今度は新しい例外値 (si の評価の結果) をもとに、マッチングを再び始める。

例題: 多くのプログラムにおいて、1 つの操作にはメモリーを割り当てる必要がある。操作が完了した後には、このメモリーはそれ以上必要でなくなる。このことは *always* 文と共に実行される:

```
( dcl mem : Memory;
  always Free(mem) in
  ( mem := Allocate();
    Command(mem, ...)
  )
)
```

上記の例では、 *always* 文の本体文中で起きる可能性のある例外上では、何かを行うことはできない。*trap* 文 を用いることで、これらの例外を捉えることができる:

```
trap pat with ErrorAction(pat) in
( dcl mem : Memory;
  always Free(mem) in
  ( mem := Allocate();
    Command(mem, ...)
  )
)
```

ここに *always* 文 中で起きるすべての例外は、 *trap* 文によって捉えられる。数個の例外値を区別したい場合には、ネストされた *trap* 文 かまたは再帰 *trap* 文を用いることができる:

```
DoCommand : () ==> int
DoCommand () ==
( dcl mem : Memory;
  always Free(mem) in
  ( mem := Allocate();
    Command(mem, ...)
  )
);

Example : () ==> int
Example () ==
tixe
{ <NOMEM> |-> return -1,
  <BUSY>  |-> DoCommand(),
  err     |-> return -2 }
in
  DoCommand()
```

操作 DoCommand では、メモリー割り当て中に *always* 文を用いるし、また操作 Example では、起きた例外はすべて 再帰 *trap* 文 によって捉えられる。値

<NOMEM> をもつ例外は、結果として -1 の戻り値となり例外は起きない。例外値が <BUSY> であるならば、再び操作 DoCommand の実行を試みる。これが例外を起こす場合には、 再帰 *trap* 文によってまた処理が行われる。他の例外はすべて、値 -2 を戻す結果となる。

13.12 error 文

構文:

文 = ...
| error 文
| ... ;

error 文 = 'error' ;

意味定義: *error* 文 は定義されていない式に相等する。文の結果は定義されないしこのことによりエラーが起きる、ということを明示的に述べるために用いられる。*error* 文 が評価されるときは、インタープリタは仕様記述の実行を停止し *error* 文 が評価されたことを報告する。

エラー文の実用的な使用となると、未定義式を用いた場合なので、事前条件の場合とは異なる: 事前条件の使用とは、操作が呼ばれたときは事前条件が満たされていると保証することは呼ぶ側の責任であることを意味する；error 文の使用では、エラー処理を取り扱うのは呼ばれた操作側の責任である。

例題: 106 ページ上の操作 SquareRoot は、平方する数は負かもしれないという可能性を排除するものでない。これについては操作 SquareRootErr で修正を行う:

```
SquareRootErr : real * real ==> real
SquareRootErr (r,e) ==
  if r < 0
  then error
  else
    (dcl x:real := 1;
     dcl nextx:real := r;
     while abs (x - nextx) >= e * x do
       ( x := nextx;
         nextx := ((r / x) + x) / 2;
```

```
    );
  return nextx
)
```

13.13 恒等文

構文: 文 = ...
| 恒等文 ;

恒等文 = 'skip' ;

意味定義: 恒等文 は何の評価も行われないという信号を送るために用いられる、

例題: 第 13.6 節の操作 Remove において、elem=z が明示的に述べられていない場合の for ループ内における操作の動き。以下の Remove2 がこれを示す。

```
Remove2 : (seq of nat) * nat ==> seq of nat
Remove2 (k,z) ==
  (dcl nk : seq of nat := [];
   for elem in k do
     if elem <> z then nk := nk^[elem]
     else skip;
   return nk
  );
```

ここで 恒等文を説明するために else 選択枝 を明示的に含めたが、ほとんどの場合 else 選択枝は含まれないため 恒等文 は暗黙に仮定されているのである。

13.14 start 文と startlist 文

構文: 文 = ...
| start 文
| startlist 文 ;

start 文 = 'start', '(', 式, ')' ;

startlist 文 = 'startlist', '(', 式, ')' ;

意味定義: *start* および *startlist* 文は次の形式をもつ:

```
start(aRef)
startlist(aRef_s)
```

クラス記述がスレッドを含む場合には (第 16 節参照)、このクラスから生成される各々のオブジェクトは stand-alone の仮想マシンとして演算を行う能力をもつ、別の言葉で言えば: オブジェクトが独自の処理能力をもつ。この状況で、 *new* 式 は 待ち状態のままで 'process' を生成する。このようなオブジェクトに対し、 VDM++ は前もって定義された操作に関して、これは *start* 文を通して発動することができるものだが、待ち状態を変換して活動状態にする仕組みをもっている[20]。

オブジェクト生成と start の明示的な分離では、オブジェクトが記述された動作の提示を start する以前に (同時に起きる) システムの初期化が完了する可能性を与えているが、この方法で、まだ生成・接続されていないものとしてオブジェクトが参照されるときに起きるかもしれない問題を避けている。

start 文の別の形 *startlist* 文は、多くの能動的オブジェクトを任意の順で始めるためにある。startlist に対するパラメーター aRef_s は、スレッドを含むクラスからインスタンス化されるオブジェクトに対するオブジェクト参照の集合でなければならない。

例題: オペレーティングシステムの仕様記述を考えてみよう。この構成要素は、ブート連続動作中にスタートするデーモンや他プロセスと考えられる。この見通しから、以下の定義が関連する:

```
types

  runLevel = nat;

  Process = Kerneld | Ftpd | Syslogd | Lpd | Httpd
```

[20] オブジェクトが能動的状態にあるときには、この行動はスレッド (第 16 節参照) を用いて記述することができる 。

```
instance variables
  pInit : map runLevel to set of Process
```

ここで Kerneld は他で指定されたオブジェクト参照型であり、並べられている他のプロセスも同様である。

ここで 1 つの操作としてのブート列をモデル化することができる:

```
bootSequence : runLevel ==> ()
bootSequence(rl) ==
  for all p in set pInit(rl) do
    start(p);
```

もう 1 つの方法として、 ここで startlist 文を用いることができるであろう:

```
bootSequenceList : runLevel ==> ()
bootSequenceList(rl) ==
  startlist(pInit(rl))
```

13.15 仕様記述文

構文: 文 = ...
| 仕様記述文 ;

仕様記述文 = '[', 陰操作本体, ']' ;

意味定義: 仕様記述文は、事前条件や事後条件で表した文で期待効果を記述するために用いることができる。このように、操作定義に強要されることなく抽象的 (暗黙の) 仕様記述を許すことで、1 つの文の概略を捉える。仕様記述文は、暗黙に定義された陰操作 (第 12 節参照) の本体と同等である。したがって、仕様記述文を実行することはできない。

例題: 仕様記述文をバブルソートのバブル最大部を指定するために用いることができる:

```
Sort2 : () ==> ()
Sort2 () ==
  while x < y do
    || (BubbleMin(),
        [ext wr l : seq1 of nat
            wr y : nat
            rd x : nat
         pre x < y
         post y < y~ and
              permutation (l~(x,...,y~),l(x,...,y~)) and
              forall i in set {x,...,y} & l(i) < l(y~)]
       )
```

(permutation は、もし 1 つの列が他方の並び替えであるならば真を返すような、2 つの列から結果をとる補助関数である。)

13.16 duration 文

構文:

文 = ...
| duration 文 ;

duration 文 = 'duration', '(', 数値, ')',
文 ;

意味定義: duration 文とは、閉ざされた文に対する内部クロックが増加するときに伝えられる Toolbox のインタプリタへのランタイム指示である。duration 文で与えられる値（自然数）は通常、その文のために計算される増分の代わりに使用されるべきである。したがって、duration 文は、Toolbox のデフォルト実行時間の計算を優先するためのメカニズムを提供する。

例: 初めに単純な例を示す:

```
while n < 10 do
   duration(10) n := n + 1;
```

この例では、閉ざされた duration 文の文中で、このループが実行されないと仮定すると文 `n := n + 1` を実行するために必要な時間を計算するよりも、それぞれのループの繰り返しで、Toolbox は内部クロックを 10 秒単位で増加するだろう。

duration 文が入れ子にされるなら、最外部ものが優先され、残りは無視される。例えば以下の通りである。

```
duration(30)(
  n := 1;
  while n < 10 do
     duration(10) n := n + 1;
  )
```

外側の duration 文は優先される。したがって、これが閉ざされた duration 文に関する文中で実行されないと仮定すると、この文を実行するとき、インタプリタは内部クロックを 30 秒単位で増加させるだろう。

入れ子は操作呼び出しが原因で発生することに注意する。以下の例で考える:

```
op1 : nat ==> nat
op1(m) ==
 duration (20) return m + 1;

op2 : () ==> nat
op2() ==
(dcl n : nat := 3;
 duration(10)  n := op1(1);
 return n)
```

`op2` を実行しているとき、もしも、`op1` への呼び出しが実行されたら、op1 内の duration 文は呼び出し環境内の duration 文によって優先されるだろう。このようにして、`op2` 内の文 `n := op1(1);` の実行で、内部クロックは 10 秒単位のみ増加する。

13.17 cycles 文

構文: 文 = ...

| cycles 文 ;

cycles 文 = 'cycles', '(', 数値, ')',
文 ;

意味定義: cycles 文とは、閉ざされた文に対する内部クロックが増加するときに伝えられる Toolbox のインタプリタへのランタイム指示である。cycles 文で与えられた値（自然数）はどのくらいのクロック周期かの目安として使われるべきである。また通常、文のために計算される増分の代わりに、閉ざされた文は増加されるべきである。したがって、cycles 文は duration 文と同様に、Toolbox のデフォルト実行時間の計算を優先するメカニズムを提供するが、CPU の速度に関する方法で、計算が行われている。

例題: 初めに単純な例を示す:

```
while n < 10 do
   cycles(1000) n := n + 1;
```

この例では、閉ざされた cycles 文の文中で、このループが実行されないと仮定すると状態 `n := n + 1` を実行するために必要な時間を計算するよりむしろ、それぞれのループの繰り返しで、Toolbox は内部クロックを与えられた (容量に比例した) CPU の 1000 の命令を処理するためにかかる時間によって増加するだろう。

cycles 文が入れ子にされるなら、最外部ものは優先され、残りは無視される。例えば以下の通りである。

```
cycles(3000)(
  n := 1;
  while n < 10 do
     cycles(1000) n := n + 1;
  )
```

外側の cycles 文は優先される。したがって、これが閉ざされた cycles 文に関する文中で実行されないと仮定すると、この文を実行するとき、インタプリタは内部クロックを与えられた CPU 上で 3000 の命令を実行するためにかかる時間によって増加するだろう。

入れ子は操作呼び出しが原因で発生することに注意する。以下の例で考える:

```
op1 : nat ==> nat
op1(m) ==
 cycles (2000) return m + 1;

op2 : () ==> nat
op2() ==
(dcl n : nat := 3;
 cycles(1000)  n := op1(1);
 return n)
```

op2 を実行しているとき、もしも、 op1 への呼び出しが実行されたら、 op1 内の cycles 文は呼び出し環境内の cycles 文によって優先されるだろう。このようにして、 op2 内の式 n := op1(1); の実行で、内部クロックは与えられた CPU 上のみで 1000 の命令を実行するためにかかる時間によって増加する。

14 トップレベル仕様記述

ここまでの節で, 型, 式、文、関数、そして操作、という VDM++ 構成要素を述べてきた。たくさんのこれらの構成要素も、1 つのクラス定義のなかでその定義を構築することができる。トップレベル仕様記述、あるいは文書、は 1 つまたはそれ以上のクラス定義により構成されるものである。

構文: 文書 = クラス | システム,{ クラス | システム } ;

14.1 システム

VDM++ での分散システムを述べることを可能にするために、どのようにシステムモデルの部品が異なった Core Processing Units (CPUs) を分散し、通信は、互いに接続された CPUs を運ぶのかを述べているシステム概念を含む。“class” というキーワードの代わりの “system” というキーワードを除いて、構文上、第 14.2 節以下に述べられている普通のクラスのように、システムは正確に述べられる。

構文:
```
システム = 'system', 識別子,
           [ クラス本体 ],
           'end', 識別子 ;

クラス本体 = 定義ブロック, { 定義ブロック } ;

定義ブロック = 型定義
             | 値定義
             | 関数定義
             | 操作定義
             | インスタンス変数定義
             | 同期化定義
             | スレッド定義 ;
```

意味定義: それぞれのシステムの種類は、以下の部品を持っている:

- システム名を持っているシステムヘッダー
- 任意の **システム本体**

- システムテール

システムヘッダーで与えられているシステム名はクラス名の定義している存在である。システム名は、グローバルに見える。すなわち、仕様記述内の全ての他のクラスやシステムの中が見える。

クラスヘッダーのシステム名はシステムテールの中のシステム名と同じでなければならない。その上、定義しているシステム名は仕様記述内で一意でなければならない。

システムにおける特別なものは、暗黙のうちに CPU と BUS と呼ばれる特別に定義されたクラスを利用することができるということである。システムのインスタンスを作成するのが可能ではないが、 CPU と BUS で作られたインスタンスは初期化時に作成されるだろう。CPU と BUS はシステム定義の外側では使うことが出来ないことに注意する。

