Dafny Reference Manual

K. Rustan M. Leino, Richard L. Ford, David R. Cok

October 26, 2020

Abstract: This is the Dafny reference manual which describes the Dafny programming language and how to use the Dafny verification system. Parts of this manual are more tutorial in nature in order to help the user understand how to do proofs with Dafny.

Acknowledgements

Rustan Leino is the designer of the Dafny language and the chief implementor of the dafny tools. Leino, Richard Ford, and David Cok are the principal authors of this document. Many others contributed to the implementation and to documenting various aspects of the language, as described on the project website at https://github.com/dafny-lang/dafny.

Contents

Abstract: This is the Dafny reference manual which describes the Dafny programming language and how to use the Dafny verification system. Parts of this manual are more tutorial in nature in order to help the user understand how to do proofs with Dafny.

Link to current document as pdf Link to current document as html

1 Introduction

Dafny [@Leino:Dafny:LPAR16] is a programming language with built-in specification constructs, so that verifying a program's correctness with respect to those specifications is a natural part of writing software. The Dafny static program verifier can be used to verify the functional correctness of programs. This document is a reference manual for the programming language and a user guide for the dafny tool that performns verification and compilation to an executable form.

The Dafny programming language is designed to support the static verification of programs. It is imperative, sequential, supports generic classes, inheritance and abstraction, methods and functions, dynamic allocation, inductive and coinductive datatypes, and specification constructs. The specifications include pre- and postconditions, frame specifications (read and write sets), and termination metrics. To further support specifications, the language also offers updatable ghost variables, recursive functions, and types like sets and sequences. Specifications and ghost constructs are used only during verification; the compiler omits them from the executable code.

The Dafny verifier is run as part of the compiler. As such, a programmer interacts with it much in the same way as with the static type checker—when the tool produces errors, the programmer responds by changing the program's type declarations, specifications, and statements.

The easiest way to try out Dafny is in your web browser at rise4fun[@Rise4fun:dafny]. Once you get a bit more serious, you may prefer to download it to run it on your machine. Dafny can be run from the command line (on Windows or other platforms) or from an IDE such as emacs or Microsoft Visual Studio 2012 (or newer), where the Dafny verifier runs in the background while the programmer is editing the program. An editor such as VSCode can provide syntax highlighting without the built-in verification.

The Dafny verifier is powered by Boogie [@Boogie:Architecture;@Leino:Boogie2-RefMan;@LeinoRuemmer:Boogie2] and Z3[@deMouraBjorner:Z3:overview].

From verified programs, the Dafny compiler can produce code for a number of different backends: the .NET platform via intermediate C# files, Java, Javascript, Go, and C++. Each language provides a basic Foreign Function Interface (through uses of `:extern`) and a supporting runtime library. However,

there is no automatic FFI generator, so `:extern` stubs must be written by hand.

This reference manual for the Dafny verification system is based on the following references: [@Leino:Dafny:LPAR16;@MSR:dafny:main; @MSR:dafny:source;@MSR:dafny:quickref; @LEINO:Dafny:Calc; @LEINO:Dafny:Coinduction; and the tutorials at @Rise4fun:dafny] [Co-induction Simply]: http://research.microsoft.com/en-us/um/people/leino/papers/krml230.pdf "Co-induction Simply: Automatic Co-inductive Proofs in a Program Verifier"

The main part of the reference manual is in top down order except for an initial section that deals with the lowest level constructs.

The details of using (and contributing to) the dafny tool are described in the User Guide.

1.1 Dafny Example

To give a flavor of Dafny, here is the solution to a competition problem.

```
// VSComp 2010, problem 3, find a 0 in a linked list and return
// how many nodes were skipped until the first 0 (or end-of-list)
// was found.
// Rustan Leino, 18 August 2010.
//
// The difficulty in this problem lies in specifying what the
// return value 'r' denotes and in proving that the program
// terminates.  Both of these are addressed by declaring a ghost
// field 'List' in each linked-list node, abstractly representing
// the linked-list elements from the node to the end of the linked
// list.  The specification can now talk about that sequence of
// elements and can use 'r' as an index into the sequence, and
// termination can be proved from the fact that all sequences in
// Dafny are finite.
//
// We only want to deal with linked lists whose 'List' field is
// properly filled in (which can only happen in an acyclic list,
// for example).  To that end, the standard idiom in Dafny is to
// declare a predicate 'Valid()' that is true of an object when
// the data structure representing that object's abstract value
// is properly formed.  The definition of 'Valid()' is what one
// intuitively would think of as the ''object invariant'', and
// it is mentioned explicitly in method pre- and postconditions.
//
// As part of this standard idiom, one also declares a ghost
// variable 'Repr' that is maintained as the set of objects that
// make up the representation of the aggregate object--in this
// case, the Node itself and all its successors.
```

```
class Node {
  ghost var List: seq<int>
  ghost var Repr: set<Node>
  var head: int
  var next: Node

  predicate Valid()
    reads this, Repr
  {
    this in Repr &&
    1 <= |List| && List[0] == head &&
    (next == null ==> |List| == 1) &&
    (next != null ==>
      next in Repr && next.Repr <= Repr && this !in next.Repr &&
      next.Valid() && next.List == List[1..])
  }

  static method Cons(x: int, tail: Node) returns (n: Node)
    requires tail == null || tail.Valid()
    ensures n != null && n.Valid()
    ensures if tail == null then n.List == [x]
                            else n.List == [x] + tail.List
  {
    n := new Node;
    n.head, n.next := x, tail;
    if (tail == null) {
      n.List := [x];
      n.Repr := {n};
    } else {
      n.List := [x] + tail.List;
      n.Repr := {n} + tail.Repr;
    }
  }
}

method Search(ll: Node) returns (r: int)
  requires ll == null || ll.Valid()
  ensures ll == null ==> r == 0
  ensures ll != null ==>
            0 <= r && r <= |ll.List| &&
            (r < |ll.List| ==> ll.List[r] == 0 &&
            0 !in ll.List[..r]) &&
            (r == |ll.List| ==> 0 !in ll.List)
{
  if (ll == null) {
```

```
    r := 0;
  } else {
    var jj,i := ll,0;
    while (jj != null && jj.head != 0)
      invariant jj != null ==> jj.Valid() &&
            i + |jj.List| == |ll.List| &&
            ll.List[i..] == jj.List
      invariant jj == null ==> i == |ll.List|
      invariant 0 !in ll.List[..i]
      decreases |ll.List| - i
    {
      jj := jj.next;
      i := i + 1;
    }
    r := i;
  }
}

method Main()
{
  var list: Node := null;
  list := list.Cons(0, list);
  list := list.Cons(5, list);
  list := list.Cons(0, list);
  list := list.Cons(8, list);
  var r := Search(list);
  print "Search returns ", r, "\n";
  assert r == 1;
}
```

2 Lexical and Low Level Grammar

Dafny uses the Coco/R lexer and parser generator for its lexer and parser (http://www.ssw.uni-linz.ac.at/Research/Projects/Coco)[@Linz:Coco]. The Dafny input file to Coco/R is the `Dafny.atg` file in the source tree. A Coco/R input file consists of code written in the target language (e.g. C#) intermixed with these special sections:

0. The Characters section which defines classes of characters that are used in defining the lexer.
1. The Tokens section which defines the lexical tokens.
2. The Productions section which defines the grammar. The grammar productions are distributed in the later parts of this document in the parts where those constructs are explained.

The grammar presented in this document was derived from the `Dafny.atg` file but has been simplified by removing details that, though needed by the parser, are not needed to understand the grammar. In particular, the following transformations have been performed.

- The semantics actions, enclosed by "(." and ".)", were removed.
- There are some elements in the grammar used for error recovery ("SYNC"). These were removed.
- There are some elements in the grammar for resolving conflicts ("IF(b)"). These have been removed.
- Some comments related to Coco/R parsing details have been removed.
- A Coco/R grammar is an attributed grammar where the attributes enable the productions to have input and output parameters. These attributes were removed except that boolean input parameters that affect the parsing are kept.
  - In our representation we represent these in a definition by giving the names of the parameters following the non-terminal name. For example `entity1(allowsX)`.
  - In the case of uses of the parameter, the common case is that the parameter is just passed to a lower-level non-terminal. In that case we just give the name, e.g. `entity2(allowsX)`.
  - If we want to given an explicit value to a parameter, we specify it in a keyword notation like this: `entity2(allowsX: true)`.
  - In some cases the value to be passed depends on the grammatical context. In such cases we give a description of the conditions under which the parameter is true, enclosed in parenthesis. For example:
    `FunctionSignatureOrEllipsis_(allowGhostKeyword: ("method" present))`
    means that the `allowGhostKeyword` parameter is true if the "method" keyword was given in the associated `FunctionDecl`.
  - Where a parameter affects the parsing of a non-terminal we will explain the effect of the parameter.

The names of character sets and tokens start with a lower case letter but the names of grammar non-terminals start with an upper-case letter.

The grammar uses Extended BNF notation. See the Coco/R Referenced manual for details. But in summary:

- identifiers starting with a lower case letter denote terminal symbols,
- identifiers starting with an upper case letter denote nonterminal symbols.
- Strings (a sequence of characters enclosed by double quote characters) denote the sequence of enclosed characters.
- `=` separates the sides of a production, e.g. `A = a b c`
- In the Coco grammars "." terminates a production, but for readability in this document a production starts with the defined identifier in the left margin and may be continued on subsequent lines if they are indented.
- `|` separates alternatives, e.g. `a b | c | d e` means `a b` or `c` or `d e`

- `( )` groups alternatives, e.g. `(a | b) c` means `a c` or `b c`
- `[ ]` option, e.g. `[a] b` means `a b` or `b`
- `{ }` iteration (0 or more times), e.g. `{a} b` means `b` or `a b` or `a a b` or …
- We allow `|` inside `[ ]` and `{ }`. So `[a | b]` is short for `[(a | b)]` and `{a | b}` is short for `{(a | b)}`.
- The first production defines the name of the grammar, in this case `Dafny`.

In addition to the Coco rules, for the sake of readability we have adopted these additional conventions.

- We allow `-` to be used. `a - b` means it matches if it matches `a` but not `b`.
- To aid in explaining the grammar we have added some additional productions that are not present in the original grammar. We name these with a trailing underscore. If you inline these where they are referenced, the result should let you reconstruct the original grammar.

For the convenience of the reader, any references to character sets, tokens, or grammar non-terminals in this document are hyper-links that will link to the definition of the entity.

2.1 Dafny Input

Dafny source code files are readable text encoded as UTF-8 Unicode (because this is what the Coco/R-generated scanner and parser read). All program text other than the contents of comments, character, string and verbatim string literals are printable and white-space ASCII characters, that is, ASCII characters in the range `!` to `~`, plus space, tab, cr and nl (ASCII, 9, 10, 13, 32) characters, with the exception of a few allowed unicode mathematical symbols.

However, a current limitation is that the Coco/R tool used by Dafny is not up to date, and consequently, only printable and white-space ASCII characters can be used. Use `\u` escapes in string and character literals to insert unicode characters. Unicode in comments will work fine unless the unicode is interpreted as an end-of-comment indication. Unicode in verbatim strings will likely not be interpreted as intended. [Outstanding issue #818].

2.2 Character Classes

This section defines character classes used later in the token definitions. In this section a backslash is used to start an escape sequence; so for example `'\n'` denotes the single linefeed character. Also in this section, double quotes enclose the set of characters constituting a character class; enclosing single quotes are used when there is just one character in the class. `+` indicates the union of two character classes; `-` is the set-difference between the two classes. `ANY` designates all unicode characters.

```
letter = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
```

At present, a letter is an ASCII upper or lowercase letter. Other Unicode letters are not supported.

```
digit = "0123456789"
```

A digit is just one of the base-10 digits.

```
posDigit = "123456789"
posDigit2 = "23456789"
```

A `posDigit` is a digit, excluding 0. `posDigit2` excludes both 0 and 1.

```
hexdigit = "0123456789ABCDEFabcdef"
```

A `hexdigit` character is a digit or one of the letters from 'A' to 'F' in either case.

```
special = "'_?"
```

The *special* characters are the characters in addition to alphanumeric characters that are allowed to appear in a Dafny identifier. These are

- `'` because mathematicians like to put primes on identifiers and some ML programmers like to start names of type parameters with a "'".
- `_` because computer scientists expect to be able to have underscores in identifiers.
- `?` because it is useful to have "?" at the end of names of predicates, e.g. "Cons?".

```
cr        = '\r'
```

A carriage return character.

```
lf        = '\n'
```

A line feed character.

```
tab       = '\t'
```

A tab character.

```
space     = ' '
```

A space character.

```
nondigitIdChar = letter + special
```

The characters that can be used in an identifier minus the digits.

```
idchar = nondigitIdChar + digit
```

The characters that can be used in an identifier.

```
nonidchar = ANY - idchar
```

Any character except those that can be used in an identifier.
Here the scanner generator will interpret `ANY` as any unicode character. However, `nonidchar` is used only to mark the end of the `!in` token; in this context any character other than whitespace or printable ASCII will trigger a subsequent scanning or parsing error.

```
charChar = ANY - '\'' - '\\' - cr - lf
```

Characters that can appear in a character constant. See the discussion on unicode support.

```
stringChar = ANY - '"' - '\\' - cr - lf
```

Characters that can appear in a string constant. See the discussion on unicode support.

```
verbatimStringChar = ANY - '"'
```

Characters that can appear in a verbatim string. See the discussion on unicode support.

2.2.1 Comments

Comments are in two forms.

- They may go from "/*" to "*/" and be nested.
- They may go from "//" to the end of the line.

Note that the nesting of multi-line comments is behavior that is different from most programming languages. In dafny,

```
method m() {
  /* comment
     /* nested comment
     */
     rest of outer comment
  */
}
```

is permitted; this feature is convenient for commenting out blocks of program statements that already have multi-line comments within them. Other than

looking for end-of-comment delimiters, the contents of a comment are not interpreted. Comments may contain any unicode character, but see the discussion on unicode support for more information.

2.3 Tokens

As with most languages, Dafny syntax is defined in two levels. First the stream of input characters is broken up into *tokens*. Then these tokens are parsed using the Dafny grammar. The Dafny tokens are defined in this section.

2.3.1 Reserved Words

The following reserved words appear in the Dafny grammar and may not be used as identifiers of user-defined entities:

```
reservedword =
    "abstract" | "array" | "as" | "assert" | "assume" | "bool" |
    "break" | "calc" | "case" | "char" | "class" | "codatatype" |
    "colemma" | "constructor" | "copredicate" | "datatype" |
    "decreases" | "default" | "else" | "ensures" | "exists" |
    "extends" | "false" | "forall" | "fresh" | "function" |
    "ghost" | "if" | "imap" | "import" | "in" | "include" |
    "inductive" | "int" | "invariant" | "is" | "iset" |
    "iterator" | "label" | "lemma" | "map" | "match" | "method" |
    "modifies" | "modify" | "module" | "multiset" | "nat" |
    "new" | "newtype" | "null" | "object" | "old" | "opened" |
    "predicate" | "print" | "protected" | "provides" "reads" |
    "real" | "refines" | "requires" | "return" | "returns" |
    "reveals" | "seq" | "set" | "static" | "string" | "then" |
    "this" | "trait" | "true" | "twostate" | "type" |
    "unchanged" | "var" | "where" | "while" | "yield" | "yields" |
    arrayToken

arrayToken = "array" [ posdigit2 | posDigit digit { digit }]["?"]
```

An `arrayToken` is a reserved word that denotes an array type of given rank. `array` is an array type of rank 1 (aka a vector). `array2` is the type of two-dimensional arrays, etc. `array1` and `array1?` are not reserved words; they are just ordinary identifiers.

2.3.2 Identifiers

```
ident = nondigitIdChar { idchar } - arrayToken - charToken - reservedword
```

In general Dafny identifiers are sequences of `idchar` characters where the first character is a `nondigitIdChar`. However tokens that fit this pattern are not

identifiers if they look like an array type token, a character literal, or a reserved word. Also, `ident` tokens that begin with an `_` are not permitted as user identifiers.

2.3.3 Digits

```
digits = digit {['_'] digit}
```

A sequence of decimal digits, possibly interspersed with underscores for readability (but not beginning or ending with an underscore). Example: `1_234_567`.

```
hexdigits = "0x" hexdigit {['_'] hexdigit}
```

A hexadecimal constant, possibly interspersed with underscores for readability (but not beginning or ending with an underscore). Example: `0xffff_ffff`.

```
decimaldigits = digit {['_'] digit} '.' digit {['_'] digit}
```

A decimal fraction constant, possibly interspersed with underscores for readability (but not beginning or ending with an underscore). Example: `123_456.789_123`.

2.3.4 Escaped Character

In this section the "\" characters are literal.

```
escapedChar =
    ( "\'" | "\"" | "\\" | "\0" | "\n" | "\r" | "\t"
      | "\u" hexdigit hexdigit hexdigit hexdigit
    )
```

In Dafny character or string literals, escaped characters may be used to specify the presence of a single- or double-quote character, backslash, null, new line, carriage return, tab, or a Unicode character with given hexadecimal representation.

2.3.5 Character Constant Token

```
charToken = "'" ( charChar | escapedChar ) "'"
```

A character constant is enclosed by "'" and includes either a character from the `charChar` set, or an escaped character. Note that although Unicode letters are not allowed in Dafny identifiers, Dafny does support Unicode in its character, string, and verbatim strings constants and in its comments. A character constant has type `char`.

2.3.6 String Constant Token

```
stringToken =
    '"' { stringChar | escapedChar }  '"'
  | '@' '"' { verbatimStringChar | '"' '"' } '"'
```

A string constant is either a normal string constant or a verbatim string constant. A normal string constant is enclosed by `"` and can contain characters from the `stringChar` set and escapes.

A verbatim string constant is enclosed between `@"` and `"` and can consist of any characters (including newline characters) except that two successive double quotes represent one quote character inside the string. This is the mechanism for escaping a double quote character, which is the only character needing escaping in a verbatim string.

2.4 Low Level Grammar Productions

2.4.1 Identifier Variations

```
Ident = ident
```

The `Ident` non-terminal is just an `ident` token and represents an ordinary identifier.

```
DotSuffix =
  ( ident | digits | "requires" | "reads" )
```

When using the *dot* notation to denote a component of a compound entity, the token following the "." may be an identifier, a natural number, or one of the keywords `requires` or `reads`.

- Digits can be used to name fields of classes and destructors of datatypes. For example, the built-in tuple datatypes have destructors named 0, 1, 2, etc. Note that as a field or destructor name a digit sequence is treated as a string, not a number: internal underscores matter, so 10 is different from 1_0 and from 010.
- `m.requires` is used to denote the precondition for method m.
- `m.reads` is used to denote the things that method m may read.

```
NoUSIdent = ident - "_" { idchar }
```

A `NoUSIdent` is an identifier except that identifiers with a **leading** underscore are not allowed. The names of user-defined entities are required to be `NoUSIdent`s. We introduce more mnemonic names for these below (e.g. `ClassName`).

```
WildIdent = NoUSIdent | "_"
```

Identifier, disallowing leading underscores, except the "wildcard" identifier `_`. When `_` appears it is replaced by a unique generated identifier distinct from user identifiers. This wildcard has several uses in the language, but it is not used as part of expressions.

2.4.2 NoUSIdent Synonyms

In the productions for the declaration of user-defined entities the name of the user-defined entity is required to be an identifier that does not start with an underscore, i.e., a `NoUSIdent`. To make the productions more mnemonic, we introduce the following synonyms for `NoUSIdent`.

```
ModuleName = NoUSIdent
ClassName = NoUSIdent
TraitName = NoUSIdent
DatatypeName = NoUSIdent
DatatypeMemberName = NoUSIdent
NewtypeName = NoUSIdent
NumericTypeName = NoUSIdent
SynonymTypeName = NoUSIdent
IteratorName = NoUSIdent
TypeVariableName = NoUSIdent
MethodName = NoUSIdent
FunctionName = NoUSIdent
PredicateName = NoUSIdent
CopredicateName = NoUSIdent
LabelName = NoUSIdent
AttributeName = NoUSIdent
FieldIdent = NoUSIdent
```

A `FieldIdent` is one of the ways to identify a field. The other is using digits.

2.4.3 Qualified Names

A qualified name starts with the name of the top-level entity and then is followed by zero or more `DotSuffix`s which denote a component. Examples:

- `Module.MyType1`
- `MyTuple.1`
- `MyMethod.requires`

The grammar does not actually have a production for qualified names except in the special case of a qualified name that is known to be a module name, i.e. a `QualifiedModuleName`.

2.4.4 Identifier-Type Combinations

In this section, we describe some nonterminals that combine an identifier and a type.

```
IdentType = WildIdent ":" Type
```

In Dafny, a variable or field is typically declared by giving its name followed by a `colon` and its type. An `IdentType` is such a construct.

```
GIdentType(allowGhostKeyword) = [ "ghost" ] IdentType
```

A `GIdentType` is a typed entity declaration optionally preceded by `ghost`. The *ghost* qualifier means the entity is only used during verification and not in the generated code. Ghost variables are useful for abstractly representing internal state in specifications. If `allowGhostKeyword` is false then `ghost` is not allowed.

```
LocalIdentTypeOptional = WildIdent [ ":" Type ]
```

A `LocalIdentTypeOptional` is used when declaring local variables. If a value is specified for the variable, the type may be omitted because it can be inferred from the initial value. The initial value value may also be omitted.

```
IdentTypeOptional = WildIdent [ ":" Type ]
```

A `IdentTypeOptional` is typically used in a context where the type of the identifier may be inferred from the context. Examples are in pattern matching or quantifiers.

```
TypeIdentOptional = [ "ghost" ] ( NoUSIdent | digits ) ":" ] Type
```

`TypeIdentOptional`s are used in `FormalsOptionalIds`. This represents situations where a type is given but there may not be an identifier.

```
FormalsOptionalIds = "(" [TypeIdentOptional  { "," TypeIdentOptional } ] ")"
```

A `FormalsOptionalIds` is a formal parameter list in which the types are required but the names of the parameters are optional. This is used in algebraic datatype definitions.

2.4.5 Numeric Literals

```
Nat = ( digits | hexdigits )
```

A `Nat` represents a natural number expressed in either decimal or hexadecimal.

```
Dec = decimaldigits
```

A `Dec` represents a decimal fraction literal.

3 Programs

```
Dafny = { IncludeDirective_ } { TopDecl } EOF
```

At the top level, a Dafny program (stored as files with extension `.dfy`) is a set of declarations. The declarations introduce (module-level) methods and functions, as well as types (classes, traits, inductive and co-inductive datatypes, new_types, type synonyms, opaque types, and iterators) and modules, where the order of introduction is irrelevant. A class also contains a set of declarations, introducing fields, methods, and functions.

When asked to compile a program, Dafny looks for the existence of a Main() method. If a legal Main() method is found, the compiler will emit a `.EXE`; otherwise, it will emit a `.DLL`.

(If there is more than one Main(), Dafny will try to emit an .EXE, but this may cause the C# compiler to complain. One could imagine improving this functionality so that Dafny will produce a polite error message in this case.)

In order to be a legal Main() method, the following must be true:

- The method takes no parameters
- The method is not a ghost method
- The method has no requires clause
- The method has no modifies clause
- If the method is an instance (that is, non-static) method in a class, then the enclosing class must not declare any constructor

Note, however, that the following are allowed:

- The method is allowed to be an instance method as long as the enclosing class does not declare any constructor. In this case, the runtime system will allocate an object of the enclosing class and will invoke Main() on it.
- The method is allowed to have `ensures` clauses
- The method is allowed to have `decreases` clauses, including a `decreases *`. (If Main() has a `decreases *`, then its execution may go on forever, but in the absence of a `decreases *` on Main(), Dafny will have verified that the entire execution will eventually terminate.)

An invocation of Dafny may specify a number of source files. Each Dafny file follows the grammar of the `Dafny` non-terminal.

It consists of a sequence of optional *include* directives followed by top level declarations followed by the end of the file.

3.1 Include Directives

```
IncludeDirective_ = "include" stringToken
```

Include directives have the form `"include" stringToken` where the string token is either a normal string token or a verbatim string token. The `stringToken` is interpreted as the name of a file that will be included in the Dafny source. These included files also obey the `Dafny` grammar. Dafny parses and processes the transitive closure of the original source files and all the included files, but will not invoke the verifier on these unless they have been listed explicitly on the command line.

3.2 Top Level Declarations

```
TopDecl = { { DeclModifier }
  ( SubModuleDecl
  | ClassDecl
  | DatatypeDecl
  | NewtypeDecl
  | SynonymTypeDecl
  | IteratorDecl
  | TraitDecl
  | ClassMemberDecl(moduleLevelDecl: true)
  }
```

Top-level declarations may appear either at the top level of a Dafny file, or within a `SubModuleDecl`. A top-level declaration is one of the following types of declarations which are described later.

The `ClassDecl`, `DatatypeDecl`, `NewtypeDecl`, `SynonymTypeDecl`, `IteratorDecl`, and `TraitDecl` declarations are type declarations and are describe in Section [#sec-types]. Ordinarily `ClassMemberDecl`s appear in class declarations but they can also appear at the top level. In that case they are included as part of an implicit top-level class and are implicitly `static` (but cannot be declared as static). In addition a `ClassMemberDecl` that appears at the top level cannot be a `FieldDecl`.

3.3 Declaration Modifiers

```
DeclModifier =
  ( "abstract" | "ghost" | "static" | "protected"
  | "extern" [ stringToken]
  )
```

Top level declarations may be preceded by zero or more declaration modifiers. Not all of these are allowed in all contexts.

The "abstract" modifiers may only be used for module declarations. An abstract module can leave some entities underspecified. Abstract modules are not compiled to C#.

The ghost modifier is used to mark entities as being used for specification only, not for compilation to code.

The static modifier is used for class members that that are associated with the class as a whole rather than with an instance of the class.

The protected modifier is used to control the visibility of the body of functions.

The extern modifier is used to alter the CompileName of entities. The CompileName is the name for the entity when translating to Boogie or C#.

The following table shows modifiers that are available for each of the kinds of declaration. In the table we use already-ghost to denote that the item is not allowed to have the ghost modifier because it is already implicitly ghost or non-ghost.

Declaration	allowed modifiers
module	abstract
class	extern
trait	-
datatype or codatatype	-
field	ghost
newtype	-
synonym types	-
iterators	-
method	ghost static extern
lemma, colemma, comethod	already-ghost static protected
inductive lemma	already-ghost static
constructor	-
function (non-method)	already-ghost static protected
function method	already-ghost static protected extern
predicate (non-method)	already-ghost static protected
predicate method	already-ghost static protected extern
inductive predicate	already-ghost static protected
copredicate	already-ghost static protected

4 Modules

```
SubModuleDecl = ( ModuleDefinition_ | ModuleImport_ )
```

Structuring a program by breaking it into parts is an important part of creating large programs. In Dafny, this is accomplished via *modules*. Modules provide

a way to group together related types, classes, methods, functions, and other modules, as well as to control the scope of declarations. Modules may import each other for code reuse, and it is possible to abstract over modules to separate an implementation from an interface.

4.1 Declaring New Modules

```
ModuleDefinition_ = "module" { Attribute } ModuleName
        [ [  "exclusively" ] "refines" QualifiedModuleName ]
        "{" { TopDecl } "}"
QualifiedModuleName = Ident { "." Ident }
```

A qualified name that is known to refer to a module.

A new module is declared with the `module` keyword, followed by the name of the new module, and a pair of curly braces ({}) enclosing the body of the module:

```
module Mod {
  ...
}
```

A module body can consist of anything that you could put at the top level. This includes classes, datatypes, types, methods, functions, etc.

```
module Mod {
  class C {
    var f: int
    method m()
  }
  datatype Option = A(int) | B(int)
  type T
  method m()
  function f(): int
}
```

You can also put a module inside another, in a nested fashion:

```
module Mod {
  module Helpers {
    class C {
      method doIt()
      var f: int
    }
  }
}
```

Then you can refer to the members of the `Helpers` module within the `Mod` module by prefixing them with "Helpers.". For example:

```
module Mod {
  module Helpers { ... }
  method m() {
    var x := new Helpers.C;
    x.doIt();
    x.f := 4;
  }
}
```

Methods and functions defined at the module level are available like classes, with just the module name prefixing them. They are also available in the methods and functions of the classes in the same module.

```
module Mod {
  module Helpers {
    function method addOne(n: nat): nat {
      n + 1
    }
  }
  method m() {
    var x := 5;
    x := Helpers.addOne(x); // x is now 6
  }
}
```

TO BE WRITTEN - standalone declaration of nested modules

Note that everything declared at the top-level (in all the files constituting the program) is implicitly part of a single implicit unnamed global module.

4.2 Importing Modules

```
ModuleImport_ = "import" ["opened" ] ModuleName
    [ "=" QualifiedModuleName
    | "as" QualifiedModuleName ["default" QualifiedModuleName ]
    ]
    [ ";" ]
```

Declaring new submodules is useful, but sometimes you want to refer to things from an existing module, such as a library. In this case, you can *import* one module into another. This is done via the `import` keyword, which has two forms with different meanings. The simplest form is the concrete import, which has the form `import A = B`. This declaration creates a reference to the module `B` (which must already exist), and binds it to the new name `A`. This form can also be used to create a reference to a nested module, as in `import A = B.C`.

As modules in the same scope must have different names, this ability to bind

a module to a new name allows disambiguating separately developed external modules that have the same name. Note that the new name is only bound in the scope containing the import declaration; it does not create a global alias. For example, if `Helpers` was defined outside of `Mod`, then we could import it:

```
module Helpers {
  ...
}
module Mod {
  import A = Helpers
  method m() {
    assert A.addOne(5) == 6;
  }
}
```

Note that inside `m()`, we have to use `A` instead of `Helpers`, as we bound it to a different name. The name `Helpers` is not available inside `m()`, as only names that have been bound inside `Mod` are available. In order to use the members from another module, that other module either has to be declared there with `module` or imported with `import`.

We don't have to give `Helpers` a new name, though, if we don't want to. We can write `import Helpers = Helpers` to import the module under its own name; Dafny even provides the shorthand `import Helpers` for this behavior. You can't bind two modules with the same name at the same time, so sometimes you have to use the = version to ensure the names do not clash. When importing nested modules, `import B.C` means `import C = B.C`; the new name is always the last name segment of the module designation.

The `QualifiedModuleName` in the `ModuleImport_` starts with a sibling module of the importing module, or with a submodule of the importing module. There is no way to refer to the parent module, only sibling modules (and their submodules).

Import statements may occur at the top-level of a program (that is, in the implicit top-level module of the program) as well. There they serve simply as a way to give a new name, perhaps a shorthand name, to a module. For example,

```
module MyModule { ... } // declares module MyModule
import MyModule  // error: cannot add a moduled named MyModule
                 // because there already is one
import M = MyModule // OK. M and MyModule are equivalent
```

4.3 Export Sets

TO BE WRITTEN – including provides and reveals lists TO BE WRITTEN – opened imports are not exported TO BE WRITTEN – module facades

4.4 Opening Modules

Sometimes, prefixing the members of the module you imported with the name is tedious and ugly, even if you select a short name when importing it. In this case, you can import the module as `opened`, which causes all of its members to be available without adding the module name. The `opened` keyword, if present, must immediately follow `import`. For example, we could write the previous example as:

```
module Mod {
  import opened Helpers
  method m() {
    assert addOne(5) == 6;
  }
}
```

When opening modules, the newly bound members will have low priority, so they will be hidden by local definitions. This means if you define a local function called `addOne`, the function from `Helpers` will no longer be available under that name. When modules are opened, the original name binding is still present however, so you can always use the name that was bound to get to anything that is hidden.

```
module Mod {
  import opened Helpers
  function addOne(n: nat): nat {
    n - 1
  }
  method m() {
    assert addOne(5) == 6; // this is now false,
                           // as this is the function just defined
    assert Helpers.addOne(5) == 6; // this is still true
  }
}
```

If you open two modules that both declare members with the same name, then neither member can be referred to without a module prefix, as it would be ambiguous which one was meant. Just opening the two modules is not an error, however, as long as you don't attempt to use members with common names. The `opened` keyword can be used with any kind of `import` declaration, including the module abstraction form.

An `import opened` may occur at the top-level as well. For example,

```
module MyModule { ... } // declares MyModule
import opened MyModule // does not declare a new module, but does make
                       // all names in MyModule available in the current
                       // scope, without needing qualification
import opened M = MyModule // names in MyModule are available in the
```

```
                        // current scope without qualification or
                        // qualified with either M or MyModule
```

The Dafny style guidelines suggest using opened imports sparingly. They are best used when the names being imported have obvious and unambiguous meanings and when using qualified names would be verbose enough to impede understanding.

4.5 Module Abstraction

Sometimes, using a specific implementation is unnecessary; instead, all that is needed is a module that implements some interface. In that case, you can use an *abstract* module import. In Dafny, this is written `import A : B`. This means bind the name `A` as before, but instead of getting the exact module `B`, you get any module which is a *adheres* of `B`. Typically, the module `B` may have abstract type definitions, classes with bodyless methods, or otherwise be unsuitable to use directly. Because of the way refinement is defined, any refinement of `B` can be used safely. For example, if we start with:

```
module Interface {
  function method addSome(n: nat): nat
    ensures addSome(n) > n
}
module Mod {
  import A : Interface
  method m() {
    assert 6 <= A.addSome(5);
  }
}
```

then we can be more precise if we know that `addSome` actually adds exactly one. The following module has this behavior. Further, the postcondition is stronger, so this is actually a refinement of the Interface module.

```
module Implementation {
  function method addSome(n: nat): nat
    ensures addSome(n) == n + 1
  {
    n + 1
  }
}
```

We can then substitute `Implementation` for `A` in a new module, by declaring a refinement of `Mod` which defines `A` to be `Implementation`.

```
module Mod2 refines Mod {
  import A = Implementation
```

```
  ...
}
```

You can also give an implementation directly, without introducing a refinement, by giving a default to the abstract import:

```
module Interface {
  function method addSome(n: nat): nat
    ensures addSome(n) > n
}
module Mod {
  import A : Interface default Implementation
  method m() {
    assert 6 <= A.addSome(5);
  }
}
module Implementation {
  function method addSome(n: nat): nat
    ensures addSome(n) == n + 1
  {
    n + 1
  }
}
module Mod2 refines Mod {
  import A : Interface default Implementation
  ...
}
```

Regardless of whether there is a default, the only things known about `A` in this example is that it has a function `addSome` that returns a strictly bigger result, so even with the default we still can't prove that `A.addSome(5) == 6`, only that `6 <= A.addSome(5)`.

When you refine an abstract import into a concrete one, or giving a default, Dafny checkes that the concrete module is a refinement of the abstract one. This means that the methods must have compatible signatures, all the classes and datatypes with their constructors and fields in the abstract one must be present in the concrete one, the specifications must be compatible, etc.

4.6 Module Ordering and Dependencies

Dafny isn't particular about which order the modules appear in, but they must follow some rules to be well formed. As a rule of thumb, there should be a way to order the modules in a program such that each only refers to things defined **before** it in the source text. That doesn't mean the modules have to be given in that order. Dafny will figure out that order for you, assuming you haven't made any circular references. For example, this is pretty clearly meaningless:

```
import A = B
import B = A
```

You can have import statements at the toplevel, and you can import modules defined at the same level:

```
import A = B
method m() {
  A.whatever();
}
module B { ... }
```

In this case, everything is well defined because we can put `B` first, followed by the `A` import, and then finally `m()`. If there is no ordering, then Dafny will give an error, complaining about a cyclic dependency.

Note that when rearranging modules and imports, they have to be kept in the same containing module, which disallows some pathological module structures. Also, the imports and submodules are always considered to be first, even at the toplevel. This means that the following is not well formed:

```
method doIt() { }
module M {
  method m() {
    doIt();
  }
}
```

because the module `M` must come before any other kind of members, such as methods. To define global functions like this, you can put them in a module (called `Globals`, say) and open it into any module that needs its functionality. Finally, if you import via a path, such as `import A = B.C`, then this creates a dependency of `A` on `B`, as we need to know what `B` is (is it abstract or concrete, or a refinement?).

4.7 Name Resolution

When Dafny sees something like `A<T>.B<U>.C<V>`, how does it know what each part refers to? The process Dafny uses to determine what identifier sequences like this refer to is name resolution. Though the rules may seem complex, usually they do what you would expect. Dafny first looks up the initial identifier. Depending on what the first identifier refers to, the rest of the identifier is looked up in the appropriate context.

In terms of the grammar, sequences like the above are represented as a `NameSegment` followed by 0 or more `Suffix`es. A `Suffix` is more general and the form shown above would be for when the `Suffix` is an `AugmentedDotSuffix_`.

The resolution is different depending on whether it is in an expression context or a type context.