CPU と BUS のインスタンスはインスタンス変数として作られなくてはならない。また、定義はコンストラクタを使用しなければならない。CPU クラスのコンストラクタは 2 つの変数をもつ: 1 つ目は CPU に使用される主要なスケジューリング方針を示す。一方、2 つ目は変数は CPU(Million Instructions Per Second か MIPS として、示される) の容量を提供する。BUS クラスのコンストラクタは 3 つの変数を持つ。1 つ目は、BUS の種類を示す。2 つ目は、BUS の容量 (そのバンド幅)、最後 3 つ目は、BUS インスタンスを与えられることによって、互いに接続された CPU インスタンスのセットを与える。

現在、サポートされた主要な CPU のスケジューリング方針は:

<FP>: Fixed Priority

<FCFS>: First Come First Served

現在、サポートされた主要な BUS のスケジューリング方針は:

<FCFS>: First Come First Served

CPU クラスは deploy や setPriority と呼ばれるメンバ操作を持っている。deploy 操作は一つの重要な変数を持ち、システム内部の静的インスタンス変数として宣言されるオブジェクトでなければならない。[21]。deploy 操作の意味定義は、このオブジェクト内部のすべての機能性の実行は配置された CPU 上で行われるだろう。setPriority 操作は二つの変数を持つ。1 つ

[21] また、将来の拡張のため、2 番目のパラメタが現在無視されるとき、それは、文字列を取ることができる。

目は、CPU に配置されたパブリックな操作名でなければならない。2 つ目は変数は自然数である。setPriority 操作の意味定義は、与えられた操作が与えられた優先度 (2 つ目の変数) を割り当てることである。これは、固定された主要なスケジューリングが、与えられた CPU 上で使用されるときに使われる。

そのシステムの “class” はそれが含むことだけできる方法で制限される:

インスタンス変数: システムの “class” で宣言可能な唯一のインスタンスは、異なった CPU へ割り当てたい異なったシステムの構成要素の静的インスタンスと同様に、特別なクラスである CPU と BUS である。

コンストラクタ: CPU の実際のインスタンス展開と、異なった操作のための優先度の設定は、システムの “class” に置くことができる唯一の操作であるコンストラクタの内部に設定される。このコンストラクタの内部で使用可能な唯一の文の種類は、特別な deploy と setPriority 操作の一連の呼び出しを持ったブロック文である。

さらに、異なった CPU へ展開されるインスタンスのための静的な宣言の使用に関して制限がある。もしも、インスタンスが生成されるクラスが、どんな静的操作や静的関数を含んでいても基本的に、ユーザは唯一のインスタンスが CPU へ展開されることを確かにするべきである。静的インスタンス変数が使用される場合、(BUS 以上の通信なしで) 直接アクセスされる。つまり、これは本質的に、分布の観点から適応されない。したがって、展開されたインスタンスの全てのインスタンス変数は操作の使用を通してのみアクセスされるべきである。

例題: システムクラスを定義した例:

```
system Simple

instance variables
 static public a : A := new A();
  static public b : B := new B();
  -- define the first CPU with fixed priority scheduling
  -- and 22E6 MIPS
  CPU1 : CPU := new CPU (<FP>, 22E6);

  static public c : C := new C();
```

```
  -- define the second CPU with fixed priority scheduling
  -- and 11E6 MIPS
  CPU2 : CPU := new CPU (<FP>, 11E6);

  -- create a communication bus that links the three
  -- CPU's together
  BUS1 : BUS := new BUS (<CSMACD>, 72E3, CPU1, CPU2)

operations
  public Simple: () ==> Simple
  Simple () ==
    ( -- deploy a on CPU1
      CPU1.deploy(a);
      -- deploy b on CPU1
      CPU1.deploy(b);
      -- deploy c on CPU2
      CPU2.deploy(c,"CT");
      -- "CT" is a label here which is ignored
    );

end Simple
```

A、B および C がすべてクラスとして定義される場合

14.2 クラス

標準 VDM-SL 言語と比べて、VDM++ はクラスと共に拡張されてきた。この節では、トップレベル仕様記述を生み出し構成するクラスの使用について記述する。VDM++ によって提供されるオブジェクト指向機能を用いれば、次が可能である:

- クラスの定義とオブジェクトの生成。
- 関連の定義とオブジェクト間リンクの生成。
- 継承を通して行う汎化と特化。

- 関数と操作を用いたオブジェクトの機能的動作の記述。
- スレッドおよび同期制約を通したシステムの動的動作の記述。

実際上の機能を述べる前に、クラスというものの一般的概要を記述する。

構文:

クラス = 'class', 識別子, [継承節],
[クラス本体],
'end', 識別子 ;

継承節 = 'is subclass of', 識別子, ',', { 識別子 } ;

クラス本体 = 定義ブロック, { 定義ブロック } ;

定義ブロック = 型定義
| 値定義
| 関数定義
| 操作定義
| インスタンス変数定義
| 同期定義
| スレッド定義 ;

意味定義: 各々のクラス記述は以下の構成をもつ:

- クラス名およびオプションである **継承節**からなるクラスヘッダー部
- オプションである **クラス本体**
- クラステイル部

クラス名がクラスヘッダー部で与えられると、そのクラスの名称が定義されたことになる。クラス名はグローバルに見ることができる、つまり仕様記述におけるすべての他のクラスにおいても見ることができる。

クラスヘッダー部のクラス名はクラステイル部のクラス名と同じである必要がある。さらに、クラス名の定義は仕様記述を通して一回でなければならない。

(オプションの) クラス本体は次から成る:

- 値定義 (定数) の集合

- 型定義の集合
- 関数定義の集合
- クラスからインスタンス化されたオブジェクトの内部状態を記述するインスタンス変数定義 の集合状態不変条件式は推奨されるが強制されるものではない
- 内部状態上で動く 操作定義 の集合
- 同期定義の集合で、許可述語に関してかあるいは mutex 制約を用いて記述されたもの
- 能動的オブジェクトに対する制御スレッドを記述する スレッド定義の集合
- 操作の列を示すのに使用される *traces* の集合は、どのテストケースが自動的に生産されることが望まれるかのために呼びます

一般的に、1 つのクラス内に定義される構成要素はすべて単一の名称を持たなければならない、たとえば同じ名称の操作と型を定義することはできない。しかしながら、それらの入力パラメーターの型は重複してはいないという制限のある条件下では、関数と操作の名前を 多重定義する ことが可能である (つまり、同じ名称の 2 つ以上の関数と同じ名称の 2 つ以上の操作をもつことが可能である)。これはつまり、どの関数／操作定義が各々の関数／操作呼出しに対応しているのかを、一意に曖昧さなく決定するために、静的型チェックを使うことができるべきなのである。このことは、あるクラスのローカルなインターフェイスにおいて定義された関数や操作に対してだけではなく、それらが継承したスーパークラスに対しても適用されることに注意しよう。このように、たとえば多重継承を含むデザインにおいては、クラス C はクラス A からある関数をまたクラス B から同じ名前を持つ関数を継承する可能性を持つので、この関数名を含むすべての呼出しはクラス C において解決可能でなければならない。

14.3 継承

継承の概念は、オブジェクト指向にとって不可欠なものである。既存クラスのサブクラスとしてのクラスを定義するとき、サブクラス定義として拡張クラスが導入されるが、これは新しく定義されるサブクラスの定義をスーパークラスの定義と共に構成するものである。

継承を通して、サブクラスはスーパークラスから次の継承をおこなう:

- インスタンス変数 これには、すべての不変条件および許される範囲の修正を行った上でのそれらの制限、もまた含まれる。
- 操作定義と関数定義。
- 値定義と型定義
- 第 15.2 節に述べられている同期定義

名前衝突は、同種で同じ名称をもつ 2 つの構成要素が異なるスーパークラスを継承する場合に起きる。名前衝突は 名前限定を通して明示的に解決されなければならない、つまり、スーパークラスの名前と ‘-記号 (バッククォート) で構成要素に接頭語をつけることによってである (第 20 節も参照)。

例題: 最初の例題から、サブクラスが遂行すべきある抽象インターフェイスとしてクラス定義を用いるのに、継承を活用できることがわかる:

```
class Sort

  instance variables
    protected data : seq of int

  operations

    initial_data : seq of int ==> ()
    initial_data (l) ==
      data := l;

    sort_ascending : () ==> ()
    sort_ascending () == is subclass responsibility;
  end Sort

class SelectionSort is subclass of Sort

  functions
```

```
  min_index : seq1 of nat -> nat
  min_index(l) ==
    if len l = 1
    then 1
    else let mi = min_index(tl l)
         in if l(mi+1) < hd l
           then mi+1
           else 1

operations

  sort_ascending : () ==> ()
  sort_ascending () == selectSort(1);

  selectSort : nat ==> ()
  selectSort (i) ==
    if i < len data
    then (dcl temp: nat;
          dcl mi: nat := min_index(data(i,...,len data)) +
                         i - 1;

          temp := data(mi);
          data(mi) := data(i);
          data(i) := temp;
          selectSort(i+1)
          )

end SelectionSort
```

ここでクラス Sort は、異なるソートアルゴリズムによって遂行される 1 つの抽象インターフェイスを定義する。1 つの実装は、 SelectionSort クラスで提供される。

次の例は、どのように名前空間衝突が解決されるかを明らかにする。

```
class A
  instance variables
```

```
    i: int := 1;
    j: int := 2;
end A

class B is subclass of A
end B

class C is subclass of A
  instance variables
    i: int := 3;
end C

class D is subclass of B,C
  operations
    GetValues: () ==> seq of int
    GetValues() ==
      return [
        A`i, -- 1と相等
        B`i, -- 1 (A`i)と相等
        C`i, -- 3と相等
        j    -- 2 (A`j)と相等
      ]
 end D
```

この例題で、クラス D のオブジェクトは3つのインスタンス変数:A`i, A`j、C`j をもつ。クラス D のオブジェクトは、たとえこのクラスが B 、C 両クラス共通のスーパークラスであるとしても、クラス A で定義されるインスタンス変数の唯一のコピーをもつものである、ことに注意したい。このようにクラス D において、名称 B`j、C`j、D`j、j はすべて同じ変数 A`j を参照している。さらに変数名称 i は、クラス B とクラス C では異なる変数を参照するので、クラス D において曖昧であるということに注意すべきである。

14.4 クラス要素のインターフェイスと利用可能性

VDM++ では、クラス内の定義は次のように区別される:

クラス属性: 場合によってはどんなにたくさん (ゼロの可能性もあるが) そのクラスのインスタンスが生成されたとしても、唯 1 つ具体化されるクラスの 1 属性 VDM++ におけるクラス属性は、C++ や Java のような言語における `static` クラス要素に相等する。クラスの (静的) 属性は、属性名称にクラス名称に ‘-記号 (バッククォート) を伴った接頭辞をつけることで、参照することができる、したがって、たとえば `ClassName‘val` は `ClassName` クラスで定義された `val` 値を参照する。

インスタンス属性: クラスの各インスタンスに対して 1 つの実現が存在する属性。したがって、1 つのインスタンス属性は 1 つのオブジェクト内でのみ有効であり、また各々のオブジェクトはインスタンス属性の独自のコピーをもつ。(静的でない) インスタンス属性は、属性の名称にオブジェクトの名称とドットを接頭辞としてつけて参照できるので、たとえば `object.op()` は、`object` と表記されたオブジェクトで操作 `op` を起動する (ただし `op` は `object` に見えるものとして提供されているとする)。

あるクラス内で関数、操作、インスタンス変数、そして定数[22] は、クラス属性かまたはインスタンス属性である可能性がある。このことはキーワード static で示されている:もし宣言にキーワード static が先行するならばクラス属性が記述されていて、そうでないならばインスタンス属性が記述されている。

他のクラス構成要素については以下に述べるように、既定で常にクラス属性かインスタンス属性かどちらかとなっている:

- 型定義は常にクラス属性である。
- スレッド定義は常にインスタンス属性である。したがって、各能動的オブジェクトは自分自身のスレッドを 1 つまたは複数もつ。
- 同期定義は常にインスタンス属性である。したがって各オブジェクトは生成されたときの自分自身の “履歴” をもつ。

[22] 実際には、定数は一般的に静的となる – 静的でない定数であれば、値がクラスの 1 つのインスタンスからもう 1 つへと変化することもある定数を表記することとなり、インスタンス変数を用いる方がより自然であろう。

加えて、クラス要素のインターフェイスやまたアクセスしやすさは、アクセス記述子、 public、private、また protected のうちのいずれか 1 つを用いることで明示的に定義することもできる。これらの指定子の意味は次の通り：

public: どのクラスでもそれらの要素を用いてよい

protected: 現クラスのサブクラスのみがそれらの要素を用いてよい

private: 次以外でそれらの要素を用いてはいけない - これらを指定したクラスの中でのみ用いてよい。

どのクラス要素に対しても既定のアクセスは **private** である。これは、ある要素にアクセス指定子が与えられていない場合は private となるということである。

このことは 11 表にまとめられている。ここでは少しの但書きを付け加える:

- インスタンス変数に対してアクセスを容認する (つまり public や protected というアクセス指定子を与えることで) ということは、読み込みと書き出し両方のアクセスをこれらのインスタンス変数に与えるということである。
- パブリックなインスタンス変数は、ドット (オブジェクトインスタンス変数に対して) やバッククォート記号 (クラスインスタンス変数に対して) を用いて読み込み (書き出しは行えない) が行える、たとえばオブジェクト `o` のパブリックインスタンス変数 `v` は `o.v` としてアクセスすることが許されている。
- アクセス指定子は型、値、関数、そしてインスタンス変数定義といっしょの場合のみ用いることが許されている；ただしスレッドや同期定義と共に用いることはできない。
- クラス属性をインスタンス属性にしたりその逆を行うことはできない。
- 継承されたクラスにとっては、サブクラスに対するインターフェイスとは、サブクラス内の新しい定義と共に拡張されたそのスーパークラスに対するインターフェイスと同じである。
- 継承された要素へのアクセスはそれ以上に制限を加えられることはない、たとえばスーパークラスにおけるパブリックインスタンス変数は、サブクラス中のプライベートなインスタンス変数として再宣言されることはない。

	public	protected	private
クラス内	√	√	√
サブクラス内	√	√	×
任意の外部クラス内	√	×	×

表 11: アクセス指定子意味定義のまとめ

例題 以下の例においては、クラス要素に対する既定アクセスと同様に、異なるアクセス指定子の使用が示されている。説明は定義中のコメントでなされている。

```
class A

  types
    public Atype = <A> | <B> | <C>

  values
    public Avalue = 10;

  functions
    public compare : nat -> Atype
    compare(x) ==
      if x < Avalue
      then <A>
      elseif x = Avalue
      then <B>
      else <C>

  instance variables
    public v1: nat;
    private v2: bool := false;
    protected v3: real := 3.14;

  operations
    protected AInit : nat * bool * real ==> ()
    AInit(n,b,r) ==
```

```
      (v1 := n;
       v2 := b;
       v3 := r)
end A

class B is subclass of A

  instance variables
    v4 : Atype -- A から継承

  operations

    BInit: () ==> ()
    BInit() ==
      (AInit(1,true,2.718); --OK: スーパークラスの
                            -- protected 要素にアクセス可能
       v4 := compare(v1);   --OK なぜなら v1 が public である
       v3 := 3.5;           --OK なぜなら v3 は protected であり
                            -- A のサブクラスである
       v2 := false    --illegal なぜなら v2 は
                            -- A に対し private である
      )

end B

class C

  instance variables
    a: A := new A();
    b: B := new B();


  operations

    CInit: () ==> A`Atype    --型はクラス属性である
    CInit() ==
```

```
        (a.AInit(3,false,1.1);
                              --illegal なぜなら AInit は
                              -- protected である
         b.BInit();           --illegal なぜなら BInit は(既定で)
                              -- private である
         let - = a.compare(b.v3) in skip;
                              --illegal なぜなら
                              -- C は A のサブクラスではなく
                              -- したがって b.v3 は不可である
         return b.compare(B`Avalue)
                              --OK なぜなら compare は
                              -- public インスタンス属性であり
                              -- Avalue は B において
                              -- public クラス属性である
        )

    end C
```

15 同期制約

一般的にシステム全体は、(それらの操作が発動されたときにだけ反応する) 受動特性のオブジェクトとシステムに‘命を吹き込む’能動的オブジェクトを含むものである。これらの能動的オブジェクトは、それ自身で処理を行う制御スレッドをもち仮想マシンのように動作するうえに、スタートした後もその行動を継続するための他オブジェクトとの相互作用を必要としない。別の用語法を用いれば、システムは受動的あるいは能動的なサーバーのサービスを要求するたくさんの能動的クライアントから成り立つ、という記述もできるであろう。このような並列的な環境においては、サーバーオブジェクトは内部の一貫性を保証できる、つまりそれらの状態の不変条件を保守できるような、同期制御を必要とする。それゆえ並列世界では、受動的オブジェクトは操作を入口とする Hoare のモニターのように動作することが必要である。

(同時に能動的な制御スレッドはただひとつであるような) 連続システムが記述される場合には、一般特性の特殊な場合のみがとりあげられ余分な構文は必要とされない。しかしながら、仕様記述から実装への開発の道筋においては、より多く

の相違が現れてきそうである。

以下の各オブジェクトに対する既定の同期規則が、 VDM++においては適用される:

- 操作は、呼び出す側にたてば、たとえ原子的であっても見えるものでなければならない;
- 対応する許可述語をもたない操作は、制約を全く受けないこととなる;
- 同期制約は、オブジェクト内の呼出し (オブジェクト内のある操作がそのオブジェクト内のもうひとつの操作を呼び出すもの) とオブジェクト外の呼出し (ひとつのオブジェクトのある操作からもうひとつのオブジェクトの操作を呼び出すもの) とに等しく適用される;
- 操作発動では、2 つの能動的オブジェクトが含まれる場合にランデブー (Ada におけるものと同じ、[Ada83] を参照) の意味定義をもつ。オブジェクト O_1 がオブジェクト O_2 内の操作 o を呼ぶ場合に、もしオブジェクト O_2 が現在は操作 o をスタートすることができないでいるならば、 O_1 が操作が実行され得るときまでブロックする。このように呼び出し側のオブジェクトと呼び出されるオブジェクトの双方が準備できたときに、発動は起きる。(ここでは Ada の意味定義との微小な相違に注意: Ada ではランデブーへの両方の当事者が実効オブジェクトである; VDM++においては呼出した当事者のみ実効がある)

クラス記述における同期定義ブロックは、上記の既定を上書きする方法をユーザーに提供する。

構文: 同期定義 = 'sync', [同期] ;

同期 = 許可述語 ;

意味定義: 同期は VDM++においては許可述語を用いて記述される。

15.1 許可述語

以下は、同時に呼び出し可能な操作の実行を受け入れるための規則を述べた構文である。これらの特徴を説明するいくつかの記述がなされている。

構文: 許可述語 = 許可述語, { ';',
許可述語 } ;

許可述語 = 'per', 名称, '=>', 式
| 排他制御述語 ;

排他制御述語 = 'mutex', '(', 'all', ')'
| 'mutex', '(', 名称リスト ')' ;

意味定義: 要求された操作の実行を受け入れる許可は、その形式の (deontic) 許可述語における保護条件に従う:

```
per 操作名称 => 保護条件
```

許可を表現するのに含意を用いるのは、保護条件 (式) が真であることが発動のために必要条件ではあるが十分条件ではない、ということを意味する。もし保護条件が偽であるならば許可なしである、というところから始まるとして、許可述語を読みとるべきである。この方法で許可を表現することで、サブクラスへの継承を通しての矛盾のリスクなしに、さらに同様の制約が加えられることを許している。ここにすべての操作に対する既定が存在する:

```
per 操作名称 => true
```

しかしある操作に対して許可述語が指定された場合には、この既定は上書きされる。

保護条件は概念上次のように分類される:

- 過去のイベントへの依存を定義する**履歴保護**、
- オブジェクトのインスタンス変数に依存する**オブジェクト状態保護**、そして
- オブジェクトによるサービスをまつ操作発動 (メッセージ) により形成されたキューの状態に依存する **キュー条件保護**。

これらの保護は自由に混在させることができる。**注意** したいのは、これらの保護の間に構文的な相違はない - すべて式である。ただし意味定義レベルで区別することは可能だ。

排他制御述語は、クラスのすべての操作が相互に排他的に実行されるべきか、または一連の操作が互いに相互に排他的に実行されるべきか、をユーザーが指定することを許す。1 つの 排他制御述語内に現れる操作は、同様に他の排他制御述語内にも現れることが許され、さらに通常の許可述語において用いられることも可能である。各々の 排他制御述語は、名称リストで述べられた各々の操作に対する履歴保護を用いることで、暗黙に許可述語に翻訳されるであろう。たとえば、

```
sync
  mutex(opA, opB);
  mutex(opB, opC, opD);
  per opD => someVariable > 42;
```

これは以下のような許可述語に翻訳される:

```
sync
  per opA => #active(opB) = 0;
  per opB => #active(opA) = 0 and
             #active(opC) + #active(opD) = 0;
  per opC => #active(opB) + #active(opD) = 0;
  per opD => #active(opB) + #active(opC) = 0 and
             someVariable > 42;
```

各操作に対して 1 つの許可述語のみが許されることに注意しよう。#active 演算子は以下で説明される。

mutex(all) 制約は、そのクラス およびスーパークラス 内において記述された操作すべてが、相互に排他的に実行されるべきであることを指定する。

15.1.1 履歴保護

意味定義: 履歴保護とは、履歴式に関して式化されたオブジェクト操作の初期発動の列に依存する保護である (第 7.22 節参照)。履歴式は操作の発動と完了の数を表示するが、それぞれは関数#act と #fin として与えられる。

#act: 操作名称 $\to \mathbb{N}$
#fin: 操作名称 $\to \mathbb{N}$

そのうえ、#active(A) = #act(A) - #fin(A) といった導出された関数 #active が利用できることで、 A の現在発動中のインスタンス数が得られる。もう 1 つの履歴関数 - #req - は第 15.1.3 節で定義される。

例題: 10 の同時接続を支える能力を持ちさらに 100 の要求を保持できる Web サーバー を考える。この場合、URL からローカルなファイルへの写像を表す 1 つのインスタンス変数をもつことになる:

```
instance variables
  site_map : map URL to Filename := {|->}
```

以下に述べる操作はこのクラス中に定義される (簡略のため定義は省略):

ExecuteCGI:	URL ==> File	CGI スクリプトをサーバー上で実行させる
RetrieveURL:	URL ==> File	html のページを送る
UploadFile:	File * URL ==> ()	サーバー上にファイルをアップロードする
ServerBusy:	() ==> File	“server busy” ページを送る
DeleteURL:	URL ==> ()	不要ファイルを取り除く

サーバーは 10 の同時接続だけは保持することができるので、すでに発動されている数が 10 に満たない場合は、実行または回復の操作が発動される許可だけは与えられる:

```
per RetrieveURL => #active(RetrieveURL) +
                   #active(ExecuteCGI) < 10;
per ExecuteCGI  => #active(RetrieveURL) +
                   #active(ExecuteCGI) < 10;
```

15.1.2 オブジェクト状態保護

意味定義: オブジェクト状態保護は、オブジェクト自身の 1 つ (またはそれ以上) のインスタンス変数の値に依存するブール式である。オブジェクト状態保護は操作である事前条件とは異なり、そこにおいて許可述語が偽である操作の呼出しは、その述語が条件を満たすまで呼出しはブロックされる結果となる。一方で、事前条件が偽となる操作の呼出しとは、その操作の行動は指定されていないことを意味する。

例題: web サーバーの例を再び用いるが、いくつかのファイルがすでに存在する場合にファイル削除のみを許可することができる:

```
per DeleteURL   => dom site_map <> {}
```

スタックオブジェクトにおいて操作 Push および Pop を安全に実行するための制約は、次のようなオブジェクト状態保護を用いて式化できる:

```
per Push => length < maxsize;

per Pop => length > 0
```

ここでの maxsize と length はスタックオブジェクトのインスタンス変数である。

たとえば次はスタックの空状態であるが、履歴結果としてこのような制約を式化することが多くの場合に可能である:

```
length = 0 <=> #fin(Push) = #fin(Pop)
```

ただしサイズというのは、特定のスタックインスタンスのプロパティとしてよくみなされるが 1 つのプロパティであるので、このような場合は、履歴の結果を保存する利用可能なインスタンス変数を用いる方がより洗練されている。

15.1.3 キュー条件保護

意味定義: キュー条件保護は、操作の実行のために列をなして待つ要求のもとで働く。これは第 3 の履歴関数 #req の使用を必要とするが、#req(A) は操作 A の実行を要求したオブジェクトが受け取る伝達の数を数えるものである。再び以下の関数 #waiting を導入することが有効だ: これはキューの項目数を数える。

例題: 再び web サーバーで、もし 100 あるいはそれより多くの接続が待ち状態にある場合に、ServerBusy 操作を発動することだけが可能である:

```
per ServerBusy  => #waiting(RetrieveURL)
                 + #waiting(ExecuteCGI) >= 100;
```

このようなキュー状態関数を含む式の最も重要な用い方に、操作間での優先順位を式化するための使用がある。次にプロトコルを示す:

```
per B => #waiting(A) = 0
```

これは A の起動を待つ要求に対して優先権を与える。しかしながら、操作派遣が要求待ち状態に依存する場合、多くの他の状況が存在する。要求到着時刻に基づく操作選択指示を許可するための、あるいは‘次に最も不足するジョブ’行動を記述するための、要求キューの全記述がこれからの開発に委ねられている。

#req(A) は操作 A の初動に対する許可述語の評価では、値 1 をもつことに注意しよう。これは、次のようにすれば常にブロックするであろう。

```
per A => #req(A) = 0
```

15.1.4 保護の評価

前の例を用いて、次の状況を考えよう: つまり web サーバーはすでに 10 RetrieveURL の要求に対処している。これらの要求を処理する間に、更に 2 つの RetrieveURL 要求 (オブジェクト O_1 と O_2 から) と 1 つの ExecuteCGI 要求 (オブジェクト O_3 から) を受けた。これら 2 つの操作に対する許可述語は、発動中の RetrieveURL 操作数がすでに 10 なので、偽である。このようにこれらのオブジェクトはブロックをおこなう。

その後、起動中の RetrieveURL 操作の 1 つが完了へと到達する。そこまで O_1、O_2、O_3 をブロックしていた許可述語が、同時に “真” となるであろう。ここで疑問がおきる: どのオブジェクトが先に進むことを許されるのであろうか？またはそれらすべてもなのか？