4.7.1 Expression Context Name Resolution

The leading `NameSegment` is resolved using the first following rule that succeeds.

0. Local variables, parameters and bound variables. These are things like `x`, `y`, and `i` in `var x;, ... returns (y: int)`, and `forall i :: ....` The declaration chosen is the match from the innermost matching scope.
1. If in a class, try to match a member of the class. If the member that is found is not static an implicit `this` is inserted. This works for fields, functions, and methods of the current class (if in a static context, then only static methods and functions are allowed). You can refer to fields of the current class either as `this.f` or `f`, assuming of course that `f` hasn't be hidden by one of the above. You can always prefix this if needed, which cannot be hidden. (Note, a field whose name is a string of digits must always have some prefix.)
2. If there is no `Suffix`, then look for a datatype constructor, if unambiguous. Any datatypes that don't need qualification (so the datatype name itself doesn't need a prefix), and also have a uniquely named constructor, can be referred to just by its name. So if `datatype List = Cons(List) | Nil` is the only datatype that declares `Cons` and `Nil` constructors, then you can write `Cons(Cons(Nil))`. If the constructor name is not unique, then you need to prefix it with the name of the datatype (for example `List.Cons(List.Nil))`. This is done per constructor, not per datatype.
3. Look for a member of the enclosing module.
4. Module-level (static) functions and methods

TODO: Not sure about the following paragraph. Opened modules are treated at each level, after the declarations in the current module. Opened modules only affect steps 2, 3 and 5. If a ambiguous name is found, an error is generated, rather than continuing down the list. After the first identifier, the rules are basically the same, except in the new context. For example, if the first identifier is a module, then the next identifier looks into that module. Opened modules only apply within the module it is opened into. When looking up into another module, only things explicitly declared in that module are considered.

To resolve expression `E.id`:

First resolve expression E and any type arguments.

- If `E` resolved to a module `M`:
  0. If `E.id<T>` is not followed by any further suffixes, look for unambiguous datatype constructor.

1. Member of module M: a sub-module (including submodules of imports), class, datatype, etc.
2. Static function or method.

- If `E` denotes a type:
  3. Look up id as a member of that type
- If `E` denotes an expression:
  4. Let T be the type of E. Look up id in T.

4.7.2 Type Context Name Resolution

In a type context the priority of `NameSegment` resolution is:

1. Type parameters.
2. Member of enclosing module (type name or the name of a module).

To resolve expression `E.id`:

- If `E` resolved to a module `M`:
  0. Member of module M: a sub-module (including submodules of imports), class, datatype, etc.
- If `E` denotes a type:
  1. If `allowDanglingDotName`: Return the type of `E` and the given `E.id`, letting the caller try to make sense of the final dot-name. TODO: I don't under this sentence. What is `allowDanglingDotName`?

5 Specifications

Specifications describe logical properties of Dafny methods, functions, lambdas, iterators and loops. They specify preconditions, postconditions, invariants, what memory locations may be read or modified, and termination information by means of *specification clauses*. For each kind of specification zero or more specification clauses (of the type accepted for that type of specification) may be given, in any order.

We document specifications at these levels:

- At the lowest level are the various kinds of specification clauses, e.g. a `RequiresClause_`.
- Next are the specifications for entities that need them, e.g. a `MethodSpec`.
- At the top level are the entity declarations that include the specifications, e.g. `MethodDecl`.

This section documents the first two of these in a bottom-up manner. We first document the clauses and then the specifications that use them.

5.1 Specification Clauses

5.1.1 Requires Clause

```
RequiresClause_ =
    "requires" Expression(allowLemma: false, allowLambda: false)
```

The **requires** clauses specify preconditions for methods, functions, lambda expressions and iterators. Dafny checks that the preconditions are met at all call sites. The callee may then assume the preconditions hold on entry.

If no **requires** clause is specified it is taken to be `true`.

If more than one **requires** clause is given, then the precondition is the conjunction of all of the expressions from all of the **requires** clauses.

5.1.2 Ensures Clause

```
EnsuresClause_ =
    "ensures" { Attribute } Expression(allowLemma: false, allowLambda: false)
ForAllEnsuresClause_ =
    "ensures" Expression(allowLemma: false, allowLambda: true)
FunctionEnsuresClause_ =
    "ensures" Expression(allowLemma: false, allowLambda: false)
```

An **ensures** clause specifies the post condition for a method, function or iterator.

If no **ensures** clause is specified it is taken to be `true`.

If more than one **ensures** clause is given, then the postcondition is the conjunction of all of the expressions from all of the **ensures** clauses.

TODO: In the present sources `FunctionEnsuresClause_` differs from `EnsuresClause_` only in that it is not allowed to specify `Attribute`s. This seems like a bug and will likely be fixed in a future version.

5.1.3 Decreases Clause

```
DecreasesClause_(allowWildcard, allowLambda) =
    "decreases" { Attribute } DecreasesList(allowWildcard, allowLambda)
FunctionDecreasesClause_(allowWildcard, allowLambda) =
    "decreases" DecreasesList(allowWildcard, allowLambda)
```

```
DecreasesList(allowWildcard, allowLambda) =
  PossiblyWildExpression(allowLambda)
  { "," PossiblyWildExpression(allowLambda) }
```

If `allowWildcard` is false but one of the `PossiblyWildExpression`s is a wildcard, an error is reported.

TODO: A `FunctionDecreasesClause_` is not allowed to specify `Attributes`. this will be fixed in a future version.

Decreases clauses are used to prove termination in the presence of recursion. if more than one **decreases** clause is given it is as if a single **decreases** clause had been given with the collected list of arguments. That is,

```
decreases A, B
decreases C, D
```

is equivalent to

```
decreases A, B, C, D
```

If any of the expressions in the **decreases** clause are wild (i.e. "*") then proof of termination will be skipped.

Termination metrics in Dafny, which are declared by **decreases** clauses, are lexicographic tuples of expressions. At each recursive (or mutually recursive) call to a function or method, Dafny checks that the effective **decreases** clause of the callee is strictly smaller than the effective **decreases** clause of the caller.

What does "strictly smaller" mean? Dafny provides a built-in well-founded order for every type and, in some cases, between types. For example, the Boolean "false" is strictly smaller than "true", the integer 78 is strictly smaller than 102, the set `{2,5}` is strictly smaller than the set `{2,3,5}`, and for "s" of type `seq<Color>` where `Color` is some inductive datatype, the color `s[0]` is strictly less than `s` (provided `s` is nonempty).

What does "effective decreases clause" mean? Dafny always appends a "top" element to the lexicographic tuple given by the user. This top element cannot be syntactically denoted in a Dafny program and it never occurs as a run-time value either. Rather, it is a fictitious value, which here we will denote $\top$, such that each value that can ever occur in a Dafny program is strictly less than $\top$. Dafny sometimes also prepends expressions to the lexicographic tuple given by the user. The effective decreases clause is any such prefix, followed by the user-provided decreases clause, followed by $\top$. We said "user-provided decreases clause", but if the user completely omits a "decreases" clause, then Dafny will usually make a guess at one, in which case the effective decreases clause is any prefix followed by the guess followed by $\top$. (If you're using the Dafny IDE in Visual Studio, you can hover the mouse over the name of a recursive function or method, or the "while" keyword for a loop, to see the "decreases" clause that Dafny guessed, if any.)

Here is a simple but interesting example: the Fibonacci function.

```
function Fib(n: nat) : nat
{
  if n < 2 then n else Fib(n-2) + Fib(n-1)
}
```

In this example, if you hover your mouse over the function name you will see that Dafny has supplied a `decreases n` clause.

Let's take a look at the kind of example where a mysterious-looking decreases clause like "Rank, 0" is useful.

Consider two mutually recursive methods, `A` and `B`:

```
method A(x: nat)
{
  B(x);
}

method B(x: nat)
{
  if x != 0 { A(x-1); }
}
```

To prove termination of `A` and `B`, Dafny needs to have effective decreases clauses for A and B such that:

- the measure for the callee `B(x)` is strictly smaller than the measure for the caller `A(x)`, and
- the measure for the callee `A(x-1)` is strictly smaller than the measure for the caller `B(x)`.

Satisfying the second of these conditions is easy, but what about the first? Note, for example, that declaring both `A` and `B` with "decreases x" does not work, because that won't prove a strict decrease for the call from `A(x)` to `B(x)`.

Here's one possibility (for brevity, we will omit the method bodies):

```
method A(x: nat)
  decreases x, 1

method B(x: nat)
  decreases x, 0
```

For the call from `A(x)` to `B(x)`, the lexicographic tuple `"x, 0"` is strictly smaller than `"x, 1"`, and for the call from `B(x)` to `A(x-1)`, the lexicographic tuple `"x-1, 1"` is strictly smaller than `"x, 0"`.

Two things to note: First, the choice of "0" and "1" as the second components of these lexicographic tuples is rather arbitrary. It could just as well have been "false" and "true", respectively, or the sets `{2,5}` and `{2,3,5}`. Second, the keyword **decreases** often gives rise to an intuitive English reading of the declaration. For example, you might say that the recursive calls in the definition of the familiar Fibonacci function `Fib(n)` "decreases n". But when the lexicographic tuple contains constants, the English reading of the declaration becomes mysterious and may give rise to questions like "how can you decrease the constant 0?". The keyword is just that—a keyword. It says "here comes a list of expressions that make up the lexicographic tuple we want to use for the termination measure". What is important is that one effective decreases clause is compared against another one, and it certainly makes sense to compare something to a constant (and to compare one constant to another).

We can simplify things a little bit by remembering that Dafny appends $\top$ to the user-supplied decreases clause. For the A-and-B example, this lets us drop the constant from the **decreases** clause of A:

```
method A(x: nat)
  decreases x

method B(x: nat)
  decreases x, 0
```

The effective decreases clause of `A` is "$x, \top$" and the effective decreases clause of `B` is "$x, 0, \top$". These tuples still satisfy the two conditions $(x, 0, \top) < (x, \top)$ and $(x - 1, \top) < (x, 0, \top)$. And as before, the constant "0" is arbitrary; anything less than $\top$ (which is any Dafny expression) would work.

Let's take a look at one more example that better illustrates the utility of $\top$. Consider again two mutually recursive methods, call them `Outer` and `Inner`, representing the recursive counterparts of what iteratively might be two nested loops:

```
method Outer(x: nat)
{
  // set y to an arbitrary non-negative integer
  var y :| 0 <= y;
  Inner(x, y);
}

method Inner(x: nat, y: nat)
{
  if y != 0 {
    Inner(x, y-1);
  } else if x != 0 {
    Outer(x-1);
  }
}
```

The body of `Outer` uses an assign-such-that statement to represent some computation that takes place before `Inner` is called. It sets "y" to some arbitrary non-negative value. In a more concrete example, `Inner` would do some work for each "y" and then continue as `Outer` on the next smaller "x".

Using a **decreases** clause `"x, y"` for `Inner` seems natural, but if we don't have any bound on the size of the `"y"` computed by `Outer`, there is no expression we can write in **decreases** clause of `Outer` that is sure to lead to a strictly smaller value for `"y"` when `Inner` is called. $\top$ to the rescue. If we arrange for the effective decreases clause of `Outer` to be "`x`, $\top$" and the effective decreases clause for `Inner` to be "`x`, `y`, $\top$", then we can show the strict decreases as required. Since $\top$ is implicitly appended, the two decreases clauses declared in the program text can be:

```
method Outer(x: nat)
  decreases x

method Inner(x: nat, y: nat)
  decreases x, y
```

Moreover, remember that if a function or method has no user-declared **decreases** clause, Dafny will make a guess. The guess is (usually) the list of arguments of the function/method, in the order given. This is exactly the decreases clauses needed here. Thus, Dafny successfully verifies the program without any explicit decreases clauses:

```
method Outer(x: nat)
{
  var y :| 0 <= y;
  Inner(x, y);
}

method Inner(x: nat, y: nat)
{
  if y != 0 {
    Inner(x, y-1);
  } else if x != 0 {
    Outer(x-1);
  }
}
```

The ingredients are simple, but the end result may seem like magic. For many users, however, there may be no magic at all – the end result may be so natural that the user never even has to bothered to think about that there was a need to prove termination in the first place.

5.1.4 Framing

```
FrameExpression(allowLemma, allowLambda) =
  ( Expression(allowLemma, allowLambda) [ FrameField ]
  | FrameField )

FrameField = "`" Ident

PossiblyWildFrameExpression(allowLemma) =
    ( "*" | FrameExpression(allowLemma, allowLambda: false) )
```

Frame expressions are used to denote the set of memory locations that a Dafny program element may read or write. A frame expression is a set expression. The form `{}` (that is, the empty set) says that no memory locations may be modified, which is also the default if no **modifies** clause is given explicitly.

Note that framing only applies to the heap, or memory accessed through references. Local variables are not stored on the heap, so they cannot be mentioned (well, they are not in scope in the declaration) in reads annotations. Note also that types like sets, sequences, and multisets are value types, and are treated like integers or local variables. Arrays and objects are reference types, and they are stored on the heap (though as always there is a subtle distinction between the reference itself and the value it points to.)

The `FrameField` construct is used to specify a field of a class object. The identifier following the back-quote is the name of the field being referenced. If the

`FrameField` is preceded by an expression the expression must be a reference to an object having that field. If the `FrameField` is not preceded by an expression then the frame expression is referring to that field of the current object. This form is only used from a method of a class.

The use of `FrameField` is discouraged as in practice it has not been shown to either be more concise or to perform better. Also, there's (unfortunately) no form of it for array elements—one could imagine

```
  modifies a`[j]
```

Also, `FrameField` is not taken into consideration for lambda expressions.

5.1.5 Reads Clause

```
FunctionReadsClause_ =
  "reads"
  PossiblyWildFrameExpression (allowLemma: false)
  { "," PossiblyWildFrameExpression(allowLemma: false) }
LambdaReadsClause_ =
  "reads" PossiblyWildFrameExpression(allowLemma: true)
  { "," PossiblyWildFrameExpression(allowLemma: true) }
IteratorReadsClause_ =
  "reads" { Attribute }
  FrameExpression(allowLemma: false, allowLambda: false)
  { "," FrameExpression(allowLemma: false, allowLambda: false) }
PossiblyWildExpression(allowLambda) =
    ( "*" | Expression(allowLemma: false, allowLambda) )
```

Functions are not allowed to have side effects but may be restricted in what they can read. The *reading frame* of a function (or predicate) is all the memory locations that the function is allowed to read. The reason we might limit what a function can read is so that when we write to memory, we can be sure that functions that did not read that part of memory have the same value they did before. For example, we might have two arrays, one of which we know is sorted. If we did not put a reads annotation on the sorted predicate, then when we modify the unsorted array, we cannot determine whether the other array stopped being sorted. While we might be able to give invariants to preserve it in this case, it gets even more complex when manipulating data structures. In this case, framing is essential to making the verification process feasible.

It is not just the body of a function that is subject to **reads** checks, but also its precondition and the **reads** clause itself.

A reads clause can list a wildcard (“*”), *which allows the enclosing function to read anything. In many cases, and in particular in all cases where the function is defined recursively, this makes it next to impossible to make any use of the*

function. Nevertheless, as an experimental feature, the language allows it (and it is sound). Note that a "" makes the rest of the frame expression irrelevant.

A **reads** clause specifies the set of memory locations that a function, lambda, or iterator may read. If more than one **reads** clause is given in a specification the effective read set is the union of the sets specified. If there are no **reads** clauses the effective read set is empty. If `"*"` is given in a **reads** clause it means any memory may be read.

TODO: It would be nice if the different forms of read clauses could be combined. In a future version the single form of read clause will allow a list and attributes.

TO BE WRITTEN: multiset of objects allowed in reads clauses

5.1.6 Modifies Clause

```
ModifiesClause_ =
  "modifies" { Attribute }
  FrameExpression(allowLemma: false, allowLambda: false)
  { "," FrameExpression(allowLemma: false, allowLambda: false) }
```

Frames also affect methods. As you might have guessed, methods are not required to list the things they read. Methods are allowed to read whatever memory they like, but they are required to list which parts of memory they modify, with a modifies annotation. They are almost identical to their reads cousins, except they say what can be changed, rather than what the value of the function depends on. In combination with reads, modification restrictions allow Dafny to prove properties of code that would otherwise be very difficult or impossible. Reads and modifies are one of the tools that allow Dafny to work on one method at a time, because they restrict what would otherwise be arbitrary modifications of memory to something that Dafny can reason about.

Note that fields of newly allocated objects can always be modified.

It is also possible to frame what can be modified by a block statement by means of the block form of the modify statement (Section [#sec-modify-statement]).

A **modifies** clause specifies the set of memory locations that a method, iterator or loop body may modify. If more than one **modifies** clause is given in a specification, the effective modifies set is the union of the sets specified. If no **modifies** clause is given the effective modifies set is empty. A loop can also have a **modifies** clause. If none is given, the loop gets to modify anything the enclosing context is allowed to modify.

5.1.7 Invariant Clause

```
InvariantClause_ =
    "invariant" { Attribute }
    Expression(allowLemma: false, allowLambda: true)
```

An **invariant** clause is used to specify an invariant for a loop. If more than one **invariant** clause is given for a loop the effective invariant is the conjunction of the conditions specified.

The invariant must hold on entry to the loop. And assuming it is valid on entry, Dafny must be able to prove that it then holds at the end of the loop.

5.2 Method Specification

```
MethodSpec =
  { ModifiesClause_
  | RequiresClause_
  | EnsuresClause_
  | DecreasesClause_(allowWildcard: true, allowLambda: false)
  }
```

A method specification is zero or more **modifies**, **requires**, **ensures** or **decreases** clauses, in any order. A method does not have **reads** clauses because methods are allowed to read any memory.

5.3 Function Specification

```
FunctionSpec =
  { RequiresClause_
  | FunctionReadsClause_
  | FunctionEnsuresClause_
  | FunctionDecreasesClause_(allowWildcard: false, allowLambda: false)
  }
```

A function specification is zero or more **reads**, **requires**, **ensures** or **decreases** clauses, in any order. A function specification does not have **modifies** clauses because functions are not allowed to modify any memory.

5.4 Lambda Specification

```
LambdaSpec_ =
  { LambdaReadsClause_
  | RequiresClause_
  }
```

A lambda specification is zero or more **reads** or **requires** clauses. Lambda specifications do not have **ensures** clauses because the body is never opaque. Lambda specifications do not have **decreases** clauses because they do not have names and thus cannot be recursive. A lambda specification does not have **modifies** clauses because lambdas are not allowed to modify any memory.