保護式はイベントが起きたとき (この場合 RetrieveURL 操作の完了時) のみ、再評価される。それに加えて、あるオブジェクトによる許可述語のテストおよび (潜在する) 発動は、原子的な操作である。このことは、最初のオブジェクトがその保護式を評価するとき、真であることを発見し相応の操作 (この場合は RetrieveURL または ExecuteCGI) を発動するであろう、ということを意味する。保護式を評価する他のオブジェクトはその後、#active(RetrieveURL) + #active(ExecuteCGI) = 10 であること、またこのようにいまだにブロックされていることを発見するであろう。どのオブジェクトが最初に保護式の評価を許されるかは未定義である。

発動時にのみ保護式を真 と評価しなければならないことを理解することが重要である。例の中では、O_1、O_2、O_3 の要求が発動されるやいなやその保護式は再び偽となる。

15.2 同期制約の継承

スーパークラスにおいて記述された同期制約は、そのサブクラスにおいて継承される。これを行う方法はある種の同期に依存するものである。

15.2.1 排他制御制約

基底クラスおよび派生クラスからの排他制御制約は簡単に加えられる。もし基底クラスおよび派生クラスが各々で排他制御定義 M_A と M_B をもつ場合は、派生クラスはすんなりと排他制御制約 M_A と M_B の両方をもつことになる。実際の操作に対する操作名称の束縛は、常に制約が定義されたクラス内で行われる。そのために、スーパークラスで定義されサブクラスで継承された mutex(all) 制約は基底クラスからの操作を相互に排他的にすることのみを行い、派生クラスの操作に影響を与えることはない。

排他制約の継承は、許可述語に対する継承図式に全体的に類似している。内部的には排他制約は常に拡張されて適当な許可述語となり、1 つの結合として存在する許可述語に加えられる。この継承図式では、排他制御定義が基底クラス中で拡張されて許可述語として継承されているか、または、排他制御定義が排他制御定義として継承され派生クラスでのみ拡張されているかにかかわらず、結果は同じであることを保証するものである。

同期制約を現在行われている方法で継承するということは、どのような派生クラスも少なくとも基底クラスの制約を満たす、ということを保証することである。それに加えて、同期制約を強化することも可能である必要がある。以下に述べる例のように、派生クラスが新しい操作を追加する場合にこのことが必要となる可能性がある:

```
class A
  operations
```

```
    writer: () ==> () is not yet specified

    reader: () ==> () is not yet specified

  sync
    per reader => #active(writer) = 0;
    per writer => #active(reader, writer) = 0;
end A

class B is subclass of A
  operations

    newWriter: () ==> () is not yet specified

  sync
    per reader => #active(newWriter) = 0;
    per writer => #active(newWriter) = 0;
    per newWriter => #active(reader, writer, newWriter) = 0;

end B
```

クラス A は、多重読込み単一書出しプロトコルを指定する許可述語を含み、読込みと書出しの操作を実装する。派生クラス B は newWriter を追加している。決定動作を確定するために、 B は更に継承された操作に対する許可述語を追加しなければならない。

派生クラスにおける実際の許可述語は、そのため次のようになる:

```
per reader => #active(writer)=0 and #active(newWriter)=0;
per writer => #active(reader, writer)=0 and #active(newWriter)=0;
per newWriter => #active(reader, writer, newWriter)=0;
```

あるサブクラスが基底クラスからの操作を上書きしたときには、特殊な状況が起こる。操作の上書きは新しい操作として扱われる。1 つでもサブクラスで定義されないかぎり、許可述語をもたない (特別な継承においてももたない) ことになる。

上書された操作に対する排他制御制約を継承することの意味定義は、全体として次のことと類似する：新しく定義された上書き操作は、基底クラス中の同じ名称の操作に対する排他制御定義によって制限されることはない。mutex(all) 省略形は、すべての継承されたまたはローカルに定義された操作を相互に排他的にするものである。上書きされた操作 (基底クラスで定義されたもの) はなんら影響をうけない。言いかえれば、すべての操作、つまり限定されない名称で呼ばれる可能性のあるもの (“ローカルに見える操作”) は互いに排他制御となる。

16 スレッド

スレッド部をもつクラスからインスタンス化されたオブジェクトを、**能動的** オブジェクトと呼ぶ。現クラス内にあるインスタンス変数と操作のスコープは、スレッド記述にまで拡張するものと考えられる。

構文: スレッド定義 = ‘thread’, [スレッド定義] ;

スレッド定義 = 周期スレッド定義
| 手続きスレッド定義 ;

サブクラスはスーパークラスからスレッドを継承する。あるクラスが複数のクラスから継承をおこなっている場合には、それらのクラス中の 1 つだけは自身のスレッドを (もしかすると継承によって) 宣言しているかもしれない。さらに、あるサブクラス中で明示的にスレッドを宣言することは、何らかの継承されたスレッドを上書きすることになる。

16.1 周期スレッド定義

周期スレッド定義は、あるスレッド内の活動を記述する暗黙の方法とみなすことができる。

構文: 周期スレッド定義 = 周期義務 ;

周期義務 = 'periodic','(', 数値, 数値, 数値,
数値, ')', '(', 名称, ')' ;

意味定義: それぞれの周期的なスレッドに関して、4 つの異なった番号が使用されている。それらは出現の順になっている:

1. **period:** これは、負またゼロでない値であり、厳密に周期的なイベントの流れ (jitter = 0) で 2 つの隣り合ったイベント間の時間間隔の長さを述べる
2. **jitter:** これは、負でない値であり、単一のイベントの周りで許されている時間の変化量を述べるその間隔はバランスのとれていると仮定する [-j、j] jitter は特徴付けるための周期より大きくなることを、いわゆる event bursts を許すことに注意する
3. **delay:** これは、2 つの隣り合ったイベント間の到着距離の内部における最小値を示すために使われる周期よりも小さい負でない値である
4. **offset:** これは、負でない値であり、イベントの流れが始まった最初の周期の時間値の絶対値を示すために使われる最初のイベントはその間隔 [offset, offset+ jitter] で発生することに注意する

1 つの定義された時間単位 ΔT が与えられているとすると、周期義務をもつスレッドが 長さが**周期**の各時間間隔の最初に、記載された操作を発動する。これは操作の周期的実行を生み出し、インスタンス変数、パラメーター値、もしかしたら操作発動を通して得るその他の外部値も含めた値間で保持されるべき永続関係に、不連続な等価を与える役を演じているのである。この間隔の長さを動的に変えることはできない。

周期義務は、たとえば (転写関数などの) 公式中の値間のアナログな物理的な関係やそれらの離散イベントのシミュレーションなどを、記述することを意図している。操作の実行時間は少なくとも用いられている周期時間の長さより小さいものであることを保障するのが、実装上要求されることの 1 つである。他の操作が存在する場合は、内部的にも用いられ外部からの発動に対しても利用される時間断片について判断をくだすことにより、これらの他の操作の発動に対する公平な基準が保持されることを、ユーザーが保証しなくてはならない。

周期スレッドは、対応するクラスのインスタンスが生成されたときには、生成されても始まってもいない。そのかわりスタート文は、手続きスレッドと同様、周期スレッドとともに用いられるべきである。

例題: 自分自身のスレッド中にあって周期的に時計を進めるタイマークラスを考えよう。これはスタートの操作をはじめ、計測のストップ、さらに現時刻の読出しを提供する。

```
class Timer
```

タイマーは、現時刻およびタイマーが活動中か否かを示すフラグという 2 つのインスタンス変数をもつ (現時刻のみはタイマーの活動中に増加する)。

```
instance variables
curTime : nat := 0;
active  : bool := false;
```

タイマーは、それ以上の説明は不要の素直な操作を提供する。

```
operations
public Start : () ==> ()
Start() ==
  (active := true;
   curTime := 0);

public Stop : () ==> ()
Stop() ==
  active := false;

public GetTime : () ==> nat
GetTime() ==
  return curTime;

IncTime: () ==> ()
IncTime() ==
  if active
  then curTime := curTime + 100;
```

このタイマーのスレッドは、現時刻が増加していることを保証する。 これが行われる期間は 1000 秒単位である。許容 jitter は 10 秒単位であり、2 つのインスタンス間の最小間隔は 200 秒単位である。そして、最終的にオフセットは全く使用されない。

```
    thread
    periodic(1000,10,200,0)(IncTime)

end Timer
```

16.2 手続きスレッド定義

手続きスレッドは、**文**の使用を通して活動中のオブジェクトの外部動作を陽に定義する仕組みを提供するが、そのオブジェクトがスタートしたときに実行されるものである (第 13.14 節参照)。

構文: 手続きスレッド定義 = 文 ;

意味定義: 手続きスレッドは、そのスレッドを所有するオブジェクトへのスタート文適用に続いて、実行スケジュールがなされる。スレッド内の文はその後連続して実行され、文の実行が完了したときにスレッドは消滅する。多重スレッド間の同期は、共有オブジェクトにおける許可述語を用いることで達成される。

例題: 以下の例は手続きスレッドを用いて、与えられた整数の階乗を同時的に計算することを実演する。

```
class Factorial

instance variables
  result : nat := 5;
operations

public factorial : nat ==> nat
factorial(n) ==
  if n = 0 then return 1
  else (
    dcl m : Multiplier;
    m := new Multiplier();
    m.calculate(1,n);
    start(m);
```

```
    result:= m.giveResult();
    return result
  )

end Factorial

class Multiplier

instance variables
  i : nat1;
  j : nat1;
  k : nat1;
  result : nat1

operations

public calculate : nat1 * nat1 ==> ()
calculate (first, last) ==
  (i := first; j := last);

doit : () ==> ()
doit() ==
  (
   if  i = j then result := i
   else (
     dcl p : Multiplier;
     dcl q : Multiplier;
     p := new Multiplier();
     q := new Multiplier();
     start(p);start(q);
     k := (i + j)  div 2;
     -- 切下げの除算
     p.calculate(i,k);
     q.calculate(k+1,j);
     result := p.giveResult() *  q.giveResult ()
    )
```

```
  );


public giveResult : () ==> nat1
giveResult() ==
  return result;

sync
-- 列計算のみを許す繰返し制約
-- ; doit; giveResult

per doit => #fin (calculate) > #act(doit);
per giveResult => #fin (doit) > #act (giveResult);
per calculate => #fin (giveResult) = #act (calculate)

thread
  doit();

end Multiplier
```

17 traces定義

テスト工程を自動化するために、VDM++は網羅的テストを可能にするtraces記法を含んでいる。tracesはテストしたい操作に対する、全ての組み合わせを表すことに用いられる。これはある意味、記号ではなく、実数を取り扱うこと以外は、限定的にモデル検査と類似している。しかしながら、エラーを起こしたテストケースをフィルターにかけた上で取り除かれ、さらに同じプレフィックスを持つ他のテストケースは自動的にスキップされる。

構文: traces定義 = 'traces', { traces名 } ;

traces名 = 識別子, { '/', 識別子 }, ':', traces定義リスト ;

traces定義リスト = traces定義項, { ';', traces定義項 } ;

```
traces定義項 = traces定義項
             | traces定義項, '|', traces定義項 ;

traces定義項 = tracesコア定義
             | traces束縛群, tracesコア定義
             | tracesコア定義, traces繰り返しパターン
             | traces束縛群, tracesコア定義, traces繰り返しパターン ;

tracesコア定義 = traces適用式
               | traces括弧式 ;

traces適用式 = 識別子, '.', 識別子, '(', 式リスト, ')' ;

traces繰り返しパターン = '*'
                       | '+'
                       | '?'
                       | '{', 数値リテラル, '}'
                       | '{', 数値リテラル, ',' 数値リテラル, '}' ;

traces括弧式 = '(', traces定義リスト, ')' ;

traces束縛群 = traces束縛, { traces束縛 } ;

traces束縛 = 'let', ローカル定義, { ',', ローカル定義 }, 'in'
           | 'let', 束縛, 'in'
           | 'let', 束縛, 'be', 'st', 式, 'in' ;
```

意味定義: 意味定義的に、クラスで提供される traces 定義は効果がない。これらの定義は、組み合わせテスト（オールペアテストと同様に）からの法則を用い、単に VDM++モデルのテストを増強するために使用される。したがって、traces 定義は、VDM++モデルをテストするために、異なる操作が実行されるべきテストシーケンスについて記述する正規表現と見なすことができる。traces 定義の中には束縛が現れる可能性がある。そのような束縛が実現することは、個々のテストケースを自動的に導き出すことである。つまり、1 つの traces 定義が 1 つのテストケース集合に拡大するということだ。このような意味で、テストケースは互いに実行された操作の系列である。各テストケース間で、VDM++モデルは初期化される。したがって、それらは完全に独立したようになる。静的意味定義の観点から、traces 定義の中で

使われる式は、その式の過程で実行されなければならないことに注意することは重要だ。これは、直接インスタンス変数を参照することができないことを意味する。なぜなら、インスタンス変数は実行の間、変更することができるからだ。

異なる種類の繰り返しパターンは以下の意味を持つ。

- '*' 0 から n 回発生する（n はツールの仕様）
- '+' 1 から n 回発生する（n はツールの仕様）
- '?' 0 か 1 回発生する
- '{', n, '}' n 回発生する
- '{', n, ',' m '}' n から m 回発生する