5.5 Iterator Specification

```
IteratorSpec =
  { IteratorReadsClause_
  | ModifiesClause_
  | [ "yield" ] RequiresClause_
  | [ "yield" ] EnsuresClause_
  | DecreasesClause_(allowWildcard: false, allowLambda: false)
  }
```

An iterator specification applies both to the iterator's constructor method and to its `MoveNext` method. The **reads** and **modifies** clauses apply to both of them. For the **requires** and **ensures** clauses, if `yield` is not present they apply to the constructor, but if `yield` is present they apply to the `MoveNext` method.

TODO: What is the meaning of a **decreases** clause on an iterator? Does it apply to `MoveNext`? Make sure our description of iterators explains these.

TODO: What is the relationship between the post condition and the `Valid()` predicate?

5.6 Loop Specification

```
LoopSpec =
  { InvariantClause_
  | DecreasesClause_(allowWildcard: true, allowLambda: true)
  | ModifiesClause_
  }
```

A loop specification provides the information Dafny needs to prove properties of a loop. The `InvariantClause_` clause is effectively a precondition and it along with the negation of the loop test condition provides the postcondition. The `DecreasesClause_` clause is used to prove termination.

5.7 Auto-generated boilerplate specifications

TO BE WRITTEN - {:autocontracts}

6 Types

```
Type = DomainType [ "->" Type ]
```

A Dafny type is a domain type (i.e. a type that can be the domain of a function type) optionally followed by an arrow and a range type.

```
DomainType =
  ( BoolType_ | CharType_ | NatType_ | IntType_ | RealType_ | ObjectType_
  | FiniteSetType_ | InfiniteSetType_ | MultisetType_
  | SequenceType_ | StringType_
  | FiniteMapType_ | InfiniteMapType_ | ArrayType_
  | TupleType_ | NamedType_ )
```

The domain types comprise the builtin scalar types, the builtin collection types, tuple types (including as a special case a parenthesized type) and reference types.

Dafny types may be categorized as either value types or reference types.

TO BE WRITTEN -bitvector types

TO BE WRITTEN - ORDINAL type

6.1 Value Types

The value types are those whose values do not lie in the program heap. These are:

- The basic scalar types: `bool`, `char`, `nat`, `int`, `real`
- The built-in collection types: `set`, `multiset`, `seq`, `string`, `map`, `imap`
- Tuple Types
- Inductive and co-inductive types

Data items having value types are passed by value. Since they are not considered to occupy *memory*, framing expressions do not reference them.

6.2 Reference Types

Dafny offers a host of *reference types*. These represent *references* to objects allocated dynamically in the program heap. To access the members of an object, a reference to (that is, a *pointer* to or *object identity* of) the object is *dereferenced*.

The reference types are class types, traits and array types.

The special value `null` is part of every reference type.[1]

[1] This will change in a future version of Dafny that will support both nullable and (by default) non-null reference types.

6.3 Named Types

```
NamedType_ = NameSegmentForTypeName { "." NameSegmentForTypeName }
```

A `NamedType_` is used to specify a user-defined type by name (possibly module-qualified). Named types are introduced by class, trait, inductive, co-inductive, synonym and opaque type declarations. They are also used to refer to type variables.

```
NameSegmentForTypeName = Ident  [ GenericInstantiation ]
```

A `NameSegmentForTypeName` is a type name optionally followed by a `GenericInstantiation` which supplies type parameters to a generic type, if needed. It is a special case of a `NameSegment` (See Section [#sec-name-segment]) that does not allow a `HashCall`.

The following sections describe each of these kinds of types in more detail.

7 Basic types

Dafny offers these basic types: `bool` for booleans, `char` for characters, `int` and `nat` for integers, and `real` for reals.

7.1 Booleans

```
BoolType_ = "bool"
```

There are two boolean values and each has a corresponding literal in the language: `false` and `true`.

In addition to equality (`==`) and disequality (`!=`), which are defined on all types, type `bool` supports the following operations:

operator	description
`<==>`	equivalence (if and only if)
`==>`	implication (implies)
`<==`	reverse implication (follows from)
`&&`	conjunction (and)
`||`	disjunction (or)
`!`	negation (not)

Negation is unary; the others are binary. The table shows the operators in

groups of increasing binding power, with equality binding stronger than conjunction and disjunction, and weaker than negation. Within each group, different operators do not associate, so parentheses need to be used. For example,

```
A && B || C    // error
```

would be ambiguous and instead has to be written as either

```
(A && B) || C
```

or

```
A && (B || C)
```

depending on the intended meaning.

7.1.1 Equivalence Operator

The expressions `A <==> B` and `A == B` give the same value, but note that `<==>` is *associative* whereas `==` is *chaining*. So,

```
A <==> B <==> C
```

is the same as

```
A <==> (B <==> C)
```

and

```
(A <==> B) <==> C
```

whereas

```
A == B == C
```

is simply a shorthand for

```
A == B && B == C
```

7.1.2 Conjunction and Disjunction

Conjunction is associative and so is disjunction. These operators are *short circuiting (from left to right)*, meaning that their second argument is evaluated only if the evaluation of the first operand does not determine the value of the expression. Logically speaking, the expression `A && B` is defined when `A` is defined and either `A` evaluates to `false` or `B` is defined. When `A && B` is defined, its meaning is the same as the ordinary, symmetric mathematical conjunction . The same holds for `||` and .

7.1.3 Implication and Reverse Implication

Implication is *right associative* and is short-circuiting from left to right. Reverse implication `B <== A` is exactly the same as `A ==> B`, but gives the ability to

write the operands in the opposite order. Consequently, reverse implication is *left associative* and is short-circuiting from *right to left*. To illustrate the associativity rules, each of the following four lines expresses the same property, for any `A`, `B`, and `C` of type `bool`:

```
A ==> B ==> C
A ==> (B ==> C)  // parentheses redundant, since ==> is right associative
C <== B <== A
(C <== B) <== A  // parentheses redundant, since <== is left associative
```

To illustrate the short-circuiting rules, note that the expression `a.Length` is defined for an array `a` only if `a` is not `null` (see Section [#sec-reference-types]), which means the following two expressions are well-formed:

```
a != null ==> 0 <= a.Length
0 <= a.Length <== a != null
```

The contrapositive of these two expressions would be:

```
a.Length < 0 ==> a == null  // not well-formed
a == null <== a.Length < 0  // not well-formed
```

but these expressions are not well-formed, since well-formedness requires the left (and right, respectively) operand, `a.Length < 0`, to be well-formed by itself.

Implication `A ==> B` is equivalent to the disjunction `!A || B`, but is sometimes (especially in specifications) clearer to read. Since, `||` is short-circuiting from left to right, note that

```
a == null || 0 <= a.Length
```

is well-formed, whereas

```
0 <= a.Length || a == null  // not well-formed
```

is not.

In addition, booleans support *logical quantifiers* (forall and exists), described in section [#sec-quantifier-expression].

7.2 Numeric types

```
IntType_ = "int"
RealType_ = "real"
```

Dafny supports *numeric types* of two kinds, *integer-based*, which includes the basic type `int` of all integers, and *real-based*, which includes the basic type `real` of all real numbers. User-defined numeric types based on `int` and `real`, called *newtypes*, are described in Section [#sec-newtypes]. Also, the *subset type* `nat`,

representing the non-negative subrange of `int`, is described in Section [#sec-subset-types].

The language includes a literal for each non-negative integer, like `0`, `13`, and `1985`. Integers can also be written in hexadecimal using the prefix "`0x`", as in `0x0`, `0xD`, and `0x7c1` (always with a lower case `x`, but the hexadecimal digits themselves are case insensitive). Leading zeros are allowed. To form negative integers, use the unary minus operator.

There are also literals for some of the non-negative reals. These are written as a decimal point with a nonempty sequence of decimal digits on both sides. For example, `1.0`, `1609.344`, and `0.5772156649`.

For integers (in both decimal and hexadecimal form) and reals, any two digits in a literal may be separated by an underscore in order to improve human readability of the literals. For example:

```
1_000_000         // easier to read than 1000000
0_12_345_6789     // strange but legal formatting of 123456789
0x8000_0000       // same as 0x80000000 -- hex digits are often placed in groups of 4
0.000_000_000_1   // same as 0.0000000001 -- 1 \([&Aring;ngstr&ouml;m]{.comment-color}\)
```

In addition to equality and disequality, numeric types support the following relational operations:

operator	description
`<`	less than
`<=`	at most
`>=`	at least
`>`	greater than

Like equality and disequality, these operators are chaining, as long as they are chained in the "same direction". That is,

```
A <= B < C == D <= E
```

is simply a shorthand for

```
A <= B && B < C && C == D && D <= E
```

whereas

```
A < B > C
```

is not allowed.

There are also operators on each numeric type:

operator	description
`+`	addition (plus)
`-`	subtraction (minus)
`*`	multiplication (times)
`/`	division (divided by)
`%`	modulus (mod)
`-`	negation (unary minus)

The binary operators are left associative, and they associate with each other in the two groups. The groups are listed in order of increasing binding power, with equality binding more strongly than the multiplicative operators and weaker than the unary operator. Modulus is supported only for integer-based numeric types. Integer division and modulus are the *Euclidean division and modulus*. This means that modulus always returns a non-negative, regardless of the signs of the two operands. More precisely, for any integer `a` and non-zero integer `b`,

```
a == a / b * b + a % b
0 <= a % b < B
```

where `B` denotes the absolute value of `b`.

Real-based numeric types have a member `Floor` that returns the *floor* of the real value, that is, the largest integer not exceeding the real value. For example, the following properties hold, for any `r` and `r'` of type `real`:

```
3.14.Floor == 3
(-2.5).Floor == -3
-2.5.Floor == -2
real(r.Floor) <= r
r <= r' ==> r.Floor <= r'.Floor
```

Note in the third line that member access (like `.Floor`) binds stronger than unary minus. The fourth line uses the conversion function `real` from `int` to `real`, as described in Section [#sec-numeric-conversion-operations].

7.3 Characters

```
CharType_ = "char"
```

Dafny supports a type `char` of *characters*. Character literals are enclosed in single quotes, as in `'D'`. Their form is described by the `charToken` nonterminal in the grammar. To write a single quote as a character literal, it is necessary to use an *escape sequence*. Escape sequences can also be used to write other characters. The supported escape sequences are as follows:

escape sequence	meaning
`\'`	the character `'`
`\"`	the character `"`
`\\`	the character `\`
`\0`	the null character, same as `\u0000`
`\n`	line feed
`\r`	carriage return
`\t`	horizontal tab
`\u`*xxxx*	universal character whose hexadecimal code is *xxxx*, where each *x* is a hexadecimal digit

The escape sequence for a double quote is redundant, because `'"'` and `'\"'` denote the same character—both forms are provided in order to support the same escape sequences as for string literals (Section [#sec-strings]). In the form `\u\(_xxxx_\)`, the `u` is always lower case, but the four hexadecimal digits are case insensitive.

Character values are ordered and can be compared using the standard relational operators:

operator	description
`<`	less than
`<=`	at most
`>=`	at least
`>`	greater than

Sequences of characters represent *strings*, as described in Section [#sec-strings].

The only other operations on characters are obtaining a character by indexing into a string, and the implicit conversion to string when used as a parameter of a `print` statement.

TODO: Are there any conversions between `char` values and numeric values?

8 Type parameters

```
GenericParameters = "<" TypeVariableName [ "(" "==" ")" ]
      { "," TypeVariableName [ "(" "==" ")" ] } ">"
```

Many of the types (as well as functions and methods) in Dafny can be parameterized by types. These *type parameters* are typically declared inside angle brackets and can stand for any type.

It is sometimes necessary to restrict these type parameters so that they can only be instantiated by certain families of types. As such, Dafny distinguishes types that support the equality operation not only in ghost contexts but also in compiled contexts. To indicate that a type parameter is restricted to such *equality supporting* types, the name of the type parameter takes the suffix "`(==)`".[2] For example,

```
method Compare<T(==)>(a: T, b: T) returns (eq: bool)
{
  if a == b { eq := true; } else { eq := false; }
}
```

is a method whose type parameter is restricted to equality-supporting types. Again, note that *all* types support equality in *ghost* contexts; the difference is only for non-ghost (that is, compiled) code. Co-inductive datatypes, function types, as well as inductive datatypes with ghost parameters are examples of types that are not equality supporting.

Dafny has some inference support that makes certain signatures less cluttered (described in a different part of the Dafny language reference). In some cases, this support will infer that a type parameter must be restricted to equality-supporting types, in which case Dafny adds the "`(==)`" automatically.

TO BE WRITTEN: Type parameter variance with + - = * ! default

TO BE WRITTEN: Type parameter characteristiscs: == 0 !new

TODO: Need to describe type inference somewhere.

9 Generic Instantiation

```
GenericInstantiation = "<" Type { "," Type } ">"
```

When a generic entity is used, actual types must be specified for each generic parameter. This is done using a `GenericInstantiation`. If the `GenericInstantiation` is omitted, type inference will try to fill these in.

10 Collection types

Dafny offers several built-in collection types.

[2] Being equality-supporting is just one of many *modes* that one can imagine types in a rich type system to have. For example, other modes could include having a total order, being zero-initializable, and possibly being uninhabited. If Dafny were to support more modes in the future, the "`(\( \))`"-suffix syntax may be extended. For now, the suffix can only indicate the equality-supporting mode.

10.1 Sets

```
FiniteSetType_ = "set" [ GenericInstantiation ]
InfiniteSetType_ = "iset" [ GenericInstantiation ]
```

For any type `T`, each value of type `set<T>` is a finite set of `T` values.

TODO: Set membership is determined by equality in the type `T`, so `set<T>` can be used in a non-ghost context only if `T` is equality supporting.

For any type `T`, each value of type `iset<T>` is a potentially infinite set of `T` values.

A set can be formed using a *set display* expression, which is a possibly empty, unordered, duplicate-insensitive list of expressions enclosed in curly braces. To illustrate,

```
{}        {2, 7, 5, 3}        {4+2, 1+5, a*b}
```

are three examples of set displays. There is also a *set comprehension* expression (with a binder, like in logical quantifications), described in section [#sec-set-comprehension-expressions].

In addition to equality and disequality, set types support the following relational operations:

operator	description
`<`	proper subset
`<=`	subset
`>=`	superset
`>`	proper superset

Like the arithmetic relational operators, these operators are chaining.

Sets support the following binary operators, listed in order of increasing binding power:

operator	description
`!!`	disjointness
`+`	set union
`-`	set difference
`*`	set intersection

The associativity rules of `+`, `-`, and `*` are like those of the arithmetic operators

with the same names. The expression `A !! B`, whose binding power is the same as equality (but which neither associates nor chains with equality), says that sets `A` and `B` have no elements in common, that is, it is equivalent to

```
A * B == {}
```

However, the disjointness operator is chaining, so `A !! B !! C !! D` means:

```
A * B == {} && (A + B) * C == {} && (A + B + C) * D == {}
```

In addition, for any set `s` of type `set<T>` or `iset<T>` and any expression `e` of type `T`, sets support the following operations:

expression	description
|s|	set cardinality
`e in s`	set membership
`e !in s`	set non-membership

The expression `e !in s` is a syntactic shorthand for `!(e in s)`.

10.2 Multisets

```
MultisetType_ = "multiset" [ GenericInstantiation ]
```

A *multiset* is similar to a set, but keeps track of the multiplicity of each element, not just its presence or absence. For any type `T`, each value of type `multiset<T>` is a map from `T` values to natural numbers denoting each element's multiplicity. Multisets in Dafny are finite, that is, they contain a finite number of each of a finite set of elements. Stated differently, a multiset maps only a finite number of elements to non-zero (finite) multiplicities.

Like sets, multiset membership is determined by equality in the type `T`, so `multiset<T>` can be used in a non-ghost context only if `T` is equality supporting.

A multiset can be formed using a *multiset display* expression, which is a possibly empty, unordered list of expressions enclosed in curly braces after the keyword `multiset`. To illustrate,

```
multiset{}    multiset{0, 1, 1, 2, 3, 5}    multiset{4+2, 1+5, a*b}
```

are three examples of multiset displays. There is no multiset comprehension expression.

In addition to equality and disequality, multiset types support the following relational operations:

operator	description
`<`	proper multiset subset
`<=`	multiset subset
`>=`	multiset superset
`>`	proper multiset superset

Like the arithmetic relational operators, these operators are chaining.

Multisets support the following binary operators, listed in order of increasing binding power:

operator	description
`!!`	multiset disjointness
`+`	multiset union
`-`	multiset difference
`*`	multiset intersection

The associativity rules of `+`, `-`, and `*` are like those of the arithmetic operators with the same names. The `+` operator adds the multiplicity of corresponding elements, the `-` operator subtracts them (but 0 is the minimum multiplicity), and the `*` has multiplicity that is the minimum of the multiplicity of the operands.

The expression `A !! B` says that multisets `A` and `B` have no elements in common, that is, it is equivalent to

```
A * B == multiset{}
```

Like the analogous set operator, `!!` is chaining.

In addition, for any multiset `s` of type `multiset<T>`, expression `e` of type `T`, and non-negative integer-based numeric `n`, multisets support the following operations:

expression	description
`|s|`	multiset cardinality
`e in s`	multiset membership
`e !in s`	multiset non-membership
`s[e]`	multiplicity of `e` in `s`
`s[e := n]`	multiset update (change of multiplicity)

The expression `e in s` returns `true` if and only if `s[e] != 0`. The expression

`e !in s` is a syntactic shorthand for `!(e in s)`. The expression `s[e := n]` denotes a multiset like `s`, but where the multiplicity of element `e` is `n`. Note that the multiset update `s[e := 0]` results in a multiset like `s` but without any occurrences of `e` (whether or not `s` has occurrences of `e` in the first place). As another example, note that `s - multiset{e}` is equivalent to:

```
if e in s then s[e := s[e] - 1] else s
```

10.3 Sequences

```
SequenceType_ = "seq" [ GenericInstantiation ]
```

For any type `T`, a value of type `seq<T>` denotes a *sequence* of `T` elements, that is, a mapping from a finite downward-closed set of natural numbers (called *indices*) to `T` values. (Thinking of it as a map, a sequence is therefore something of a dual of a multiset.)

10.3.1 Sequence Displays

A sequence can be formed using a *sequence display* expression, which is a possibly empty, ordered list of expressions enclosed in square brackets. To illustrate,

```
[]        [3, 1, 4, 1, 5, 9, 3]        [4+2, 1+5, a*b]
```

are three examples of sequence displays. There is no sequence comprehension expression.

10.3.2 Sequence Relational Operators

In addition to equality and disequality, sequence types support the following relational operations:

operator	description
`<`	proper prefix
`<=`	prefix

Like the arithmetic relational operators, these operators are chaining. Note the absence of `>` and `>=`.

10.3.3 Sequence Concatenation

Sequences support the following binary operator:

operator	description
`+`	concatenation

Operator `+` is associative, like the arithmetic operator with the same name.

10.3.4 Other Sequence Expressions

In addition, for any sequence `s` of type `seq<T>`, expression `e` of type `T`, integer-based numeric `i` satisfying `0 <= i < |s|`, and integer-based numerics `lo` and `hi` satisfying `0 <= lo <= hi <= |s|`, sequences support the following operations:

expression	description
`|s|`	sequence length
`s[i]`	sequence selection
`s[i := e]`	sequence update
`e in s`	sequence membership
`e !in s`	sequence non-membership
`s[lo..hi]`	subsequence
`s[lo..]`	drop
`s[..hi]`	take
`s[\(_slices_\)]`	slice
`multiset(s)`	sequence conversion to a `multiset<T>`

Expression `s[i := e]` returns a sequence like `s`, except that the element at index `i` is `e`. The expression `e in s` says there exists an index `i` such that `s[i] == e`. It is allowed in non-ghost contexts only if the element type `T` is equality supporting. The expression `e !in s` is a syntactic shorthand for `!(e in s)`.

Expression `s[lo..hi]` yields a sequence formed by taking the first `hi` elements and then dropping the first `lo` elements. The resulting sequence thus has length `hi - lo`. Note that `s[0..|s|]` equals `s`. If the upper bound is omitted, it defaults to `|s|`, so `s[lo..]` yields the sequence formed by dropping the first `lo` elements of `s`. If the lower bound is omitted, it defaults to `0`, so `s[..hi]` yields the sequence formed by taking the first `hi` elements of `s`.

In the sequence slice operation, `\(_slices_\)` is a nonempty list of length designators separated and optionally terminated by a colon, and there is at least one colon. Each length designator is a non-negative integer-based numeric, whose sum is no greater than `|s|`. If there are k colons, the operation produces $k + 1$ consecutive subsequences from `s`, each of the length indicated by the corresponding length designator, and returns these as a sequence of sequences.[3] If `\(_slices_\)` is terminated by a colon, then the length of the last slice

[3] Now that Dafny supports built-in tuples, the plan is to change the sequence slice operation to return not a sequence of subsequences, but a tuple of subsequences.

extends until the end of `s`, that is, its length is `|s|` minus the sum of the given length designators. For example, the following equalities hold, for any sequence `s` of length at least `10`:

```
var t := [3.14, 2.7, 1.41, 1985.44, 100.0, 37.2][1:0:3];
assert |t| == 3 && t[0] == [3.14] && t[1] == [];
assert t[2] == [2.7, 1.41, 1985.44];
var u := [true, false, false, true][1:1:];
assert |u| == 3 && u[0][0] && !u[1][0] && u[2] == [false, true];
assert s[10:][0] == s[..10];
assert s[10:][1] == s[10..];
```

The operation `multiset(s)` yields the multiset of elements of sequence `s`. It is allowed in non-ghost contexts only if the element type `T` is equality supporting.

10.3.5 Strings

```
StringType_ = "string"
```

A special case of a sequence type is `seq<char>`, for which Dafny provides a synonym: `string`. Strings are like other sequences, but provide additional syntax for sequence display expressions, namely *string literals*. There are two forms of the syntax for string literals: the *standard form* and the *verbatim form*.

String literals of the standard form are enclosed in double quotes, as in `"Dafny"`. To include a double quote in such a string literal, it is necessary to use an escape sequence. Escape sequences can also be used to include other characters. The supported escape sequences are the same as those for character literals, see Section [#sec-characters]. For example, the Dafny expression `"say \"yes\""` represents the string `'say "yes"'`. The escape sequence for a single quote is redundant, because "'" and "\'" denote the same string—both forms are provided in order to support the same escape sequences as for character literals.

String literals of the verbatim form are bracketed by [@"]{.monospace} and ", as in `@"Dafny"`. To include a double quote in such a string literal, it is necessary to use the escape sequence "", that is, to write the character twice. In the verbatim form, there are no other escape sequences. Even characters like newline can be written inside the string literal (hence spanning more than one line in the program text).

For example, the following three expressions denote the same string:

```
"C:\\tmp.txt"
@"C:\tmp.txt"
['C', ':', '\\', 't', 'm', 'p', '.', 't', 'x', 't']
```

Since strings are sequences, the relational operators $<$ and `<=` are defined on them. Note, however, that these operators still denote proper prefix and prefix,

respectively, not some kind of alphabetic comparison as might be desirable, for example, when sorting strings.

10.4 Finite and Infinite Maps

```
FiniteMapType_ = "map" [ GenericInstantiation ]
InfiniteMapType_ = "imap" [ GenericInstantiation ]
```

For any types `T` and `U`, a value of type `map<T,U>` denotes a *(finite) map* from `T` to `U`. In other words, it is a look-up table indexed by `T`. The *domain* of the map is a finite set of `T` values that have associated `U` values. Since the keys in the domain are compared using equality in the type `T`, type `map<T,U>` can be used in a non-ghost context only if `T` is equality supporting.

Similarly, for any types `T` and `U`, a value of type `imap<T,U>` denotes a *(possibly) infinite map*. In most regards, `imap<T,U>` is like `map<T,U>`, but a map of type `imap<T,U>` is allowed to have an infinite domain.

A map can be formed using a *map display* expression (see `MapDisplayExpr`), which is a possibly empty, ordered list of *maplets*, each maplet having the form `t := u` where `t` is an expression of type `T` and `u` is an expression of type `U`, enclosed in square brackets after the keyword `map`. To illustrate,

```
map[]    map[20 := true, 3 := false, 20 := false]    map[a+b := c+d]
```

are three examples of map displays. By using the keyword `imap` instead of `map`, the map produced will be of type `imap<T,U>` instead of `map<T,U>`. Note that an infinite map (`imap`) is allowed to have a finite domain, whereas a finite map (`map`) is not allowed to have an infinite domain. If the same key occurs more than once, only the last occurrence appears in the resulting map.[4] There is also a *map comprehension expression*, explained in section [#sec-map-comprehension-expression].

For any map `fm` of type `map<T,U>`, any map `m` of type `map<T,U>` or `imap<T,U>`, any expression `t` of type `T`, any expression `u` of type `U`, and any `d` in the domain of `m` (that is, satisfying `d in m`), maps support the following operations:

expression	description
`|fm|`	map cardinality
`m[d]`	map selection
`m[t := u]`	map update
`t in m`	map domain membership
`t !in m`	map domain non-membership
`fm.Keys`	the domain of fm, that is, the set of T values used askeys

[4] This is likely to change in the future to disallow multiple occurrences of the same key.

expression	description
`fm.Values`	the range of fm, that is, the set of U values present in the map
`fm.Items`	set of pairs (t,u) of key-value associations in the map

`|fm|` denotes the number of mappings in `fm`, that is, the cardinality of the domain of `fm`. Note that the cardinality operator is not supported for infinite maps. Expression `m[d]` returns the `U` value that `m` associates with `d`. Expression `m[t := u]` is a map like `m`, except that the element at key `t` is `u`. The expression `t in m` says `t` is in the domain of `m` and `t !in m` is a syntactic shorthand for `!(t in m)`.[5]

The expressions `m.Keys`, `m.Values`, and `m.Items` return, as sets, the domain, the range, and the 2-tuples holding the key-value associations in the map. Note that `m.Values` will have a different cardinality than `m.Keys` and `m.Items` if different keys are associated with the same value.

Here is a small example, where a map `cache` of type `map<int,real>` is used to cache computed values of Joule-Thomson coefficients for some fixed gas at a given temperature:

```
if K in cache {  // check if temperature is in domain of cache
  coeff := cache[K];  // read result in cache
} else {
  coeff := ComputeJouleThomsonCoefficient(K);  // do expensive computation
  cache := cache[K := coeff];  // update the cache
}
```

TO BE WRITTEN – .Keys, .Values, .Items

11 Types that stand for other types

```
SynonymTypeDecl =
  ( SynonymTypeDefinition_ | OpaqueTypeDefinition_ ) [ ";" ]
```

It is sometimes useful to know a type by several names or to treat a type abstractly. Synonym and opaque types serve this purpose.

[5] This is likely to change in the future as follows: The `in` and `!in` operations will no longer be supported on maps, with `x in m` replaced by `x in m.Keys`, and similarly for `!in`.

11.1 Type synonyms

```
SynonymTypeDefinition_ =
  "type" { Attribute } SynonymTypeName [ GenericParameters ] "=" Type
```

A *type synonym* declaration:

```
type Y<T> = G
```

declares `Y<T>` to be a synonym for the type `G`. Here, `T` is a nonempty list of type parameters (each of which is optionally designated with the suffix "`(==)`"), which can be used as free type variables in `G`. If the synonym has no type parameters, the "`<T>`" is dropped. In all cases, a type synonym is just a synonym. That is, there is never a difference, other than possibly in error messages produced, between `Y<T>` and `G`.

For example, the names of the following type synonyms may improve the readability of a program:

```
type Replacements<T> = map<T,T>
type Vertex = int
```

As already described in Section [#sec-strings], `string` is a built-in type synonym for `seq<char>`, as if it would have been declared as follows:

```
type string = seq<char>
```

11.2 Opaque types

```
OpaqueTypeDefinition_ = "type" { Attribute } SynonymTypeName
  [ "(" "==" ")" ] [ GenericParameters ]
```

A special case of a type synonym is one that is underspecified. Such a type is declared simply by:

```
type Y<T>
```

It is known as an *opaque type*. Its definition can be revealed in a refining module. To indicate that `Y` designates an equality-supporting type, "`(==)`" can be written immediately following the name "`Y`".

For example, the declarations

```
type T
function F(t: T): T
```

can be used to model an uninterpreted function `F` on some arbitrary type `T`. As another example,

```
type Monad<T>
```

can be used abstractly to represent an arbitrary parameterized monad.

12 Well-founded Functions and Extreme Predicates

This section is a tutorial on well-founded functions and extreme predicates. We place it here in preparation for Section [#sec-class-types] where function and predicate definitions are described.

Recursive functions are a core part of computer science and mathematics. Roughly speaking, when the definition of such a function spells out a terminating computation from given arguments, we may refer to it as a *well-founded function*. For example, the common factorial and Fibonacci functions are well-founded functions.

There are also other ways to define functions. An important case regards the definition of a boolean function as an extreme solution (that is, a least or greatest solution) to some equation. For computer scientists with interests in logic or programming languages, these *extreme predicates* are important because they describe the judgments that can be justified by a given set of inference rules (see, e.g., [@CamilleriMelham:InductiveRelations; @Winskel:FormalSemantics; @LeroyGrall:CoinductiveBigStep; @Pierce:SoftwareFoundations; @NipkowKlein:ConcreteSemantics]).

To benefit from machine-assisted reasoning, it is necessary not just to understand extreme predicates but also to have techniques for proving theorems about them. A foundation for this reasoning was developed by Paulin-Mohring [@PaulinMohring:InductiveCoq] and is the basis of the constructive logic supported by Coq [@Coq:book] as well as other proof assistants [@BoveDybjerNorell:BriefAgda; @SwamyEtAl:Fstar2011]. Essentially, the idea is to represent the knowledge that an extreme predicate holds by the proof term by which this knowledge was derived. For a predicate defined as the least solution, such proof terms are values of an inductive datatype (that is, finite proof trees), and for the greatest solution, a coinductive datatype (that is, possibly infinite proof trees). This means that one can use induction and coinduction when reasoning about these proof trees. Therefore, these extreme predicates are known as, respectively, *inductive predicates* and *coinductive predicates* (or, *co-predicates* for short). Support for extreme predicates is also available in the proof assistants Isabelle [@Paulson:CADE1994] and HOL [@Harrison:InductiveDefs].

Dafny supports both well-founded functions and extreme predicates. This section is a tutorial that describes the difference in general terms, and then describes novel syntactic support in Dafny for defining and proving lemmas with extreme predicates. Although Dafny's verifier has at its core a first-order SMT

solver, Dafny's logical encoding makes it possible to reason about fixpoints in an automated way.

The encoding for coinductive predicates in Dafny was described previously [@LeinoMoskal:Coinduction] and is here described in Section [#sec-co-inductive-datatypes].

12.1 Function Definitions

To define a function $f : X \to Y$ in terms of itself, one can write an equation like
~ Equation {#eq-general}

$$f = \mathcal{F}(f)$$

~

where $\mathcal{F}$ is a non-recursive function of type $(X \to Y) \to X \to Y$.
Because it takes a function as an argument, $\mathcal{F}$ is referred to as a *functor* (or *functional*, but not to be confused by the category-theory notion of a functor). Throughout, I will assume that $\mathcal{F}(f)$ by itself is well defined, for example that it does not divide by zero. I will also assume that f occurs only in fully applied calls in $\mathcal{F}(f)$; eta expansion can be applied to ensure this. If f is a `boolean` function, that is, if Y is the type of booleans, then I call f a *predicate*.

For example, the common Fibonacci function over the natural numbers can be defined by the equation

$$\mathit{fib} = \lambda n \bullet \textbf{if } n < 2 \textbf{ then } n \textbf{ else } \mathit{fib}(n-2) + \mathit{fib}(n-1)$$

With the understanding that the argument n is universally quantified, we can write this equation equivalently as

~ Equation {#eq-fib}

$$\mathit{fib}(n) = \textbf{if } n < 2 \textbf{ then } n \textbf{ else } \mathit{fib}(n-2)$$

~

The fact that the function being defined occurs on both sides of the equation causes concern that we might not be defining the function properly, leading to a logical inconsistency. In general, there could be many solutions to an equation like [#eq-general] or there could be none. Let's consider two ways to make sure we're defining the function uniquely.

TO BE WRITTEN - two-state functions and predicates

TO BE WRITTEN - functions with named results

TO BE WRITTEN - various kinds of arrow types: ~> -> –>

12.1.1 Well-founded Functions

A standard way to ensure that equation [#eq-general] has a unique solution in f is to make sure the recursion is well-founded, which roughly means that the recursion terminates. This is done by introducing any well-founded relation $\ll$ on the domain of f and making sure that the argument to each recursive call goes down in this ordering. More precisely, if we formulate [#eq-general] as

$$f(x) = \mathcal{F}'(f)$$

then we want to check $E \ll x$ for each call $f(E)$ in $f(x) = \mathcal{F}'(f)$. When a function definition satisfies this *decrement condition*, then the function is said to be *well-founded*.

For example, to check the decrement condition for *fib* in [#eq-fib], we can pick $\ll$ to be the arithmetic less-than relation on natural numbers and check the following, for any n:

$$2 \leq n \implies n-2 \ll n \ \wedge \ n-1 \ll n$$

Note that we are entitled to use the antecedent $2 \leq n$ because that is the condition under which the else branch in [#eq-fib] is evaluated.

A well-founded function is often thought of as "terminating" in the sense that the recursive *depth* in evaluating f on any given argument is finite. That is, there are no infinite descending chains of recursive calls. However, the evaluation of f on a given argument may fail to terminate, because its *width* may be infinite. For example, let P be some predicate defined on the ordinals and let $P_{\downarrow}$ be a predicate on the ordinals defined by the following equation:

$$P\_\downarrow = P(o) \ \wedge \ \forall p \bullet \ p \ll o \implies P\_\downarrow(p)$$

With $\ll$ as the usual ordering on ordinals, this equation satisfies the decrement condition, but evaluating $P\_\downarrow(\omega)$ would require evaluating $P\_\downarrow(n)$ for every natural number n. However, what we are concerned about here is to avoid mathematical inconsistencies, and that is indeed a consequence of the decrement condition.

12.1.1.1 Example with Well-founded Functions So that we can later see how inductive proofs are done in Dafny, let's prove that for any n, $\mathit{fib}(n)$ is even iff n is a multiple of 3. We split our task into two cases. If $n < 2$, then the property follows directly from the definition of *fib*. Otherwise, note that exactly one of the three numbers $n-2$, $n-1$, and n is a multiple of 3. If n is the multiple of 3, then by invoking the induction hypothesis on $n-2$ and $n-1$, we obtain that $\mathit{fib}(n-2) + \mathit{fib}(n-1)$ is the sum of two odd numbers, which is even.

If $n-2$ or $n-1$ is a multiple of 3, then by invoking the induction hypothesis on $n-2$ and $n-1$, we obtain that $\mathit{fib}(n-2) + \mathit{fib}(n-1)$ is the sum of an even number and an odd number, which is odd. In this proof, we invoked the induction hypothesis on $n-2$ and on $n-1$. This is allowed, because both are smaller than n, and hence the invocations go down in the well-founded ordering on natural numbers.

12.1.2 Extreme Solutions

We don't need to exclude the possibility of equation [#eq-general] having multiple solutions—instead, we can just be clear about which one of them we want. Let's explore this, after a smidgen of lattice theory.

For any complete lattice $(Y, \leq)$ and any set X, we can by *pointwise extension* define a complete lattice $(X \to Y, \dot{\Rightarrow})$, where for any $f, g\colon X \to Y$,

Equation

$$f \dot{\Rightarrow} g \quad \equiv \quad \forall x \bullet\ f(x) \leq g(x)$$

In particular, if Y is the set of booleans ordered by implication (`false` $\leq$ `true`), then the set of predicates over any domain X forms a complete lattice. Tarski's Theorem [@Tarski:theorem] tells us that any monotonic function over a complete lattice has a least and a greatest fixpoint. In particular, this means that $\mathcal{F}$ has a least fixpoint and a greatest fixpoint, provided $\mathcal{F}$ is monotonic.

Speaking about the *set of solutions* in f to [#eq-general] is the same as speaking about the *set of fixpoints* of functor $\mathcal{F}$. In particular, the least and greatest solutions to [#eq-general] are the same as the least and greatest fixpoints of $\mathcal{F}$. In casual speak, it happens that we say "fixpoint of [#eq-general]", or more grotesquely, "fixpoint of f" when we really mean "fixpoint of $\mathcal{F}$".

In conclusion of our little excursion into lattice theory, we have that, under the proviso of $\mathcal{F}$ being monotonic, the set of solutions in f to [#eq-general] is nonempty, and among these solutions, there is in the $\dot{\Rightarrow}$ ordering a least solution (that is, a function that returns `false` more often than any other) and a greatest solution (that is, a function that returns `true` more often than any other).