例: 以下の例では、Reset の呼び出しでスタートし、1 から 4 回スタックに Push し、1 から 3 回スタックから Pop されるような、全ての可能なテストケースの組み合わせが生成される。

```
class Stack

  instance variables
    stack : seq of int := [];

  operations

    public Reset : () ==> ()
    Reset () ==
      stack := [];

    public Pop : () ==> int
    Pop() ==
      def res = hd stack in
        (stack := tl stack;
         return res)
    pre stack <> []
    post stack~ = [RESULT] ^ stack;

    public Push: int ==> ()
```

```
    Push(elem) ==
      stack := stack ^ [elem];

    public Top : () ==> int
    Top() ==
      return (hd stack);

end Stack
class UseStack

instance variables

  s : Stack := new Stack();

traces

  PushBeforePop : s.Reset(); (let x in set 1,2 in s.Push(x)){1,4};
                  s.Pop(){1,3}

end UseStack
```

18 VDM++と ISO /VDM-SL の相違点

VDM++ のこの版は ISO/VDM-SL 標準を基本とするが、少しだけ異なる点がある。これらの相違は構文上および意味定義上の両面にあり、主に言語の拡張に起因するもので VDM++ 構成要素を実行可能なものにしようとする要求に原因がある[23]。

VDM++ と ISO/VDM-SL の間の大きな違いは、 VDM++で利用できるオブジェクト指向と同時処理 の拡張である。これはいくつかの構文上の違いを引起す。

一番には、VDM++ 仕様記述はクラス定義の集合で構成される。平坦な ISO/VDM-SL 仕様記述は取り入れていない。VDM++の定義節に関して、以下に述べるような ISO/VDM-SL との違いが存在する:

[23] ここでの意味定義とはインタープリタの意味定義のことである。

構文上の相違:

- 標準では部分列構成要素間 (たとえば関数定義間) の分離符としてセミコロン (";") が使われる。VDM++ ではこの規則に、このような構成要素の列の最後尾に随意でセミコロンをつけることができることを付け加える。この変更は以下に述べる構文上の定義に対しても適用される (付録 A を参照) : **型定義**, **値定義**, **関数定義**, **操作定義**, *def* **式**, *def* **文**, **ブロック文**。
- 陽関数定義および操作定義においては、 VDM++ におけるオプションの事後条件を指定することが可能である (第 6 節と第 12 節、または第 A.4.3 節か A.4.4 節を参照)。
- 陽関数定義および操作定義の本体は 節 is subclass responsibility と is not yet specified を用いて仮の方法で指定することができる。
- 陽関数定義および操作定義に対する拡張形式が組み入れられてきた。拡張は、陰仕様定義に用いられたのと同様の見出しの使用を、関数と操作の定義で可能にするものである。これはまず最初に陰仕様定義を書くことをより容易にし、そしてアルゴリズム部分を後に続けて加えることを容易にする。加えて、結果識別子の型ペアは 2 つ以上の識別子とともに働くために生成されたものである。
- *if* 文 の中で "else" 部はオプションである (第 13.5 節または第 A.7.3 節参照)
- 空集合と空列は直接にパターンとして用いることができる (第 8 節か A.8.1 節参照)
- "制限する写像定義域" と "制限される写像定義域" は適切にグループ化される (第 C.7 節参照)
- 写像型構成子に対する演算子優先順位は標準と異なる (第 C.8 章参照)
- VDM++ においては、組選択、型判断、事前条件式が加わる
- VDM++ においては、原子代入文が加わる
- VDM++ においては、 **定義** が **インスタンス変数定義**、**スレッド定義**、**同期定義**にて拡張される
- VDM++ においては、以下の式が加わる: *new* **式**, *self* **式**, *isofbaseclass* **式**, *isofclass* **式**, *samebaseclass* **式**, *sameclass* **式**, *act* **式**, *fin* **式**, *active* **式** , *req* **式**, *waiting* **式**

- VDM++ においては、以下の文が加わる: **仕様記述文**, *select* **文**, *start* **文**そして *startlist* **文**
- VDM-SL 状態定義は VDM++ インスタンス変数に置き換えられた。

意味定義上の相違 (wrt. インタープリタ):

- VDM++ は条件論理によってのみ動作する (第 4.1.1 節参照)。
- VDM++ においては、相互に再帰する値定義は実行不可能であり、またそれらは用いられる前に定義されているように順序付けられなければならない (第 10 節参照)。
- *let* 文と *let* 式におけるローカル定義は再帰的に定義されることは許されない。さらにそれらは用いられる前に定義されているように順序付けられなければならない (第 7.1 節と第 13.1 節参照)。
- VDM++ における数値型 rat は型 real と同じ型を表す (第 4.1.2 節参照)。
- ISO/VDM-SL において用いられるインタープリタ実行の自由度の 2 つの形式 は '劣決定系' と '非決定系である。ISO/VDM-SL の操作における自由度では、関数に対して劣決定系である場合はすべて非決定系となる。VDM++ においては、操作と関数の両方における自由度は劣決定系である。これはしかしながら、標準と一致するものでもある、なぜならインタープリタは単に仕様記述に対する可能な様式のひとつに相応するからである。

19 静的意味

構文規則に従った構文的に正しい VDM 仕様記述でも、必ずしも言語の型やスコープの規則に従ってはいない。VDM 仕様記述が良形であるかについては、**静的意味チェッカー**によって検査することができる。Toolbox にはこのような静的意味チェッカー (プログラム言語では通常は型検査と呼ばれる) が存在する。

一般的に、与えられた VDM 仕様記述が良形か否かは、静的に決定可能であるとはいえない。VDM++ の静的意味は他の言語の静的意味とは異なる。他の言語は絶対的に良形だとはいえない仕様記述のみを拒絶し、また絶対的に良形である仕様記述のみを受け入れる。VDM++ の静的意味は、VDM 仕様記述に対する

良形である度合 があるものと考える。このような良形である度合は、仕様記述が絶対的に良形であるか、絶対的に良形でないか、恐らく良形か、を示すものである。

このことは Toolbox において、静的意味チェッカーが、恐らくの正しさかあるいは絶対的な正しさかどちらかをチェックできることを意味する。しかしながら、ただのほんとに単純な仕様記述のみが、絶対的良形であることのチェックにパスすることができるのだ、ということを記しておくべきであろう。したがって、実際的な使用においては “恐らく良形” がもっとも役に立つ。

恐らく良形のチェックと絶対的良形のチェックの間の相違は、以下に続く VDM 仕様記述の断片によって実例をもって示すことができる:

```
if a = true
then a + 1
else not a
```

ここで a は型 nat | bool (nat と bool の合併型) をもっている。もし a が true と等しいならば、そのとき a に 1 を加えることは不可能となるであろうから、この式は悪形であると読者は簡単に理解することができる。しかしながら、このような式は恣意的に複雑になり得るので、一般的にはこれが静的にチェックされる可能性はない。この特別な例において、絶対的な良形であることは false となる一方で、恐らく良形であることは true となるであろう。

20 スコープ衝突

名前衝突は、同じ名称の (つまり 同じ **識別子**によって識別された)2 つの構成要素が同じスコープ内に見えているときにおきる。2 つのこのような構成要素、たとえば同じ名称の型と操作、が同じ言語の範疇にはないときに、これはまた真である。名前衝突のある仕様記述は誤っているものとみなされる。

両方の構成要素が同じクラスで定義されていたら、その場合には構成要素の 1 つの名称をつけ直す以外に衝突を解決することはできない。もしそれらが異なるクラスで定義されているならば、その場合に衝突は **名前限定**を通して解決することができる、つまり構成要素のひとつは、そこで定義されたクラスの名称と ‘‘’ (バッククォート) 分離符を前に付ける、たとえば次のように。

```
types
  Queue = seq of ComplexTypes`RealNumber
```

名前限定は、クラス ComplexTypes の中で定義された型 RealNumber に関して 型キュー を定義するために用いられる。

クラス名称が名前衝突を解決するために用いられるような名前限定のみが、分離符として ‘`’ 記号を用いることに注意しよう;‘.’ (ドット) 記号は通常の値やあるいはオブジェクトを ‘限定’ するために用いられる。たとえばこの表記

```
o.i
```

これはオブジェクトのインスタンス変数 i または合成値 (レコード) o の項目 i を参照することが許される。

参考文献

[Ada83] Reference manual for the ada programming language. Technical report, United States Government (Department of Defence), American National Standards Institute, 1983.

[Daw91] John Dawes. *The VDM-SL Reference Guide*. Pitman, 1991. ISBN 0-273-03151-1.

[Dür92] E.H.H. Dürr. Syntactic description of the vdm++ language. Technical report, CAP Gemini, P.O.Box 2575, 3500 GN Utrecht, NL, September 1992.

[FJ98] J.S. Fitzgerald and C.B. Jones. *Proof in VDM: case studies*, chapter Proof in the Validation of a Formal Model of a Tracking System for a Nuclear Plant. Springer-Verlag FACIT Series, 1998.

[Jon90] Cliff B. Jones. *Systematic Software Development Using VDM*. Prentice-Hall International, Englewood Cliffs, New Jersey, second edition, 1990. ISBN 0-13-880733-7.

[P. 96] P. G. Larsen and B. S. Hansen and H. Brunn N. Plat and H. Toetenel and D. J. Andrews and J. Dawes and G. Parkin and others. Information technology — Programming languages, their environments and system software interfaces — Vienna Development Method — Specification Language — Part 1: Base language, December 1996.

[Pau91] Lawrence C. Paulson. *ML for the Working Programmer*. Cambridge University Press, 1991.

A VDM++構文

この付録では VDM++の全構文を示す。

A.1 文書

文書 = クラス | システム, { クラス | システム } ;

A.2 システム

システム = 'system', 識別子,
[クラス本体],
'end', 識別子 ;

A.3 クラス

クラス = 'class', 識別子, [継承節],
[クラス本体],
'end', 識別子 ;

継承節 = 'is subclass of', 識別子, ',', { 識別子 } ;

A.4 定義

クラス本体 = 定義ブロック, { 定義ブロック } ;

定義ブロック = 型定義群
| 値定義群
| 関数定義群
| 操作定義群
| インスタンス変数定義

| 同期定義
| スレッド定義
| traces 定義 ;

A.4.1 型定義

型定義群 = 'types', [アクセス型定義,
{ ';', アクセス型定義 }, [';']] ;

アクセス型定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
型定義 ;

アクセス = 'public'
| 'private'
| 'protected' ;

型定義 = 識別子, '=', 型, [不変条件]
| 識別子, '::', 項目リスト, [不変条件] ;

型 = 括弧型
| 基本型
| 引用型
| レコード型
| 合併型
| 組型
| 選択型
| 集合型
| 列型
| 写像型
| 部分関数型
| 型名称
| 型変数 ;

括弧型 = '(', 型, ')' ;

基本型 = 'bool' | 'nat' | 'nat1' | 'int' | 'rat'
| 'real' | 'char' | 'token' ;

引用型 = 引用リテラル ;

レコード型 = 'compose', 識別子, 'of', 項目リスト, 'end' ;

項目リスト = { 項目 } ;

項目 = [識別子, ':'], 型
| [識別子, ':-'], 型 ;

合併型 = 型, '|', 型, { '|', 型 } ;

組型 = 型, '*', 型, { '*', 型 } ;

選択型 = '[', 型, ']' ;

集合型 = 'set of', 型 ;

列型 = 空列を含む列型
| 空列を含まない列型 ;

空列を含む列型 = 'seq of', 型 ;

空列を含まない列型 = 'seq1 of', 型 ;

写像型 = 一般写像型
| 1 対 1 写像型 ;

一般写像型 = 'map', 型, 'to', 型 ;

1 対 1 写像型 = 'inmap', 型, 'to', 型 ;

関数型 = 部分関数型
| 全関数型 ;

部分関数型 = 任意の型, '->', 型 ;

全関数型 = 任意の型, '+>', 型 ;

任意の型 = 型
| '(', ')' ;

型名称 = 名称 ;

型変数 = 型変数識別子 ;

不変条件 = 'inv', 不変条件初期関数 ;

不変条件初期関数 = パターン, '==', 式 ;

A.4.2 値定義

値定義群 = 'values', [アクセス値定義,
{ ';', アクセス値定義 }, [';']] ;

アクセス値定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
値定義 ;

値定義 = パターン, [':', 型], '=', 式 ;

A.4.3 関数定義

関数定義群 = 'functions', [アクセス関数定義,
{ ';', アクセス関数定義 }, [';']] ;

アクセス関数定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
関数定義 ;

関数定義 = 陽関数定義
| 陰関数定義
| 拡張陽関数定義 ;

陽関数定義 = 識別子, [型変数リスト], ':',
関数型,
識別子, パラメーターリスト,
'==', 関数本体,
['pre', 式],
['post', 式],
['measure', 名称] ;

陰関数定義 = 識別子, [型変数リスト],
パラメーター型,
識別子型ペアリスト,
['pre', 式],
'post', 式 ;

拡張陽関数定義 = 識別子, [型変数リスト],
パラメーター型,
識別子型ペアリスト,
'==', 関数本体,
['pre', 式],
['post', 式] ;

型変数リスト = '[', 型変数識別子,
{ ',', 型変数識別子 }, ']' ;

識別子型ペア = 識別子, ':', 型 ;

パラメーター型 = '(', [パターン型ペアリスト], ')' ;

識別子型ペアリスト = 識別子, ':', 型,
{ ',', 識別子, ':', 型 } ;

パターン型ペアリスト = パターンリスト, ':', 型,
{ ',', パターンリスト,':', 型 } ;

パラメーターリスト = パラメーター群, { パラメーター群 } ;