When discussing extreme solutions, I will now restrict my attention to boolean functions (that is, with Y being the type of booleans). Functor $\mathcal{F}$ is monotonic if the calls to f in $\mathcal{F}'(f)$ are in *positive positions* (that is, under an even number of negations). Indeed, from now on, I will restrict my attention to such monotonic functors $\mathcal{F}$.

Let me introduce a running example. Consider the following equation, where x ranges over the integers:

~ Equation {#eq-EvenNat}

$$g(x) = (x = 0 \ \vee \ g(x-2))$$

~

This equation has four solutions in g. With w ranging over the integers, they are:

Equation

$$\begin{array}{lcl} g(x) & \equiv & x \in \{w \mid 0 \leq w \ \wedge \ w \text{ even}\} \\ g(x) & \equiv & x \in \{w \mid w \text{ even}\} \\ g(x) & \equiv & x \in \{w \mid (0 \leq w \ \wedge \ w \text{ even}) \ \vee \ w \text{ odd}\} \\ g(x) & \equiv & x \in \{w \mid \mathit{true}\} \end{array}$$

The first of these is the least solution and the last is the greatest solution.

In the literature, the definition of an extreme predicate is often given as a set of *inference rules*. To designate the least solution, a single line separating the antecedent (on top) from conclusion (on bottom) is used:

Equation {#g-ind-rule} $\frac{}{g(0)}$ $\qquad$ $\frac{g(x-2)}{g(x)}$

Through repeated applications of such rules, one can show that the predicate holds for a particular value. For example, the *derivation*, or *proof tree*, to the left in Figure [#fig-proof-trees] shows that $g(6)$ holds. (In this simple example, the derivation is a rather degenerate proof "tree".) The use of these inference rules gives rise to a least solution, because proof trees are accepted only if they are *finite*.

When inference rules are to designate the greatest solution, a thick line is used:

~ Equation {#g-coind-rule} $\dfrac{}{g(0)}$ $\qquad$ $\dfrac{g(x-2)}{g(x)}$

In this case, proof trees are allowed to be infinite. For example, the left-hand example below shows a finite proof tree that uses the rules of [#g-ind-rule] to establish $g(6)$. On the right is a partial depiction of an infinite proof tree that uses the rules of [#g-coind-rule] to establish $g(1)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{g(0)}}{g(2)}}{g(4)}}{g(6)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\vdots}{g(-5)}}{g(-3)}}{g(-1)}}{g(1)}$$

Note that derivations may not be unique. For example, in the case of the greatest solution for g, there are two proof trees that establish $g(0)$: one is the

finite proof tree that uses the left-hand rule of [#g-coind-rule] once, the other is the infinite proof tree that keeps on using the right-hand rule of [#g-coind-rule].

12.1.3 Working with Extreme Predicates

In general, one cannot evaluate whether or not an extreme predicate holds for some input, because doing so may take an infinite number of steps. For example, following the recursive calls in the definition [#eq-EvenNat] to try to evaluate $g(7)$ would never terminate. However, there are useful ways to establish that an extreme predicate holds and there are ways to make use of one once it has been established.

For any $\mathcal{F}$ as in [#eq-general], I define two infinite series of well-founded functions, ${}^\flat f_k$ and ${}^\sharp f_k$ where k ranges over the natural numbers:

~ Equation {#eq-least-approx}

$$ {}^\flat f_k(x) = \left\{ \begin{array}{ll} \mathit{false} & \text{if } k = 0 \\ \mathcal{F}({}^\flat f_{k-1})(x) & \text{if } k > 0 \end{array} \right\} $$

.

~ Equation {#eq-greatest-approx}

$$ {}^\sharp f_k(x) = \left\{ \begin{array}{ll} \mathit{true} & \text{if } k = 0 \\ \mathcal{F}({}^\sharp f_{k-1})(x) & \text{if } k > 0 \end{array} \right\} $$

.
~

These functions are called the *iterates* of f, and I will also refer to them as the *prefix predicates* of f (or the *prefix predicate* of f, if we think of k as being a parameter). Alternatively, we can define ${}^\flat f_k$ and ${}^\sharp f_k$ without mentioning x: Let $\bot$ denote the function that always returns `false`, let $\top$ denote the function that always returns `true`, and let a superscript on $\mathcal{F}$ denote exponentiation (for example, $\mathcal{F}^0(f) = f$ and $\mathcal{F}^2(f) = \mathcal{F}(\mathcal{F}(f))$). Then, [#eq-least-approx] and [#eq-greatest-approx] can be stated equivalently as ${}^\flat f_k = \mathcal{F}^k(\bot)$ and ${}^\sharp f_k = \mathcal{F}^k(\top)$.

For any solution f to equation [#eq-general], we have, for any k and ℓ such that $k \leq \ell$:

Equation {#eq-prefix-postfix}

$$ {}^\flat f_k \quad \dot{\Rightarrow} \quad {}^\flat f_\ell \quad \dot{\Rightarrow} \quad f \quad \dot{\Rightarrow} \quad {}^\sharp f_\ell \quad \dot{\Rightarrow} \quad {}^\sharp f_k $$

In other words, every ${}^\flat f_k$ is a *pre-fixpoint* of f and every ${}^\sharp f_k$ is a *post-fixpoint* of f. Next, I define two functions, $f^\downarrow$ and $f^\uparrow$, in terms of the prefix predicates:

Equation {#eq-least-is-exists}

$$f^{\downarrow}(x) \;=\; \exists k \bullet {}^{\flat}f_k(x)$$

Equation {#eq-greatest-is-forall}

$$f^{\uparrow}(x) \;=\; \forall k \bullet {}^{\sharp}f_k(x)$$

By [#eq-prefix-postfix], we also have that $f^{\downarrow}$ is a pre-fixpoint of $\mathcal{F}$ and $f^{\uparrow}$ is a post-fixpoint of $\mathcal{F}$. The marvelous thing is that, if $\mathcal{F}$ is *continuous*, then $f^{\downarrow}$ and $f^{\uparrow}$ are the least and greatest fixpoints of $\mathcal{F}$. These equations let us do proofs by induction when dealing with extreme predicates. I will explain in Section [#sec-friendliness] how to check for continuity.

Let's consider two examples, both involving function g in [#eq-EvenNat]. As it turns out, g's defining functor is continuous, and therefore I will write $g^{\downarrow}$ and $g^{\uparrow}$ to denote the least and greatest solutions for g in [#eq-EvenNat].

12.1.3.1 Example with Least Solution The main technique for establishing that $g^{\downarrow}(x)$ holds for some x, that is, proving something of the form $Q \implies g^{\downarrow}(x)$, is to construct a proof tree like the one for $g(6)$ in Figure [#fig-proof-trees]. For a proof in this direction, since we're just applying the defining equation, the fact that we're using a least solution for g never plays a role (as long as we limit ourselves to finite derivations).

The technique for going in the other direction, proving something *from* an established $g^{\downarrow}$ property, that is, showing something of the form $g^{\downarrow}(x) \implies R$, typically uses induction on the structure of the proof tree. When the antecedent of our proof obligation includes a predicate term $g^{\downarrow}(x)$, it is sound to imagine that we have been given a proof tree for $g^{\downarrow}(x)$. Such a proof tree would be a data structure—to be more precise, a term in an *inductive datatype*. For this reason, least solutions like $g^{\downarrow}$ have been given the name *inductive predicate*.

Let's prove $g^{\downarrow}(x) \implies 0 \le x \;\wedge\; x$ even. We split our task into two cases, corresponding to which of the two proof rules in [#g-ind-rule] was the last one applied to establish $g^{\downarrow}(x)$. If it was the left-hand rule, then $x = 0$, which makes it easy to establish the conclusion of our proof goal. If it was the right-hand rule, then we unfold the proof tree one level and obtain $g^{\downarrow}(x-2)$. Since the proof tree for $g^{\downarrow}(x-2)$ is smaller than where we started, we invoke the *induction hypothesis* and obtain $0 \le (x-2) \;\wedge\; (x-2)$ even, from which it is easy to establish the conclusion of our proof goal.

Here's how we do the proof formally using [#eq-least-is-exists]. We massage the general form of our proof goal:

```
  | f↑(x) ⟹ R |
= |      { [#eq-least-is-exists] } |
  | (
```

$exists k \bullet {}^\flat f_k(x)) \implies R \mid$
$= \mid \quad \{$ distribute $\implies$ over $\exists$ to the left $\} \mid$
$\mid \forall k \bullet ({}^\flat f_k(x) \implies R) \mid$

The last line can be proved by induction over k. So, in our case, we prove ${}^\flat g\_k(x) \implies 0 \le x \wedge x$ even for every k. If $k = 0$, then ${}^\flat g\_k(x)$ is `false`, so our goal holds trivially. If $k > 0$, then ${}^\flat g\_k(x) = (x = 0 \vee {}^\flat g\_k - 1(x - 2))$. Our goal holds easily for the first disjunct ($x = 0$). For the other disjunct, we apply the induction hypothesis (on the smaller $k-1$ and with $x-2$) and obtain $0 \le (x-2) \wedge (x-2)$ even, from which our proof goal follows.

12.1.3.2 Example with Greatest Solution We can think of a given predicate $g^\uparrow(x)$ as being represented by a proof tree—in this case a term in a *coinductive datatype*, since the proof may be infinite. For this reason, greatest solutions like $g^\uparrow$ have been given the name *coinductive predicate*, or *co-predicate* for short. The main technique for proving something from a given proof tree, that is, to prove something of the form $g^\uparrow(x) \implies R$, is to destruct the proof. Since this is just unfolding the defining equation, the fact that we're using a greatest solution for g never plays a role (as long as we limit ourselves to a finite number of unfoldings).

To go in the other direction, to establish a predicate defined as a greatest solution, like $Q \implies g^\uparrow(x)$, we may need an infinite number of steps. For this purpose, we can use induction's dual, *coinduction*. Were it not for one little detail, coinduction is as simple as continuations in programming: the next part of the proof obligation is delegated to the *coinduction hypothesis*. The little detail is making sure that it is the "next" part we're passing on for the continuation, not the same part. This detail is called *productivity* and corresponds to the requirement in induction of making sure we're going down a well-founded relation when applying the induction hypothesis. There are many sources with more information, see for example the classic account by Jacobs and Rutten [@JacobsRutten:IntroductionCoalgebra] or a new attempt by Kozen and Silva that aims to emphasize the simplicity, not the mystery, of coinduction [@Kozen-Silva:Coinduction].

Let's prove $true \implies g^\uparrow(x)$. The intuitive coinductive proof goes like this: According to the right-hand rule of [#g-coind-rule], $g^\uparrow(x)$ follows if we establish $g^\uparrow(x-2)$, and that's easy to do by invoking the coinduction hypothesis. The "little detail", productivity, is satisfied in this proof because we applied a rule in [#g-coind-rule] before invoking the coinduction hypothesis.

For anyone who may have felt that the intuitive proof felt too easy, here is a formal proof using [#eq-greatest-is-forall], which relies only on induction. We massage the general form of our proof goal:

The last line can be proved by induction over k. So, in our case, we prove

12.1.4 Other Techniques

Although in this paper I consider only well-founded functions and extreme predicates, it is worth mentioning that there are additional ways of making sure that the set of solutions to [#eq-general] is nonempty. For example, if all calls to f in $\mathcal{F}'(f)$ are *tail-recursive calls*, then (under the assumption that Y is nonempty) the set of solutions is nonempty. To see this, consider an attempted evaluation of $f(x)$ that fails to determine a definite result value because of an infinite chain of calls that applies f to each value of some subset X' of X. Then, apparently, the value of f for any one of the values in X' is not determined by the equation, but picking any particular result values for these makes for a consistent definition. This was pointed out by Manolios and Moore [@ManoliosMoore:PartialFunctions]. Functions can be underspecified in this way in the proof assistants ACL2 [@ACL2:book] and HOL [@Krauss:PhD].

12.2 Functions in Dafny

In this section, I explain with examples the support in Dafny[6] for well-founded functions, extreme predicates, and proofs regarding these.

12.2.1 Well-founded Functions in Dafny

Declarations of well-founded functions are unsurprising. For example, the Fibonacci function is declared as follows:

```
function fib(n: nat): nat
{
  if n < 2 then n else fib(n-2) + fib(n-1)
}
```

Dafny verifies that the body (given as an expression in curly braces) is well defined. This includes decrement checks for recursive (and mutually recursive) calls. Dafny predefines a well-founded relation on each type and extends it to lexicographic tuples of any (fixed) length. For example, the well-founded relation $x \ll y$ for integers is $x < y \ \wedge \ 0 \leq y$, the one for reals is $x \leq y - 1.0 \ \wedge \ 0.0 \leq y$ (this is the same ordering as for integers, if you read the integer relation as $x \leq y - 1 \ \wedge \ 0 \leq y$), the one for inductive datatypes is structural inclusion, and the one for coinductive datatypes is `false`.

Using a `decreases` clause, the programmer can specify the term in this predefined order. When a function definition omits a `decreases` clause, Dafny makes a simple guess. This guess (which can be inspected by hovering over the function name in the Dafny IDE) is very often correct, so users are rarely bothered to provide explicit `decreases` clauses.

[6] Dafny is open source at dafny.codeplex.com and can also be used online at rise4fun.com/dafny.

If a function returns `bool`, one can drop the result type `: bool` and change the keyword `function` to `predicate`.

12.2.2 Proofs in Dafny

Dafny has `lemma` declarations. These are really just special cases of methods: they can have pre- and postcondition specifications and their body is a code block. Here is the lemma we stated and proved in Section [#sec-fib-example]:

```
lemma FibProperty(n: nat)
  ensures fib(n) % 2 == 0 <==> n % 3 == 0
{
  if n < 2 {
  } else {
    FibProperty(n-2); FibProperty(n-1);
  }
}
```

The postcondition of this lemma (keyword `ensures`) gives the proof goal. As in any program-correctness logic (e.g., [@Hoare:AxiomaticBasis]), the postcondition must be established on every control path through the lemma's body. For `FibProperty`, I give the proof by an `if` statement, hence introducing a case split. The then branch is empty, because Dafny can prove the postcondition automatically in this case. The else branch performs two recursive calls to the lemma. These are the invocations of the induction hypothesis and they follow the usual program-correctness rules, namely: the precondition must hold at the call site, the call must terminate, and then the caller gets to assume the postcondition upon return. The "proof glue" needed to complete the proof is done automatically by Dafny.

Dafny features an aggregate statement using which it is possible to make (possibly infinitely) many calls at once. For example, the induction hypothesis can be called at once on all values `n'` smaller than `n`:

```
forall n' | 0 <= n' < n {
  FibProperty(n');
}
```

For our purposes, this corresponds to *strong induction*. More generally, the `forall` statement has the form

```
forall k | P(k)
  ensures Q(k)
{ Statements; }
```

Logically, this statement corresponds to *universal introduction*: the body proves that `Q(k)` holds for an arbitrary `k` such that `P(k)`, and the conclusion of the `forall` statement is then $\forall k \bullet P(k) \implies Q(k)$. When the body of the `forall` statement is a single call (or `calc` statement), the `ensures` clause is inferred

and can be omitted, like in our `FibProperty` example.

Lemma `FibProperty` is simple enough that its whole body can be replaced by the one `forall` statement above. In fact, Dafny goes one step further: it automatically inserts such a `forall` statement at the beginning of every lemma [@Leino:induction]. Thus, `FibProperty` can be declared and proved simply by:

```
lemma FibProperty(n: nat)
  ensures fib(n) % 2 == 0 <==> n % 3 == 0
{ }
```

Going in the other direction from universal introduction is existential elimination, also known as Skolemization. Dafny has a statement for this, too: for any variable `x` and boolean expression `Q`, the *assign such that* statement `x :| Q;` says to assign to `x` a value such that `Q` will hold. A proof obligation when using this statement is to show that there exists an `x` such that `Q` holds. For example, if the fact
$existsk\bullet\ 100 \leq fib(k) < 200$ is known, then the statement `k :| 100 <= fib(k) < 200;` will assign to `k` some value (chosen arbitrarily) for which `fib(k)` falls in the given range.

12.2.3 Extreme Predicates in Dafny

In this previous subsection, I explained that a `predicate` declaration introduces a well-founded predicate. The declarations for introducing extreme predicates are `inductive predicate` and `copredicate`. Here is the definition of the least and greatest solutions of g from above, let's call them `g` and `G`:

```
inductive predicate g(x: int) { x == 0 || g(x-2) }
copredicate G(x: int) { x == 0 || G(x-2) }
```

When Dafny receives either of these definitions, it automatically declares the corresponding prefix predicates. Instead of the names ${}^{\flat}g_k$ and ${}^{\sharp}g_k$ that I used above, Dafny names the prefix predicates `g#[k]` and `G#[k]`, respectively, that is, the name of the extreme predicate appended with `#`, and the subscript is given as an argument in square brackets. The definition of the prefix predicate derives from the body of the extreme predicate and follows the form in [#eq-least-approx] and [#eq-greatest-approx]. Using a faux-syntax for illustrative purposes, here are the prefix predicates that Dafny defines automatically from the extreme predicates `g` and `G`:

```
predicate g#[_k: nat](x: int) { _k != 0 && (x == 0 || g#[_k-1](x-2)) }
predicate G#[_k: nat](x: int) { _k != 0 ==> (x == 0 || G#[_k-1](x-2)) }
```

The Dafny verifier is aware of the connection between extreme predicates and their prefix predicates, [#eq-least-is-exists] and [#eq-greatest-is-forall].

Remember that to be well defined, the defining functor of an extreme predicate must be monotonic, and for [#eq-least-is-exists] and [#eq-greatest-is-forall] to

hold, the functor must be continuous. Dafny enforces the former of these by checking that recursive calls of extreme predicates are in positive positions. The continuity requirement comes down to checking that they are also in *continuous positions*: that recursive calls to inductive predicates are not inside unbounded universal quantifiers and that recursive calls to co-predicates are not inside unbounded existential quantifiers [@Milner:CCS; @LeinoMoskal:Coinduction].