パラメーター群 = '(', [パターンリスト], ')' ;

関数本体 = 式
| 'is not yet specified'
| 'is subclass responsibility' ;

A.4.4 操作定義

操作定義群 = 'operations', [アクセス操作定義,
{ ';', アクセス操作定義 }, [';']] ;

アクセス操作定義 = (['async'] [アクセス], ['static'])
| (['async'] ['static'], [アクセス]),
操作定義 ;

操作定義 = 陽操作定義
| 陰操作定義
| 拡張陽操作定義 ;

陽操作定義 = 識別子, ‘:’, 操作型,
識別子, パラメーター群,
‘==’, 操作本体,
[‘pre’, 式],
[‘post’, 式],
;

陰操作定義 = 識別子, パラメーター型,
[識別子型ペアリスト],
陰操作本体 ;

陰操作本体 = [外部節],
[‘pre’, 式],
‘post’, 式,
[例外] ;

拡張陽操作定義 = 識別子, パラメーター型,
[識別子型ペアリスト],
‘==’, 操作本体,
[外部節],
[‘pre’, 式],
[‘post’, 式],
[例外] ;

操作型 = 任意の型, ‘==>’, 任意の型 ;

操作本体 = 文
| ‘is not yet specified’
| ‘is subclass responsibility’ ;

外部節 = ‘ext’, var 情報, { var 情報 } ;

var 情報 = モード, 名称リスト, [‘:’, 型] ;

モード = 'rd' | 'wr' ;

例外 = 'errs', エラーリスト ;

エラーリスト = エラー, { エラー } ;

エラー = 識別子, ':', 式, '->', 式 ;

A.4.5 インスタンス変数定義

インスタンス変数定義群 = 'instance', 'variables',
[インスタンス変数定義,
{ ';', インスタンス変数定義 }] ;

インスタンス変数定義 = アクセス指定定義
| 不変条件定義 ;

アクセス指定定義 = ([アクセス], ['static']) | (['static'], [アクセス]),
指定定義 ;

不変条件定義 = 'inv', 式 ;

A.4.6 同期定義

同期定義 = 'sync', [同期] ;

同期 = 許可述語 ;

許可述語 = 許可述語,
{ ';', 許可述語 } ;

許可述語 = 'per', 名称, '=>', 式
| 排他制御述語 ;

排他制御述語 = 'mutex', '(', 'all', ')'
| 'mutex', '(', 名称リスト ')' ;

A.4.7 スレッド定義

スレッド定義 = 'thread', [スレッド定義] ;

スレッド定義 = 手続きスレッド定義 ;

周期スレッド定義 = 周期義務 ;

周期義務 = 'periodic','(', 数値, 数値, 数値,
数値, ')', '(', 名称, ')' ;

手続きスレッド定義 = 文 ;

A.4.8 traces 定義

traces 定義 = 'traces', { traces 名 } ;

traces 名 = 識別子, { '/', 識別子 }, ':', traces 定義リスト ;

traces 定義リスト = traces 定義項, { ';', traces 定義項 } ;

traces 定義項 = traces 定義
| traces 定義項, '|', traces 定義 ;

traces 定義 = traces コア定義
| traces 束縛群, traces コア定義
| traces コア定義, traces 繰り返しパターン
| traces 束縛群, traces コア定義, traces 繰り返しパターン ;

traces コア定義 = traces 適用式
| traces 括弧式 ;

traces 適用式 = 識別子, '.', 識別子, '(', 式リスト, ')' ;

traces 繰り返しパターン = '*'
| '+'
| '?'
| '{', 数値リテラル, '}'
| '{', 数値リテラル, ',' 数値リテラル, '}' ;

traces 括弧式 = '(', traces 定義リスト, ')' ;

traces 束縛群 = traces 束縛, { traces 束縛 } ;

traces 束縛 = 'let', ローカル定義, { ',', ローカル定義 }, 'in'
| 'let', 束縛, 'in'
| 'let', 束縛, 'be', 'st', 式, 'in' ;

A.5 式

式リスト = 式, { ',', 式 } ;

式 = 括弧式
| let 式
| let be 式
| def 式
| if 式

- cases 式
- 単項式
- 2 項式
- 限量式
- iota 式
- 集合列挙
- 集合内包
- 集合範囲式
- 列列挙
- 列内包
- 部分列
- 写像列挙
- 写像内包
- 組構成子
- レコード構成子
- レコード修正子
- 適用
- 項目選択
- 組選択
- 関数型インスタンス化
- ラムダ式
- new 式
- self 式
- スレッド ID 式
- 一般 is 式
- 未定義式
- 事前条件式
- isofbaseclass 式
- isofclass 式
- samebaseclass 式
- sameclass 式
- act 式
- fin 式
- active 式
- req 式
- waiting 式

```
    |   time 式
    |   名称
    |   旧名称
    |   記号リテラル ;
```

A.5.1 括弧式

```
括弧式 = '(', 式, ')' ;
```

A.5.2 ローカル束縛式

```
let 式 = 'let', ローカル定義, { ',', ローカル定義 },
         'in', 式 ;

let be 式 = 'let', 束縛, [ 'be', 'st', 式 ], 'in',
            式 ;

def 式 = 'def', パターン束縛, '=', 式,
         { ';', パターン束縛, '=', 式 }, [ ';' ],
         'in', 式 ;
```

A.5.3 条件式

```
if 式 = 'if', 式, 'then', 式,
        { elseif 式 },
        'else', 式 ;

elseif 式 = 'elseif', 式, 'then', 式 ;

cases 式 = 'cases', 式, ':',
           cases 式選択肢群,
           [ ',', others 式 ], 'end' ;
```

cases 式選択肢群 = cases 式選択肢,
{ ',' cases 式選択肢 } ;

cases 式選択肢 = パターンリスト, '->' 式 ;

others 式 = 'others', '->' 式 ;

A.5.4 単項式

単項式 = 接頭辞式
| 逆写像 ;

接頭辞式 = 単項演算子, 式 ;

単項演算子 = 正符号
| 負符号
| 算術絶対値
| 底値
| 否定
| 集合濃度
| 有限べき集合
| 分配的集合合併
| 分配的集合共通部分
| 列先頭
| 列尾部
| 列長
| 列要素
| 列索引
| 分配的列連結
| 写像定義域
| 写像値域
| 分配的写像併合 ;

正符号 = '+' ;

負符号 = '-' ;

算術絶対値 = 'abs' ;

底値 = 'floor' ;

否定 = 'not' ;

集合濃度 = 'card' ;

有限べき集合 = 'power' ;

分配的集合合併 = 'dunion' ;

分配的集合共通部分 = 'dinter' ;

列先頭 = 'hd' ;

列尾部 = 'tl' ;

列長 = 'len' ;

列要素 = 'elems' ;

列索引 = 'inds' ;

分配的列連結 = 'conc' ;

写像定義域 = 'dom' ;

写像値域 = 'rng' ;

分配的写像併合 = 'merge' ;

逆写像 = 'inverse', 式 ;

A.5.5 2 項式

2 項式 = 式, 2 項演算子, 式 ;

2 項演算子 = 加算
| 減算
| 乗算
| 除算
| 整数除算
| 剰余算
| 法算
| より小さい
| より小さいか等しい
| より大きい
| より大きいか等しい
| 相等
| 不等
| 論理積
| 論理和
| 含意
| 同値
| 帰属
| 非帰属
| 包含
| 真包含
| 集合合併
| 集合差
| 集合共通部分
| 列連結
| 写像修正または列修正
| 写像併合
| 写像定義域限定
| 写像定義域削減
| 写像値域限定
| 写像値域削減
| 合成
| 反復 ;

加算 = ‘+’ ;

減算 = ‘-’ ;

乗算 = ‘*’ ;

除算 = ‘/’ ;

整数除算 = ‘div’ ;

剰余算 = ‘rem’ ;

法算 = ‘mod’ ;

より小さい = ‘<’ ;

より小さいか等しい = ‘<=’ ;

より大きい = ‘>’ ;

より大きいか等しい = ‘>=’ ;

相等 = ‘=’ ;

不等 = ‘<>’ ;

論理和 = ‘or’ ;

論理積 = ‘and’ ;

含意 = ‘=>’ ;

同値 = ‘<=>’ ;

帰属 = ‘in set’ ;

非帰属 = ‘not in set’ ;

包含 = ‘subset’ ;

真包含 = ‘psubset’ ;

集合合併 = ‘union’ ;

集合差 = ‘\’ ;

集合共通部分 = ‘inter’ ;

列連結 = ‘^’ ;

写像修正または列修正 = ‘++’ ;

写像併合 = ‘munion’ ;

写像定義域限定 = ‘<:’ ;

写像定義域削減 = ‘<-:’ ;

写像値域限定 = ‘:>’ ;

写像値域削減 = ‘:->’ ;

合成 = ‘comp’ ;

反復 = ‘**’ ;

A.5.6 限量式

限量式 = 全称限量式
| 存在限量式
| 1 存在限量式 ;

全称限量式 = 'forall', 束縛リスト, '&', 式 ;

存在限量式 = 'exists', 束縛リスト, '&', 式 ;

1 存在限量式 = 'exists1', 束縛, '&', 式 ;

A.5.7 iota 式

iota 式 = 'iota', 束縛, '&', 式 ;

A.5.8 集合式

集合列挙 = '{', [式リスト], '}' ;

集合内包 = '{', 式, '|', 束縛リスト,
['&', 式], '}' ;

集合範囲式 = '{', 式, ',', '...', ',',
式, '}' ;

A.5.9 列式

列列挙 = '[', [式リスト], ']' ;

列内包 = '[', 式, '|', 集合束縛,
['&', 式], ']' ;

部分列 = 式, '(', 式, ',', '...', ',',
式, ')' ;

A.5.10 写像式

写像列挙 = '{', 写, { ',', 写 }, '}'
| '{', '|->', '}' ;

写 = 式, '|->', 式 ;

写像内包 = '{', 写, '|', 束縛リスト,
['&', 式], '}' ;

A.5.11 組構成子式

組構成子 = 'mk_', '(', 式, ',', 式リスト, ')' ;

A.5.12 レコード式

レコード構成子 = 'mk_',[24] 名称, '(', [式リスト], ')' ;

レコード修正子 = 'mu', '(', 式, ',',
レコード修正,
{ ',', レコード修正 }, ')' ;

レコード修正 = 識別子, '|->', 式 ;

A.5.13 適用式

適用 = 式, '(', [式リスト], ')' ;

項目選択 = 式, '.', 識別子 ;

組選択 = 式, '.#', 数値 ;

関数型インスタンス化 = 名称, '[', 型, { ',', 型 }, ']' ;

[24] **Note:** 境界文字は許されない

A.5.14 ラムダ式

ラムダ式 = 'lambda', 型束縛リスト, '&', 式 ;

A.5.15 new 式

new 式 = 'new', 名称, '(', [式リスト], ')' ;

A.5.16 self 式

self 式 = 'self' ;

A.5.17 スレッド ID 式

スレッド ID 式 = 'threadid' ;

A.5.18 is 式

一般 is 式 = is 式
| 型判定 ;

is 式 = 'is_',[25] 名称, '(', 式, ')'
| is 基本型, '(', 式, ')' ;

型判定 = 'is_', '(', 式, ',', 型, ')' ;

A.5.19 未定義式

未定義式 = 'undefined' ;

[25] **Note:** 境界文字は許されない

A.5.20 事前条件式

事前条件式 = 'pre_', '(', 式,
[{ ',', 式 }], ')' ;

A.5.21 基底クラス構成要素

isofbaseclass 式 = 'isofbaseclass', '(', 名称, 式, ')' ;

A.5.22 クラス構成要素

isofclass 式 = 'isofclass', '(', 名称, 式, ')' ;

A.5.23 同基底クラス構成要素

samebaseclass 式 = 'samebaseclass', '(', 式,
式, ')' ;

A.5.24 同クラス構成要素

sameclass 式 = 'sameclass', '(', 式,
式, ')' ;

A.5.25 履歴式

act 式 = '#act', '(', 名称, ')'
| '#act', '(', 名称リスト, ')' ;

fin 式 = '#fin', '(', 名称, ')'
| '#fin', '(', 名称リスト, ')' ;

active式 = '#active', '(', 名称, ')'
| '#active', '(', 名称リスト, ')' ;

req式 = '#req', '(', 名称, ')'
| '#req', '(', 名称リスト, ')' ;

waiting式 = '#waiting', '(', 名称, ')'
| '#waiting', '(', 名称リスト, ')' ;

A.5.26 time式

time式 = 'time' ;

A.5.27 名称

名称 = 識別子, ['`', 識別子] ;

名称リスト = 名称, { ',', 名称 } ;

旧名称 = 識別子, '~' ;

A.6 状態指示子

状態指示子 = 名称
| 項目参照
| 写像参照または列参照 ;

項目参照 = 状態指示子, '.', 識別子 ;

写像参照または列参照 = 状態指示子, '(', 式, ')' ;

A.7 文

文 = let 文
| let be 文
| def 文
| ブロック文
| 一般代入文
| if 文
| cases 文
| 列 for ループ
| 集合 for ループ
| 索引 for ループ
| while ループ
| 非決定文
| call 文
| 仕様記述文
| start 文
| startlist 文
| duration 文
| cycles 文
| return 文
| always 文
| trap 文
| 再帰 trap 文
| exit 文
| error 文
| 恒等文 ;

A.7.1 ローカル束縛文

let 文 = 'let', ローカル定義, { ',', ローカル定義 },
'in', 文 ;

ローカル定義 = 値定義
| 関数定義 ;

let be 文 = 'let', 束縛, ['be', 'st', 式], 'in',
文 ;

def 文 = 'def', 相等定義,
{ ';', 相等定義 }, [';'],
'in', 文 ;

相等定義 = パターン束縛, '=', 式 ;

A.7.2 ブロック文と代入文

ブロック文 = '(', { dcl 文 },
文, { ';', 文 }, [';'], ')' ;

dcl 文 = 'dcl', 代入定義,
{ ',', 代入定義 }, ';' ;

代入定義 = 識別子, ':', 型, [':=', 式] ;

一般代入文 = 代入文
| 多重代入文 ;

代入文 = 状態指示子, ':=', 式 ;

多重代入文 = 'atomic', '(' 代入文, ';',
代入文,
{ ';', 代入文 }')' ;

A.7.3 条件文

if 文 = 'if', 式, 'then', 文,
{ elseif 文 },
['else', 文] ;

elseif 文 = 'elseif', 式, 'then', 文 ;

cases 文 = 'cases', 式, ':',
cases 文選択肢群,
[',', others 文], 'end' ;

cases 文選択肢群 = cases 文選択肢,
{ ',', cases 文選択肢 } ;

cases 文選択肢 = パターンリスト, '->', 文 ;

others 文 = 'others', '->', 文 ;

A.7.4 ループ文

列 for ループ = 'for', パターン束縛, 'in', ['reverse'],
式, 'do', 文 ;

集合 for ループ = 'for', 'all', パターン, 'in set', 式,
'do', 文 ;

索引 for ループ = 'for', 識別子, '=', 式, 'to', 式,
['by', 式],
'do', 式 ;

while ループ = 'while', 式, 'do', 式 ;

A.7.5 非決定文

非決定文 = '||', '(', 文,
{ ',', 文 }, ')' ;

A.7.6 call 文と return 文

call 文 = [オブジェクト指定子, '.'],
名称, '(', [式リスト], ')', ;

オブジェクト指定子 = 名称
| self 式
| new 式
| オブジェクト項目参照
| オブジェクト適用 ;

オブジェクト項目参照 = オブジェクト指定子, '.', 識別子 ;

オブジェクト適用 = オブジェクト指定子, '(', [式リスト], ')' ;

return 文 = 'return', [式] ;

A.7.7 仕様記述文

仕様記述文 = '[', 陰操作本体, ']' ;

A.7.8 start 文と startlist 文

start 文 = 'start', '(', 式, ')' ;

startlist 文 = 'startlist', '(', 式, ')' ;

A.7.9 duration 文と cycles 文

duration 文 = 'duration', '(', 数値定数, ')',
文 ;

cycles 文 = 'cycles', '(', 数値, ')',
文 ;

A.7.10 例外処理文

always 文 = 'always', 文, 'in', 文 ;

trap 文 = 'trap', パターン束縛, 'with', 文,
'in', 文 ;

再帰 trap 文 = 'tixe', trap 群, 'in', 文 ;

trap 群 = '{', パターン束縛, '|->', 文,
{ ',', パターン束縛, '|->', 文 }, '}' ;

exit 文 = 'exit', [式] ;

A.7.11 error 文

error 文 = 'error' ;

A.7.12 恒等文

恒等文 = 'skip' ;

A.8 パターンと束縛

A.8.1 パターン

パターン = パターン識別子
| 一致値
| 集合列挙パターン
| 集合合併パターン
| 列列挙パターン
| 列連結パターン
| 組パターン
| レコードパターン ;

パターン識別子 = 識別子 | '-' ;

一致値 = '(', 式, ')'
| 記号リテラル ;

集合列挙パターン = '{', [パターンリスト], '}' ;

集合合併パターン = パターン, 'union', パターン ;

列列挙パターン = '[', [パターンリスト], ']' ;

列連結パターン = パターン, '^', パターン ;

組パターン = 'mk_', '(', パターン, ',', パターンリスト, ')' ;

レコードパターン = 'mk_',[26] 名称, '(', [パターンリスト], ')' ;

パターンリスト = パターン, { ',', パターン } ;

A.8.2 束縛

パターン束縛 = パターン | 束縛 ;

束縛 = 集合束縛 | 型束縛 ;

集合束縛 = パターン, 'in set', 式 ;

型束縛 = パターン, ':', 型 ;

[26] **Note:** 境界文字は許されない

束縛リスト = 多重束縛, { ‘,’, 多重束縛 } ;

多重束縛 = 多重集合束縛
| 多重型束縛 ;

多重集合束縛 = パターンリスト, ‘in set’, 式 ;

多重型束縛 = パターンリスト, ‘:’, 型 ;

型束縛リスト = 型束縛, { ‘,’, 型束縛 } ;

B 語彙

B.1 文字

文字集合は、この文書で用いられた文字形式と共に、 12 表に示される。VDM-SL 標準において文字は次のとおりに定義される:

文字 = 通常文字
| キーワード文字
| 識別文字
| ギリシャ文字
| 数字
| 境界文字
| その他の文字
| 分離符 ;

通常文字とキーワード文字は 12 表 に表示されている (この文書ではキーワード文字は単に相当するアルファベット小文字を用いている)。識別文字は相当するアルファベットの大文字と小文字を用いるが引用文字列は “<” で始め “>” で閉じる (引用文字にはアンダーバーや数字も用いることができることに注目)。ギリシャ文字も数値記号 “#” の後に相当する文字を続けることで使用できる (この情報は

LaTeX pretty printer で用いられ、ギリシャ文字が提示できるようになっている)。全境界文字 (標準 ASCII 版のもの) は表 12 に記述されている。標準では境界文字とそれらの組み合わせには違いをもたせている。ここではこれを違いとして扱わない。数学構文中のいくつかの境界文字が、ここで用いられている ASCII 構文中ではキーワードとなることにも気づいてもらいたい。

文字:

```
a   b   c   d   e   f   g   h   i   j   k   l   m
n   o   p   q   r   s   t   u   v   w   x   y   z
A   B   C   D   E   F   G   H   I   J   K   L   M
N   O   P   Q   R   S   T   U   V   W   X   Y   Z
```

漢字　　ハングル文字

キーワード文字:

```
a   b   c   d   e   f   g   h   i   j   k   l   m
n   o   p   q   r   s   t   u   v   w   x   y   z
```

境界文字:

```
,     :     ;     =     (     )     |     -     [     ]
{     }     +     /     <     >     <=    >=    <>    .
*     ->    +>    ==>   ||    =>    <=>   |->   <:    :>
<-:   :->   &     ==    **    ^     ++
```

数字:

```
0   1   2   3   4   5   6   7   8   9
```

16 進数字:

```
0   1   2   3   4   5   6   7   8   9
A   B   C   D   E   F
a   b   c   d   e   f
```

8 進数字:

```
0   1   2   3   4   5   6   7
```

その他の文字:

```
_   ‘   ’   "   @   ~
```

改行:

空白:

これらはグラフィックな形態をもたないが、空白と行替えを組み合わせる。ここに 2 つの分離符がある: 行替えしない (空白) と行替えを行う (改行) である。

表 12: 文字集合

B.2 記号

以下のような種類の記号が存在する: キーワード、境界文字、記号リテラル、そしてコメント。文字から記号への変換も以下の規則のもとに与えられている; これらは構文定義と同じ表記を用いるが、意味においては続く終了符との間に分離符がないという点で異なる。それ例外の曖昧さが生ずる場所では、2つの連続する記号は分離符によって分離されていなければならない。

```
キーワード = '#act' | '#active' | '#fin' | '#req' | '#waiting' | 'abs'
           | 'all' | 'always' | 'and' | 'async'
           | 'atomic' | 'be' | 'bool' | 'by' | 'card' | 'cases'
           | 'char' | 'class' | 'comp' | 'compose' | 'conc' | 'cycles' | 'dcl'
           | 'def' | 'dinter' | 'div' | 'do' | 'dom' | 'dunion'
           | 'duration' | 'elems' | 'else' | 'elseif' | 'end' | 'error'
           | 'errs' | 'exists' | 'exists1' | 'exit' | 'ext' | 'false' | 'floor'
           | 'for' | 'forall' | 'from' | 'functions' | 'hd' | 'if' | 'in'
           | 'inds' | 'inmap' | 'input' | 'instance' | 'int' | 'inter'
           | 'inv' | 'inverse' | 'iota' | 'is' | 'isofbaseclass'
           | 'isofclass' | 'lambda' | 'len' | 'let' | 'map' | 'measure'
           | 'merge' | 'mod' | 'mu' | 'munion' | 'mutex'
           | 'nat' | 'nat1' | 'new'
           | 'nil' | 'not' | 'of' | 'operations'
           | 'or' | 'others' | 'per' | 'periodic' | 'post' | 'power' | 'pre'
           | 'private' | 'protected' | 'psubset' | 'public' | 'rat'
           | 'rd' | 'real' | 'rem' | 'responsibility' | 'return'
           | 'reverse' | 'rng' | 'samebaseclass' | 'sameclass' | 'self'
           | 'seq' | 'seq1' | 'set' | 'skip' | 'specified' | 'st' | 'start'
           | 'startlist' | 'subclass' | 'subset' | 'sync'
           | 'system' | 'then' | 'thread' | 'threadid' | 'time' | 'tixe'
           | 'tl' | 'to' | 'token' | 'traces' | 'trap' | 'true' | 'types'
           | 'undefined' | 'union' | 'values' | 'variables' | 'while' | 'with'
           | 'wr' | 'yet' | 'RESULT' ;

分離符 = 改行 | 空白 ;

識別子 = ( 文字 | ギリシャ文字 ),
```

{ (文字 | ギリシャ文字) | 数字 | ‘’ | ‘_’ } ;

※注）CPU と BUS クラスは、VDM に予約されたクラス名であるため、ユーザは再定義できない。これらの事前に定義された 2 クラスが、上記セクション 14.1 で説明された機能性を含む。

次の予約前置詞の 1 つと共に始まるすべての識別子は予約されている: init_, inv_, is_, mk_, post_ そして pre_。

型変数識別子 = ‘@’, 識別子 ;

is 基本型 = ‘is_’, (‘bool’ | ‘nat’ | ‘nat1’ | ‘int’ | ‘rat’
| ‘real’ | ‘char’ | ‘token’) ;

記号リテラル = 数値リテラル | ブールリテラル
| nil リテラル | 文字リテラル | テキストリテラル
| 引用リテラル ;

数値 = 数字, { 数字 } ;

数値リテラル = 10 進数値リテラル | 16 進数値リテラル ;

指数 = (‘E’ | ‘e’), [‘+’ | ‘-’], 数値 ;

10 進数値リテラル = 数値, [‘.’, 数字, { 数字 }], [指数] ;

16 進数値リテラル = (‘0x’ | ‘0X’), 16 進数字, { 16 進数字 } ;

ブールリテラル = ‘true’ | ‘false’ ;

nil リテラル = ‘nil’ ;

文字リテラル = ‘’’, 文字 | エスケープ列
| 多文字, ‘’’ ;

エスケープ列 = ‘\\’ | ‘\r’ | ‘\n’ | ‘\t’ | ‘\f’ | ‘\e’ | ‘\a’
| ‘\x’ 16 進数字,16 進数字 | ‘\c’ 文字
| ‘\’ 8 進数字, 8 進数字, 8 進数字
| ‘\"’ | ‘\’’ | ;

多文字 = ギリシャ文字
| ‘<=’ | ‘>=’ | ‘<>’ | ‘->’ | ‘+>’ | ‘==>’ | ‘||’
| ‘=>’ | ‘<=>’ | ‘|->’ | ‘<:’ | ‘:>’ | ‘<-:’
| ‘:->’ | ‘==’ | ‘**’ | ‘++’ ;

テキストリテラル = ‘"’, { ‘""’ | 文字 | エスケープ列 }, ‘"’ ;

引用リテラル = 識別文字,
{ ‘_’ | 識別文字 | 数字 } ;

一行コメント = ‘--’, { 文字 – 改行 }, 改行 ;

複数行コメント = ‘/*’, { 文字 }, ‘*/’ ;

上記のエスケープ列は次のように翻訳される:

列	翻訳
'\\'	バックスラッシュ文字
'\r'	リターン文字
'\n'	改行文字
'\t'	タブ文字
'\f'	用紙送り文字
'\e'	エスケープ文字
'\a'	アラーム (ベル)
'\x' 16 進数字,16 進数字	文字の 16 進表示 (たとえば \x41 は 'A')
'\c' 文字	制御文字 (たとえば \c A ≡ \x01)
'\' 8 進数字, 8 進数字, 8 進数字	文字の 8 進表示
'\"'	" 文字
'\''	' 文字

C 演算子優先順位

具象構文における演算子の優先順位は2段階で定義される: 演算子はファミリーに区分けされて、上位の優先順位 $>$ がそれらのファミリーに対し与えられるが、その結果ファミリーである F_1 と F_2 が次を満足させるとする

$$F_1 > F_2$$

するとファミリー F_1 のすべての演算子はファミリー F_2 のすべての演算子より高位の優先順をもつ。

ファミリー内での相対的な演算子の優先順は、型情報を考慮して決定され、これが曖昧さの解決に役立つ。型構成子は別に扱われ、他の演算子とともに優先順に並べられることはない。