12.2.4 Proofs about Extreme Predicates

From what I have presented so far, we can do the formal proofs from Sections [#sec-example-least-solution] and [#sec-example-greatest-solution]. Here is the former:

```
lemma EvenNat(x: int)
  requires g(x)
  ensures 0 <= x && x % 2 == 0
{
  var k: nat :| g#[k](x);
  EvenNatAux(k, x);
}
lemma EvenNatAux(k: nat, x: int)
  requires g#[k](x)
  ensures 0 <= x && x % 2 == 0
{
  if x == 0 { } else { EvenNatAux(k-1, x-2); }
}
```

Lemma `EvenNat` states the property we wish to prove. From its precondition (keyword `requires`) and [#eq-least-is-exists], we know there is some `k` that will make the condition in the assign-such-that statement true. Such a value is then assigned to `k` and passed to the auxiliary lemma, which promises to establish the proof goal. Given the condition `g#[k](x)`, the definition of `g#` lets us conclude `k != 0` as well as the disjunction `x == 0 || g#[k-1](x-2)`. The then branch considers the case of the first disjunct, from which the proof goal follows automatically. The else branch can then assume `g#[k-1](x-2)` and calls the induction hypothesis with those parameters. The proof glue that shows the proof goal for `x` to follow from the proof goal with `x-2` is done automatically.

Because Dafny automatically inserts the statement

```
forall k', x' | 0 <= k' < k && g#[k'](x') {
  EvenNatAux(k', x');
}
```

at the beginning of the body of `EvenNatAux`, the body can be left empty and Dafny completes the proof automatically.

Here is the Dafny program that gives the proof from Section [#sec-example-greatest-solution]:

```
lemma Always(x: int)
  ensures G(x)
{ forall k: nat { AlwaysAux(k, x); } }
lemma AlwaysAux(k: nat, x: int)
  ensures G#[k](x)
{ }
```

While each of these proofs involves only basic proof rules, the setup feels a bit clumsy, even with the empty body of the auxiliary lemmas. Moreover, the proofs do not reflect the intuitive proofs I described in Section [#sec-example-least-solution] and [#sec-example-greatest-solution]. These shortcoming are addressed in the next subsection.

12.2.5 Nicer Proofs of Extreme Predicates

The proofs we just saw follow standard forms: use Skolemization to convert the inductive predicate into a prefix predicate for some `k` and then do the proof inductively over `k`; respectively, by induction over `k`, prove the prefix predicate for every `k`, then use universal introduction to convert to the coinductive predicate. With the declarations `inductive lemma` and `colemma`, Dafny offers to set up the proofs in these standard forms. What is gained is not just fewer characters in the program text, but also a possible intuitive reading of the proofs. (Okay, to be fair, the reading is intuitive for simpler proofs; complicated proofs may or may not be intuitive.)

Somewhat analogous to the creation of prefix predicates from extreme predicates, Dafny automatically creates a *prefix lemma* `L#` from each "extreme lemma" `L`. The pre- and postconditions of a prefix lemma are copied from those of the extreme lemma, except for the following replacements: For an inductive lemma, Dafny looks in the precondition to find calls (in positive, continuous positions) to inductive predicates `P(x)` and replaces these with `P#[_k](x)`. For a co-lemma, Dafny looks in the postcondition to find calls (in positive, continuous positions) to co-predicates `P` (including equality among coinductive datatypes, which is a built-in co-predicate) and replaces these with `P#[_k](x)`. In each case, these predicates `P` are the lemma's *focal predicates*.

The body of the extreme lemma is moved to the prefix lemma, but with replacing each recursive call `L(x)` with `L#[_k-1](x)` and replacing each occurrence of a call to a focal predicate `P(x)` with `P#[_k-1](x)`. The bodies of the extreme lemmas are then replaced as shown in the previous subsection. By construction, this new body correctly leads to the extreme lemma's postcondition.

Let us see what effect these rewrites have on how one can write proofs. Here are the proofs of our running example:

```
inductive lemma EvenNat(x: int)
  requires g(x)
  ensures 0 <= x && x % 2 == 0
```

```
{ if x == 0 { } else { EvenNat(x-2); } }
colemma Always(x: int)
  ensures G(x)
{ Always(x-2); }
```

Both of these proofs follow the intuitive proofs given in Sections [#sec-example-least-solution] and [#sec-example-greatest-solution]. Note that in these simple examples, the user is never bothered with either prefix predicates nor prefix lemmas—the proofs just look like "what you'd expect".

Since Dafny automatically inserts calls to the induction hypothesis at the beginning of each lemma, the bodies of the given extreme lemmas `EvenNat` and `Always` can be empty and Dafny still completes the proofs. Folks, it doesn't get any simpler than that!

13 Class Types

```
ClassDecl = "class" { Attribute } ClassName [ GenericParameters ]
  ["extends" Type {"," Type} ]
  "{" { { DeclModifier } ClassMemberDecl(moduleLevelDecl: false) } "}"
```

```
ClassMemberDecl(moduleLevelDecl) =
  ( FieldDecl | FunctionDecl |
    MethodDecl(isGhost: ("ghost" was present),
               allowConstructor: !moduleLevelDecl)
  )
```

The `ClassMemberDecl` parameter `moduleLevelDecl` will be true if the member declaration is at the top level or directly within a module declaration. It will be false for `ClassMemberDecl`s that are part of a class or trait declaration. If `moduleLevelDecl` is false `FieldDecl`s are not allowed.

A *class* `C` is a reference type declared as follows:

```
class C<T> extends J1, ..., Jn
{
  \(_members_\)
}
```

where the list of type parameters `T` is optional and so is "`extends J1, ..., Jn`", which says that the class extends traits `J1` … `Jn`. The members of a class are *fields*, *functions*, and *methods*. These are accessed or invoked by dereferencing a reference to a `C` instance.

A function or method is invoked on an *instance* of `C`, unless the function or method is declared `static`. A function or method that is not `static` is called an *instance* function or method.

An instance function or method takes an implicit *receiver* parameter, namely, the instance used to access the member. In the specification and body of an instance function or method, the receiver parameter can be referred to explicitly by the keyword `this`. However, in such places, members of `this` can also be mentioned without any qualification. To illustrate, the qualified `this.f` and the unqualified `f` refer to the same field of the same object in the following example:

```
class C {
  var f: int
  method Example() returns (b: bool)
  {
    b := f == this.f;
  }
}
```

so the method body always assigns `true` to the out-parameter `b`. There is no semantic difference between qualified and unqualified accesses to the same receiver and member.

A `C` instance is created using `new`, for example:

```
c := new C;
```

Note that `new` simply allocates a `C` object and returns a reference to it; the initial values of its fields are arbitrary values of their respective types. Therefore, it is common to invoke a method, known as an *initialization method*, immediately after creation, for example:

```
c := new C;
c.InitFromList(xs, 3);
```

When an initialization method has no out-parameters and modifies no more than `this`, then the two statements above can be combined into one:

```
c := new C.InitFromList(xs, 3);
```

Note that a class can contain several initialization methods, that these methods can be invoked at any time, not just as part of a `new`, and that `new` does not require that an initialization method be invoked at creation.

A clas can declare special initializing methods called *constructor methods*. See Section [#sec-method-declarations].

13.1 Field Declarations

```
FieldDecl = "var" { Attribute } FIdentType { "," FIdentType }
```

An `FIdentType` is used to declare a field. The field name is either an identifier (that is not allowed to start with a leading underscore) or some digits. Digits are used if you want to number your fields, e.g. “0”, “1”, etc.

```
FIdentType = ( FieldIdent | digits ) ":" Type
```

A field x of some type T is declared as:

```
var x: T
```

A field declaration declares one or more fields of the enclosing class. Each field is a named part of the state of an object of that class. A field declaration is similar to but distinct from a variable declaration statement. Unlike for local variables and bound variables, the type is required and will not be inferred.

Unlike method and function declarations, a field declaration cannot be given at the top level. Fields can be declared in either a class or a trait. A class that inherits from multiple traits will have all the fields declared in any of its parent traits.

Fields that are declared as `ghost` can only be used in specifications, not in code that will be compiled into executable code.

Fields may not be declared static.

`protected` is not allowed for fields.

13.2 Method Declarations

```
MethodDecl(isGhost, allowConstructor) =
 MethodKeyword { Attribute } [ MethodName ]
 (  MethodSignature(isGhost)  | SignatureEllipsis_ )
 MethodSpec [ BlockStmt ]
```

The `isGhost` parameter is true iff the `ghost` keyword preceded the method declaration.

If the `allowConstructor` parameter is false then the `MethodDecl` must not be a `constructor` declaration.

```
MethodKeyword = ("method" | "lemma" | "colemma"
                | "inductive" "lemma" | "constructor" )
```

The method keyword is used to specify special kinds of methods as explained below.

```
MethodSignature(isGhost) =
    [ GenericParameters ]
    Formals(allowGhost: !isGhost)
    [ "returns" Formals(allowGhost: !isGhost) ]
```

A method signature specifies the method generic parameters, input parameters and return parameters. The formal parameters are not allowed to have `ghost`

specified if `ghost` was already specified for the method.

```
SignatureEllipsis_ = "..."
```

A `SignatureEllipsis_` is used when a method or function is being redeclared in module that refines another module. In that case the signature is copied from the module that is being refined. This works because Dafny does not support method or function overloading, so the name of the class method uniquely identifies it without the signature.

```
Formals(allowGhostKeyword) =
  "(" [ GIdentType(allowGhostKeyword)
        { "," GIdentType(allowGhostKeyword) } ] ")"
```

The `Formals` specifies the names and types of the method input or output parameters.

See section [#sec-method-specification] for a description of `MethodSpec`.

A method declaration adheres to the `MethodDecl` grammar above. Here is an example of a method declaration.

```
method {:att1}{:att2} M<T1, T2>(a: A, b: B, c: C) returns (x: X, y: Y, z: Z)
  requires Pre
  modifies Frame
  ensures Post
  decreases Rank
{
  Body
}
```

where `:att1` and `:att2` are attributes of the method, `T1` and `T2` are type parameters of the method (if generic), `a, b, c` are the method's in-parameters, `x, y, z` are the method's out-parameters, `Pre` is a boolean expression denoting the method's precondition, `Frame` denotes a set of objects whose fields may be updated by the method, `Post` is a boolean expression denoting the method's postcondition, `Rank` is the method's variant function, and `Body` is a statement that implements the method. `Frame` can be a list of expressions, each of which is a set of objects or a single object, the latter standing for the singleton set consisting of that one object. The method's frame is the union of these sets, plus the set of objects allocated by the method body. For example, if `c` and `d` are parameters of a class type `C`, then

```
modifies {c, d}

modifies {c} + {d}

modifies c, {d}
```

```
modifies c, d
```

all mean the same thing.

A method can be declared as ghost by preceding the declaration with the keyword ghost. By default, a method has an implicit receiver parameter, this. This parameter can be removed by preceding the method declaration with the keyword static. A static method M in a class C can be invoked by C.M(…).

In a class, a method can be declared to be a constructor method by replacing the keyword `method` with the keyword `constructor`. A constructor can only be called at the time an object is allocated (see object-creation examples below), and for a class that contains one or more constructors, object creation must be done in conjunction with a call to a constructor.

An ordinary method is declared with the `method` keyword. Section [#sec-constructors] explains methods that instead use the `constructor` keyword. Section [#sec-lemmas] discusses methods that are declared with the `lemma` keyword. Methods declared with the `inductive lemma` keywords are discussed later in the context of inductive predicates (see [#sec-inductive-datatypes]). Methods declared with the `colemma` keyword are discussed later in the context of co-inductive types, in section [#sec-colemmas].

A method without a body is *abstract*. A method is allowed to be abstract under the following circumstances:

- It contains an `{:axiom}` attribute
- It contains an `{:imported}` attribute
- It contains a `{:decl}` attribute
- It is a declaration in an abstract module. Note that when there is no body, Dafny assumes that the *ensures* clauses are true without proof.

13.2.1 Constructors

To write structured object-oriented programs, one often relies on objects being constructed only in certain ways. For this purpose, Dafny provides *constructor (method)s*, which are a restricted form of initialization methods. A constructor is declared with the keyword `constructor` instead of `method`.
When a class contains a constructor, every call to `new` for a class must be accompanied by a call to one of its constructors. Moreover, a constructor cannot be called at other times, only during object creation. Other than these restrictions, there is no semantic difference between using ordinary initialization methods and using constructors. Classes may declare no constructors or one or more constructors.

13.2.1.1 Classes with no explicit constructors A class that declares no constructors has a default constructor created for it. This constructor is called with the syntax

```
c := new C;
```

This constructor simply initializes the fields of the class. The declaration of a const field may include an initializer, that is, a right-hand side (RHS) that specifies the constant's value. The RHS of a const field may depend on other constant fields, but circular dependencies are not allowed.

This constructor sets each class field to an arbitrary value of the field's type if the field declaration has no initializer and to the value of the initializer expression if it does declare an initializer. For the purposes of proving Dafny programs correct, assigning an arbitrary initial value means that the program must be correct for any initial value. Compiled, executable versions of the program may use a specific initial value (for example, but not necessarily, a zero-equivalent value).

13.2.1.2 Classes with one or more constructors When one or more constructors are explicitly declared, they are named, which promotes using names like `InitFromList` above. Constructors must have distinct names, even if their signatures are different. Many classes have just one constructor or have a typical constructor. Therefore, Dafny allows one *anonymous constructor*, that is, a constructor whose name is essentially "". For example:

```
class Item {
  constructor I(xy: int) // ...
  constructor (x: int, y: int)
  // ...
}
```

The named constructor is invoked as

```
  i := new Item.I(42);
```

The anonymous constructor is invoked as

```
  m := new Item(45, 29);
```

dropping the "`.`".

13.2.1.3 Two-phase constructors The body of a constructor contains two sections, an initialization phase and a post-initialization phase, separated by a `new;` statement. If there is no `new;` statement, the entire body is the initialization phase. The initialization phase is intended to initialize field variables. In this phase, uses of the object reference `this` are restricted; a program may use `this`

- as the receiver on the LHS,
- as the entire RHS of an assignment to a field of `this`,
- and as a member of a set on the RHS that is being assigned to a field of `this`.

Furthermore, `const` fields may only be assigned to in an initialization phase (and may be assigned to more than once) of their enclosing class, and then only if they do not already have an initialization value in their declaration.

There are no restrictions on expressions or statements in the post-initialization phase.

13.2.2 Lemmas

Sometimes there are steps of logic required to prove a program correct, but they are too complex for Dafny to discover and use on its own. When this happens, we can often give Dafny assistance by providing a lemma. This is done by declaring a method with the `lemma` keyword. Lemmas are implicitly ghost methods and the `ghost` keyword cannot be applied to them.

For an example, see the `FibProperty` lemma in Section [#sec-proofs-in-dafny].

See the Dafny Lemmas tutorial for more examples and hints for using lemmas.

TO BE WRITTEN - two-state lemmas; unchanged predicate

13.3 Function Declarations

```
FunctionDecl =
  ( "function" [ "method" ] { Attribute }
    FunctionName
    FunctionSignatureOrEllipsis_(allowGhostKeyword: ("method" present))
  | "predicate" [ "method" ] { Attribute }
    PredicateName
    PredicateSignatureOrEllipsis_(allowGhostKeyword: ("method" present))
  | "inductive" "predicate" { Attribute }
    PredicateName
    PredicateSignatureOrEllipsis_(allowGhostKeyword: false)
  | "copredicate" { Attribute }
    CopredicateName
    PredicateSignatureOrEllipsis_(allowGhostKeyword: false)
  )
  FunctionSpec [ FunctionBody ]

FunctionSignatureOrEllipsis_(allowGhostKeyword) =
    FunctionSignature_ | SignatureEllipsis_
FunctionSignature_(allowGhostKeyword) =
    [ GenericParameters ] Formals(allowGhostKeyword) ":" Type

PredicateSignatureOrEllipsis_(allowGhostKeyword) =
    PredicateSignature_(allowGhostKeyword) | SignatureEllipsis_
PredicateSignature_(allowGhostKeyword) =
    [ GenericParameters ] Formals(allowGhostKeyword)

FunctionBody = "{" Expression(allowLemma: true, allowLambda: true) "}"
```

In the above productions, allowGhostKeyword is true if the optional "method" keyword was specified. This allows some of the formal parameters of a function method to be specified as ghost.

See section [#sec-function-specification] for a description of `FunctionSpec`.

A Dafny function is a pure mathematical function. It is allowed to read memory that was specified in its `reads` expression but is not allowed to have any side effects.

Here is an example function declaration:

```
function {:att1}{:att2} F<T1, T2>(a: A, b: B, c: C): T
  requires Pre
  reads Frame
  ensures Post
  decreases Rank
{
```

```
  Body
}
```

where `:att1` and `:att2` are attributes of the function, if any, `T1` and `T2` are type parameters of the function (if generic), `a, b, c` are the functions's parameters, `T` is the type of the function's result, `Pre` is a boolean expression denoting the function's precondition, `Frame` denotes a set of objects whose fields the function body may depend on, `Post` is a boolean expression denoting the function's postcondition, `Rank` is the function's variant function, and `Body` is an expression that defines the function return value. The precondition allows a function to be partial, that is, the precondition says when the function is defined (and Dafny will verify that every use of the function meets the precondition). The postcondition is usually not needed, since the body of the function gives the full definition. However, the postcondition can be a convenient place to declare properties of the function that may require an inductive proof to establish. For example:

```
function Factorial(n: int): int
  requires 0 <= n
  ensures 1 <= Factorial(n)
{
  if n == 0 then 1 else Factorial(n-1) * n
}
```

says that the result of Factorial is always positive, which Dafny verifies inductively from the function body. To refer to the function's result in the postcondition, use the function itself, as shown in the example.

By default, a function is *ghost*, and cannot be called from non-ghost code. To make it non-ghost, replace the keyword function with the two keywords "function method".

By default, a function has an implicit receiver parameter, `this`. This parameter can be removed by preceding the function declaration with the keyword `static`. A static function `F` in a class `C` can be invoked by `C.F(…)`. This can give a convenient way to declare a number of helper functions in a separate class.

As for methods, a `SignatureEllipsis_` is used when declaring a function in a module refinement. For example, if module `M0` declares function `F`, a module `M1` can be declared to refine `M0` and `M1` can then refine `F`. The refinement function, `M1.F` can have a `SignatureEllipsis_` which means to copy the signature form `M0.F`. A refinement function can furnish a body for a function (if `M0.F` does not provide one). It can also add **ensures** clauses. And if `F` is a predicate, it can add conjuncts to a previously given body.

13.3.1 Function Transparency

A function is said to be *transparent* in a location if the contents of the body of the function is visible at that point. A function is said to be *opaque* at a location if it is not transparent. However the `FunctionSpec` of a function is always available.

A function is usually transparent up to some unrolling level (up to 1, or maybe 2 or 3). If its arguments are all literals it is transparent all the way.

But the transparency of a function is affected by the following:

- whether the function was declared to be protected, and
- whether the function was given the `{:opaque}` attribute (as explained in Section [#sec-opaque]).