演算子には6つのファミリーすなわち、結合子、適用子、評価子、関係子、連結子、構成子がある:

結合子: 関数値、写像値の結合および、関数値、写像値、数値の反復を許す操作。

適用子: 関数適用、項目選択、列索引、その他、

評価子: 非述語である演算子。

関係子: 関係の演算子。

連結子: 論理連結子。

構成子: 式の構成において、陰に陽に用いられる演算子; たとえば if-then-elseif-else, '|->', '...', その他。

ファミリー上の優先順は次の通り:

結合子 $>$ 適用子 $>$ 評価子 $>$ 関係子 $>$ 連結子 $>$ 構成子

C.1 結合子のファミリー

これらの結合子は最高位の優先順位をもつ。

結合子 = 反復 | 合成 ;

反復 = '**' ;

合成 = 'comp' ;

優先順位	結合子
1	comp
2	iterate

C.2 適用子のファミリー

すべての適用子は等しい優先順位をもつ。

適用子 = 部分列
| 適用
| 関数型インスタンス化
| 項目選択 ;

部分列 = 式, '(', 式, ',', '...', ',',
式, ')' ;

適用 = 式, '(', [式リスト], ')' ;

関数型インスタンス化 = 式, '[', 型, { ',', 型 }, ']' ;

項目選択 = 式, '.', 識別子 ;

C.3 評価子のファミリー

評価子のファミリーは、それらが用いられている式の型に従い、9つのグループに区分けされる。

```
評価子 = 算術前置演算子
       | 集合前置演算子
       | 列前置演算子
       | 写像前置演算子
       | 逆写像
       | 算術中置演算子
       | 集合中置演算子
       | 列中置演算子
       | 写像中置演算子 ;

算術前置演算子 = '+' | '-' | 'abs' | 'floor' ;

集合前置演算子 = 'card' | 'power' | 'dunion' | 'dinter' ;

列前置演算子 = 'hd' | 'tl' | 'len'
             | 'inds' | 'elems' | 'conc' ;

写像前置演算子 = 'dom' | 'rng' | 'merge' | 'inverse' ;

算術中置演算子 = '+' | '-' | '*' | '/' | 'rem' | 'mod' | 'div' ;

集合中置演算子 = 'union' | 'inter' | '\' ;

列中置演算子 = '^' ;

写像中置演算子 = 'munion' | '++' | '<:' | '<-:' | ':>' | ':->' ;
```

優先順位はアナログの演算子のパターンを追いかける。以下の表においてファミリーは定義されている。

優先順位	算術	集合	写像	列
1	+ -	union \	munion ++	^
2	* / rem mod div	inter		
3			inverse	
4			<: <-:	
5			:> :->	
6	(単項) + (単項) - abs floor	card power dinter dunion	dom rng merge	len elems hd tl conc inds

C.4 関係子のファミリー

このファミリーは、結果値が bool 型であるすべての関係演算子を含む。

関係子 = 関係中置演算子 | 集合関係演算子 ;

関係中置演算子 = '=' | '<>' | '<' | '<=' | '>' | '>=' ;

集合関係演算子 = 'subset' | 'psubset' | 'in set' | 'not in set' ;

優先順位	関係子	
1	<=	<
	>=	>
	=	<>
	subset	psubset
	in set	not in set

関係子ファミリーのすべての演算子は等しい優先順位をもつ。タイプしていくということが、これらを隣り合わせに用いるとき意味をもたせる方法のないことを語るものである。

C.5 連結子のファミリー

このファミリーは、結果が bool 型であるすべての論理演算子を含む。

連結子 = 論理前置演算子 | 論理中置演算子 ;

論理前置演算子 = 'not' ;

論理中置演算子 = 'and' | 'or' | '=>' | '<=>' ;

優先順位	連結子
1	<=>
2	=>
3	or
4	and
5	not

C.6 構成子のファミリー

このファミリーは値を構成するために用いられるすべての演算子を含む。これらの優先順は、演算子の暗黙部である括弧によってかまたは構文によって与えられる。

C.7 グループ化

2 項演算子の演算対象のグループ化は以下の通り:

結合子:	右グループ化
適用子:	左グループ化
連結子:	'=>' 演算子は右グループ化 他の演算子は組み合わされるもののため、グループ化の左右は同等である
評価子:	左グループ化[27].
関係子:	グループ化は行わない、意味をなさないからである
構成子:	グループ化は行わない、意味をなさないからである

C.8 型演算子

型演算子は独自の優先順位をもち、以下の通り:

1. 関数型: ->，+> (右グループ化).
2. 合併型: | (左グループ化).
3. 他の 2 項型演算子: * (グループ化なし).
4. 写像型: map ... to ... および inmap ... to ... (右グループ化).
5. 単項型演算子: seq of, seq1 of, set of.

D 2つの具象構文間の相違

以下は数学構文と ASCII 構文との間で異なる記号のリストである:

[27] 右グループ化を行う "写像定義域限定" および "写像定義域削減" 演算子を除く（これは標準ではない）

数学構文	ASCII 構文
$\cdot$	&
$\times$	*
$\leq$	<=
$\geq$	>=
$\neq$	<>
$\xrightarrow{o}$	==>
$\rightarrow$	->
$\Rightarrow$	=>
$\Leftrightarrow$	<=>
$\mapsto$	|->
$\triangleq$	==
$\uparrow$	**
$\dagger$	++
$\biguplus$	munion
$\lhd$	<:
$\rhd$	:>
$\not\lhd$	<-:
$\not\rhd$	:->
$\subset$	psubset
$\subseteq$	subset
$\curvearrowright$	^
$\bigcap$	dinter
$\bigcup$	dunion
$\mathcal{F}$	power
...-set	set of ...
$\ldots^*$	seq of ...
$\ldots^+$	seq1 of ...
$\ldots \xrightarrow{m} \ldots$	map ... to ...
$\ldots \overset{m}{\longleftrightarrow} \ldots$	inmap ... to ...
μ	mu
$\mathbb{B}$	bool
$\mathbb{N}$	nat
$\mathbb{Z}$	int
$\mathbb{R}$	real
$\neg$	not

数学構文	ASCII 構文
$\cap$	`inter`
$\cup$	`union`
$\in$	`in set`
$\notin$	`not in set`
$\wedge$	`and`
$\vee$	`or`
$\forall$	`forall`
$\exists$	`exists`
$\exists!$	`exists1`
λ	`lambda`
ι	`iota`
$\ldots^{-1}$	`inverse ...`

E 標準ライブラリ

E.1 数学ライブラリ

数学ライブラリは `math.vpp` ファイルに定義されている。以下の数学関数を提供する:

関数		事前条件
`sin: real +> real`	Sine	
`cos: real +> real`	Cosine	
`tan: real -> real`	Tangent	引数は $\pi/2$ の整数倍でない
`cot: real -> real`	Cotagent	引数は π の整数倍でない
`asin: real -> real`	Inverse sine	引数は-1 から 1 の間 (両端を含む) にない
`acos: real -> real`	Inverse cosine	引数は-1 から 1 の間 (両端を含む) にない
`atan:real +> real`	Inverse tangent	
`sqrt: real -> real`	Square root	引数は負でない

また次の値が与えられる:

`pi` = 3.14159265358979323846

関数が、ありうる事前条件を満たさないような引数とともに適用される場合に、適当な VDM++ 値、`Inf` (無限値、たとえば `tan(pi/2)`) および `NaN` (数でない値、たとえば `sqrt (-1)`)、でない値を返すであろう。

標準ライブラリを用いるには

```
$TOOLBOXHOME/stdlib/math.vpp
```

を現プロジェクトに加える必要がある。これは `MATH` クラスを含む。このクラスの関数にアクセスするためには、クラスのインスタンスが生成されていなければ

ならない; しかしながら値はクラス属性なので、 pi は直接にアクセスされる可能性がある。以下の例題がこれを実演する:

```
class UseLib


  types

  coord :: x : real
           y : real

  functions

  -- 2点間の幾何距離
  dist : coord * coord -> real
  dist (c1,c2) ==
    let math = new MATH()
    in
    math.sqrt((c1.x - c2.x) * (c1.x - c2.x) +
              (c1.y - c2.y) * (c1.y - c2.y));


  -- 原点座標に交わる線の水平線からのなす角、
 -- 度数で出力する
  angle : coord -> real
  angle (c) ==
    let math = new MATH()
    in
    math.atan (c.y / c.x) * 360 / ( 2 * MATH`pi)

end UseLib
```

E.2 IO ライブラリ

IO ライブラリは io.vpp ファイルで定義され、 $TOOLBOXHOME/stdlib/ ディレクトリに置かれている。以下にリストされた IO 関数と操作が提供される。各々の read/write 関数と操作は、 相当する IO 行為の成功 (true) または失敗 (false) を表すブール値 (またはブール構成要素をもつ組) を返す。

`writeval[@p]:[@p] +> bool`
この関数は ASCII 形式での VDM 値を標準出力に書き出す。事前条件はない。

`fwriteval[@p]:seq1 of char * @p * filedirective +> bool`
この関数は ASCII 形式での VDM 値 (第 2 引数) を、第 1 引数に文字列で指定された名称のファイルに書き出す。第 3 パラメーターは以下のように定義された型 filedirective をもつ:

```
filedirective = <start>|<append>
```

<start> が用いられた場合、存在するファイルは (あった場合には) 上書される; <append> が用いられた場合、出力は存在するファイルの最後に付け足されすでに存在しているものがなければ新しいファイルが生成される。事前条件はない。

`freadval[@p]:seq1 of char +> bool * [@p]`
この関数は ASCII 形式の VDM 値を、最初の引数の文字列で指定されたファイルから読み取る。事前条件はない。関数は 2 つを返し、第 1 構成要素は読取の成功を示し、第 2 構成要素は読取が成功した場合の読み取られた値を示す。

`echo: seq of char ==> bool`
この操作は与えられたテキストを標準出力に書き出す。囲みのダブルクォートは取り除かれ、バックスラッシュ文字が escape sequences として翻訳される。事前条件はない。

`fecho: seq of char * seq of char * [filedirective] ==> bool`
この操作は echo に似ているが、標準出力ではなくファイルに書き出す。filedirective パラメーターは fwriteval に対するものとして翻訳されるべきである。この操作に対する事前条件は、ファイル名称として空列が

与えられた場合、テキストは標準出力に書かれるので [filedirective] 引数は nil であるべきということである。

ferror:() ==> seq of char read/write 関数と操作は、エラーが起きた場合に false を返す。この場合は内部エラー列がセットされる。この操作はこの文字列を返しそれを""にセットする。

IO ライブラリの使用例として、ページヒットのログを保守する web サーバーを考えよう:

```
class LoggingWebServer

  values
    logfilename : seq1 of char = "serverlog"

  instance variables
    io : IO := new IO();

  functions
    URLtoString : URL -> seq of char
    URLtoString = ...

  operations
    RetrieveURL : URL ==> File
    RetrieveURL(url) ==
      (def - = io.fecho(logfilename, URLtoString(url)^"\n", <append>);
       ...
      );

    ResetLog : () ==> bool
    ResetLog() ==
      io.fecho(logfilename,"\n",<start>)

end LoggingWebServer
```

E.3 VDMUtil ライブラリ

VDMUtil ライブラリは、VDMUtil.vpp ファイルに定義され、$TOOLBOXHOME/stdlib/ に配置されている。VDMUtil ライブラリは、以下のリストにあるような VDM のユーティリティを関数や操作として提供する。

set2seq[@T]:set of @T +> seq of @T
: このユーティリティ関数は、任意の型を持つ集合を簡単に列に変換することができる。

get_file_pos: () +> [seq of char * nat * nat * seq of char * seq of char]

: この関数は、ソースの特定部分のコンテキスト情報（ファイル名。行番号、クラス名、関数・操作名）を抽出することができる。

val2seq_of_char[@T]: @T +> seq of char
: この関数は、任意の値を文字列に変換することができる。

seq_of_char2val[@p]:seq1 of char -> bool * [@p]
: この関数は、文字列を VDM の任意の値に変換することができる。

```
class VDMUtil

--  VDMTools STANDARD LIBRARY: VDMUtil
--      --------------------------------------------
--
-- Standard library for the VDMTools Interpreter. When the interpreter
-- evaluates the preliminary functions/operations in this file,
-- corresponding internal functions is called instead of issuing a run
-- time error. Signatures should not be changed, as well as name of
-- module (VDM-SL) or class (VDM++). Pre/post conditions is
-- fully user customisable.
-- Dont care's may NOT be used in the parameter lists.

functions
-- Converts a set argument into a sequence in non-deterministic order.
static public set2seq[@T] : set of @T +> seq of @T
```

```
set2seq(x) == is not yet specified;

-- Returns a context information tuple which represents
-- (file_name * line_num * column_num * class_name * fnop_name) of
-- corresponding source text
static public
get_file_pos : () +> [ seq of char * nat * nat * seq of char * seq of char ]
get_file_pos() == is not yet specified;

-- Converts a VDM value into a seq of char.
static public val2seq_of_char[@T] : @T +> seq of char
val2seq_of_char(x) == is not yet specified;

-- converts VDM value in ASCII format into a VDM value
-- RESULT.#1 = false implies a conversion failure
static public seq_of_char2val[@p]:seq1 of char -> bool * [@p]
seq_of_char2val(s) ==
  is not yet specified
  post let mk_(b,t) = RESULT in not b => t = nil;

end VDMUtil
```

索 引