The following table summarizes where the function is transparent. The module referenced in the table is the module in which the function is defined.

Protected? | `{:opaque}`? | Transparent | Transparent | | Inside | Outside
| | Module | Module
:———-:|:———:|:———:|:———: N | N | Y | Y
Y | N | Y | N
N | Y | N | N

When `{:opaque}` is specified for function `g`, `g` is opaque, however the lemma `reveal_g` is available to give the semantics of `g` whether in the defining module or outside.

It currently is not allowed to have both `protected` and `{:opaque}` specified for a function.

13.3.2 Predicates

A function that returns a `bool` results is called a *predicate*. As an alternative syntax, a predicate can be declared by replacing the `function` keyword with the `predicate` keyword and omitting a declaration of the return type.

13.3.3 Inductive Predicates and Lemmas

See section [#sec-friendliness] for descriptions of inductive predicates and lemmas.

14 Trait Types

```
TraitDecl = "trait" { Attribute } TraitName [ GenericParameters ]
  "{" { { DeclModifier } ClassMemberDecl(moduleLevelDecl: false) } "}"
```

A *trait* is an "abstract superclass", or call it an "interface" or "mixin". Traits are new to Dafny and are likely to evolve for a while.

The declaration of a trait is much like that of a class:

```
trait J
{
  \(_members_\)
}
```

where `\(_members_\)` can include fields, functions, and methods, but no constructor methods. The functions and methods are allowed to be declared `static`.

A reference type `C` that extends a trait `J` is assignable to `J`, but not the other way around. The members of `J` are available as members of `C`. A member in `J` is not allowed to be redeclared in `C`, except if the member is a non-`static` function or method without a body in `J`. By doing so, type `C` can supply a stronger specification and a body for the member.

`new` is not allowed to be used with traits. Therefore, there is no object whose allocated type is a trait. But there can of course be objects of a class `C` that implements a trait `J`, and a reference to such a `C` object can be used as a value of type `J`.

As an example, the following trait represents movable geometric shapes:

```
trait Shape
{
  function method Width(): real
    reads this
  method Move(dx: real, dy: real)
    modifies this
  method MoveH(dx: real)
    modifies this
  {
    Move(dx, 0.0);
  }
}
```

Members `Width` and `Move` are *abstract* (that is, body less) and can be implemented differently by different classes that extend the trait. The implementation of method `MoveH` is given in the trait and thus gets used by all classes that extend `Shape`. Here are two classes that each extends `Shape`:

```
class UnitSquare extends Shape
{
  var x: real, y: real
  function method Width(): real {  // note the empty reads clause
    1.0
```

```
  }
  method Move(dx: real, dy: real)
    modifies this
  {
    x, y := x + dx, y + dy;
  }
}
class LowerRightTriangle extends Shape
{
  var xNW: real, yNW: real, xSE: real, ySE: real
  function method Width(): real
    reads this
  {
    xSE - xNW
  }
  method Move(dx: real, dy: real)
    modifies this
  {
    xNW, yNW, xSE, ySE := xNW + dx, yNW + dy, xSE + dx, ySE + dy;
  }
}
```

Note that the classes can declare additional members, that they supply implementations for the abstract members of the trait, that they repeat the member signatures, and that they are responsible for providing their own member specifications that both strengthen the corresponding specification in the trait and are satisfied by the provided body. Finally, here is some code that creates two class instances and uses them together as shapes:

```
var myShapes: seq<Shape>;
var A := new UnitSquare;
myShapes := [A];
var tri := new LowerRightTriangle;
// myShapes contains two Shape values, of different classes
myShapes := myShapes + [tri];
// move shape 1 to the right by the width of shape 0
myShapes[1].MoveH(myShapes[0].Width());
```

15 Array Types

```
ArrayType_ = arrayToken [ GenericInstantiation ]
```

Dafny supports mutable fixed-length *array types* of any positive dimension. Array types are reference types.

15.1 One-dimensional arrays

A one-dimensional array of `n` `T` elements is created as follows:

```
a := new T[n];
```

The initial values of the array elements are arbitrary values of type `T`. The length of an array is retrieved using the immutable `Length` member. For example, the array allocated above satisfies:

```
a.Length == n
```

For any integer-based numeric `i` in the range `0 <= i < a.Length`, the *array selection* expression `a[i]` retrieves element `i` (that is, the element preceded by `i` elements in the array). The element stored at `i` can be changed to a value `t` using the array update statement:

```
a[i] := t;
```

Caveat: The type of the array created by `new T[n]` is `array<T>`. A mistake that is simple to make and that can lead to befuddlement is to write `array<T>` instead of `T` after `new`. For example, consider the following:

```
var a := new array<T>;
var b := new array<T>[n];
var c := new array<T>(n);  // resolution error
var d := new array(n);  // resolution error
```

The first statement allocates an array of type `array<T>`, but of unknown length. The second allocates an array of type `array<array<T>>` of length `n`, that is, an array that holds `n` values of type `array<T>`. The third statement allocates an array of type `array<T>` and then attempts to invoke an anonymous constructor on this array, passing argument `n`. Since `array` has no constructors, let alone an anonymous constructor, this statement gives rise to an error. If the type-parameter list is omitted for a type that expects type parameters, Dafny will attempt to fill these in, so as long as the `array` type parameter can be inferred, it is okay to leave off the "`<T>`" in the fourth statement above. However, as with the third statement, `array` has no anonymous constructor, so an error message is generated.

One-dimensional arrays support operations that convert a stretch of consecutive elements into a sequence. For any array `a` of type `array<T>`, integer-based numerics `lo` and `hi` satisfying `0 <= lo <= hi <= a.Length`, the following operations each yields a `seq<T>`:

expression	description
`a[lo..hi]`	subarray conversion to sequence
`a[lo..]`	drop
`a[..hi]`	take

expression	description
`a[..]`	array conversion to sequence

The expression `a[lo..hi]` takes the first `hi` elements of the array, then drops the first `lo` elements thereof and returns what remains as a sequence. The resulting sequence thus has length `hi - lo`. The other operations are special instances of the first. If `lo` is omitted, it defaults to `0` and if `hi` is omitted, it defaults to `a.Length`. In the last operation, both `lo` and `hi` have been omitted, thus `a[..]` returns the sequence consisting of all the array elements of `a`.

The subarray operations are especially useful in specifications. For example, the loop invariant of a binary search algorithm that uses variables `lo` and `hi` to delimit the subarray where the search `key` may be still found can be expressed as follows:

```
key !in a[..lo] && key !in a[hi..]
```

Another use is to say that a certain range of array elements have not been changed since the beginning of a method:

```
a[lo..hi] == old(a[lo..hi])
```

or since the beginning of a loop:

```
ghost var prevElements := a[..];
while // ...
  invariant a[lo..hi] == prevElements[lo..hi]
{
  // ...
}
```

Note that the type of `prevElements` in this example is `seq<T>`, if `a` has type `array<T>`.

A final example of the subarray operation lies in expressing that an array's elements are a permutation of the array's elements at the beginning of a method, as would be done in most sorting algorithms. Here, the subarray operation is combined with the sequence-to-multiset conversion:

```
multiset(a[..]) == multiset(old(a[..]))
```

15.2 Multi-dimensional arrays

An array of 2 or more dimensions is mostly like a one-dimensional array, except that `new` takes more length arguments (one for each dimension), and the array selection expression and the array update statement take more indices. For example:

```
matrix := new T[m, n];
matrix[i, j], matrix[x, y] := matrix[x, y], matrix[i, j];
```

create a 2-dimensional array whose dimensions have lengths `m` and `n`, respectively, and then swaps the elements at `i,j` and `x,y`. The type of `matrix` is `array2<T>`, and similarly for higher-dimensional arrays (`array3<T>`, `array4<T>`, etc.). Note, however, that there is no type `array0<T>`, and what could have been `array1<T>` is actually named just `array<T>`.

The `new` operation above requires `m` and `n` to be non-negative integer-based numerics. These lengths can be retrieved using the immutable fields `Length0` and `Length1`. For example, the following holds of the array created above:

```
matrix.Length0 == m && matrix.Length1 == n
```

Higher-dimensional arrays are similar (`Length0`, `Length1`, `Length2`, …). The array selection expression and array update statement require that the indices are in bounds. For example, the swap statement above is well-formed only if:

```
0 <= i < matrix.Length0 && 0 <= j < matrix.Length1 &&
0 <= x < matrix.Length0 && 0 <= y < matrix.Length1
```

In contrast to one-dimensional arrays, there is no operation to convert stretches of elements from a multi-dimensional array to a sequence.

16 Type object

```
ObjectType_ = "object"
```

There is a built-in trait `object` that is like a supertype of all reference types.[7] Every class automatically extends object and so does every user-defined trait. The purpose of type `object` is to enable a uniform treatment of *dynamic frames*. In particular, it is useful to keep a ghost field (typically named `Repr` for "representation") of type `set<object>`.

[7] The current compiler restriction that `object` cannot be used as a type parameter needs to be removed.

17 Iterator types

```
IteratorDecl = "iterator" { Attribute } IteratorName
  ( [ GenericParameters ]
    Formals(allowGhostKeyword: true)
    [ "yields" Formals(allowGhostKeyword: true) ]
  | "..."
  )
  IteratorSpec [ BlockStmt ]
```

See section [#sec-iterator-specification] for a description of `IteratorSpec`.

An *iterator* provides a programming abstraction for writing code that iteratively returns elements. These CLU-style iterators are *co-routines* in the sense that they keep track of their own program counter and control can be transferred into and out of the iterator body.

An iterator is declared as follows:

```
iterator Iter<T>(\(_in-params_\)) yields (\(_yield-params_\))
  \(_specification_\)
{
  \(_body_\)
}
```

where `T` is a list of type parameters (as usual, if there are no type parameters, "`<T>`" is omitted). This declaration gives rise to a reference type with the same name, `Iter<T>`. In the signature, in-parameters and yield-parameters are the iterator's analog of a method's in-parameters and out-parameters. The difference is that the out-parameters of a method are returned to a caller just once, whereas the yield-parameters of an iterator are returned each time the iterator body performs a `yield`. The body consists of statements, like in a method body, but with the availability also of `yield` statements.

From the perspective of an iterator client, the `iterator` declaration can be understood as generating a class `Iter<T>` with various members, a simplified version of which is described next.

The `Iter<T>` class contains an anonymous constructor whose parameters are the iterator's in-parameters:

```
predicate Valid()
constructor (\(_in-params_\))
  modifies this
  ensures Valid()
```

An iterator is created using `new` and this anonymous constructor. For example, an iterator willing to return ten consecutive integers from `start` can be declared as follows:

```
iterator Gen(start: int) yields (x: int)
{
  var i := 0;
  while i < 10 {
    x := start + i;
    yield;
    i := i + 1;
  }
}
```

An instance of this iterator is created using:

```
iter := new Gen(30);
```

The predicate `Valid()` says when the iterator is in a state where one can attempt to compute more elements. It is a postcondition of the constructor and occurs in the specification of the `MoveNext` member:

```
method MoveNext() returns (more: bool)
  requires Valid()
  modifies this
  ensures more ==> Valid()
```

Note that the iterator remains valid as long as `MoveNext` returns `true`. Once `MoveNext` returns `false`, the `MoveNext` method can no longer be called. Note, the client is under no obligation to keep calling `MoveNext` until it returns `false`, and the body of the iterator is allowed to keep returning elements forever.

The in-parameters of the iterator are stored in immutable fields of the iterator class. To illustrate in terms of the example above, the iterator class `Gen` contains the following field:

```
var start: int
```

The yield-parameters also result in members of the iterator class:

```
var x: int
```

These fields are set by the `MoveNext` method. If `MoveNext` returns `true`, the latest yield values are available in these fields and the client can read them from there.

To aid in writing specifications, the iterator class also contains ghost members that keep the history of values returned by `MoveNext`. The names of these ghost fields follow the names of the yield-parameters with an "`s`" appended to the name (to suggest plural). Name checking rules make sure these names do not give rise to ambiguities. The iterator class for `Gen` above thus contains:

```
ghost var xs: seq<int>
```

These history fields are changed automatically by `MoveNext`, but are not

assignable by user code.

Finally, the iterator class contains some special fields for use in specifications. In particular, the iterator specification gets recorded in the following immutable fields:

```
ghost var _reads: set<object>
ghost var _modifies: set<object>
ghost var _decreases0: T0
ghost var _decreases1: T1
// ...
```

where there is a `_decreases\(_i_\): T\(_i_\)` field for each component of the iterator's `decreases` clause.[8] In addition, there is a field:

```
ghost var _new: set<object>;
```

to which any objects allocated on behalf of the iterator body get added. The iterator body is allowed to remove elements from the `_new` set, but cannot by assignment to `_new` add any elements.

Note, in the precondition of the iterator, which is to hold upon construction of the iterator, the in-parameters are indeed in-parameters, not fields of `this`.

It's regrettably tricky to use iterators. The language really ought to have a `foreach` statement to make this easier. Here is an example showing definition and use of an iterator.

```
iterator Iter<T>(s: set<T>) yields (x: T)
  yield ensures x in s && x !in xs[..|xs|-1];
  ensures s == set z | z in xs;
{
  var r := s;
  while (r != {})
    invariant forall z :: z in xs ==> x !in r;  // r and xs are disjoint
    invariant s == r + set z | z in xs;
  {
    var y :| y in r;
    r, x := r - {y}, y;
    yield;
    assert y == xs[|xs|-1];  // needed as a lemma to prove loop invariant
  }
}

method UseIterToCopy<T>(s: set<T>) returns (t: set<T>)
```

[8] It would make sense to rename the special fields `_reads` and `_modifies` to have the same names as the corresponding keywords, `reads` and `modifies`, as is done for function values. Also, the various `_decreases\(_i_\)` fields can combined into one field named `decreases` whose type is a n-tuple. Thse changes may be incorporated into a future version of Dafny.

```
  ensures s == t;
{
  t := {};
  var m := new Iter(s);
  while (true)
    invariant m.Valid() && fresh(m._new);
    invariant t == set z | z in m.xs;
    decreases s - t;
  {
    var more := m.MoveNext();
    if (!more) { break; }
    t := t + {m.x};
  }
}
```

18 Function types

```
Type = DomainType "->" Type
```

Functions are first-class values in Dafny. Function types have the form `(T) -> U` where `T` is a comma-delimited list of types and `U` is a type. `T` is called the function's *domain type(s)* and `U` is its *range type*. For example, the type of a function

```
function F(x: int, b: bool): real
```

is `(int, bool) -> real`. Parameters are not allowed to be ghost.

To simplify the appearance of the basic case where a function's domain consist of a list of exactly one type, the parentheses around the domain type can be dropped in this case, as in `T -> U`. This innocent simplification requires additional explanation in the case where that one type is a tuple type, since tuple types are also written with enclosing parentheses. If the function takes a single argument that is a tuple, an additional set of parentheses is needed. For example, the function

```
function G(pair: (int, bool)): real
```

has type `((int, bool)) -> real`. Note the necessary double parentheses. Similarly, a function that takes no arguments is different from one that takes a 0-tuple as an argument. For instance, the functions

```
function NoArgs(): real
function Z(unit: ()): real
```

have types `() -> real` and `(()) -> real`, respectively.

The function arrow, `->`, is right associative, so `A -> B -> C` means `A -> (B -> C)`. The other association requires explicit parentheses: `(A -> B) -> C`.

Note that the receiver parameter of a named function is not part of the type. Rather, it is used when looking up the function and can then be thought of as being captured into the function definition. For example, suppose function `F` above is declared in a class `C` and that `c` references an object of type `C`; then, the following is type correct:

```
var f: (int, bool) -> real := c.F;
```

whereas it would have been incorrect to have written something like:

```
var f': (C, int, bool) -> real := F;  // not correct
```

Outside its type signature, each function value has three properties, described next.

Every function implicitly takes the heap as an argument. No function ever depends on the *entire* heap, however. A property of the function is its declared upper bound on the set of heap locations it depends on for a given input. This lets the verifier figure out that certain heap modifications have no effect on the value returned by a certain function. For a function `f: T -> U` and a value `t` of type `T`, the dependency set is denoted `f.reads(t)` and has type `set<object>`.

The second property of functions stems from the fact that every function is potentially *partial*. In other words, a property of a function is its *precondition*. For a function `f: T -> U`, the precondition of `f` for a parameter value `t` of type `T` is denoted `f.requires(t)` and has type `bool`.

The third property of a function is more obvious—the function's body. For a function `f: T -> U`, the value that the function yields for an input `t` of type `T` is denoted `f(t)` and has type `U`.

Note that `f.reads` and `f.requires` are themselves functions. Suppose `f` has type `T -> U` and `t` has type `T`. Then, `f.reads` is a function of type `T -> set<object>` whose `reads` and `requires` properties are:

```
f.reads.reads(t) == f.reads(t)
f.reads.requires(t) == true
```

`f.requires` is a function of type `T -> bool` whose `reads` and `requires` properties are:

```
f.requires.reads(t) == f.reads(t)
f.requires.requires(t) == true
```

Dafny also support anonymous functions by means of *lambda expressions*. See section [#sec-lambda-expressions].

19 Algebraic Datatypes

Dafny offers two kinds of algebraic datatypes, those defined inductively and those defined co-inductively. The salient property of every datatype is that each value of the type uniquely identifies one of the datatype's constructors and each constructor is injective in its parameters.

```
DatatypeDecl = ( InductiveDatatypeDecl | CoinductiveDatatypeDecl )
```

19.1 Inductive datatypes

```
InductiveDatatypeDecl_ = "datatype" { Attribute } DatatypeName [ GenericParameters ]
  "=" [ "|" ] DatatypeMemberDecl { "|" DatatypeMemberDecl } [ ";" ]
DatatypeMemberDecl = { Attribute } DatatypeMemberName [ FormalsOptionalIds ]
```

The values of inductive datatypes can be seen as finite trees where the leaves are values of basic types, numeric types, reference types, co-inductive datatypes, or function types. Indeed, values of inductive datatypes can be compared using Dafny's well-founded $<$ ordering.

An inductive datatype is declared as follows:

```
datatype D<T> = \(_Ctors_\)
```

where `\(_Ctors_\)` is a nonempty `|`-separated list of *(datatype) constructors* for the datatype. Each constructor has the form:

```
C(\(_params_\))
```

where `\(_params_\)` is a comma-delimited list of types, optionally preceded by a name for the parameter and a colon, and optionally preceded by the keyword `ghost`. If a constructor has no parameters, the parentheses after the constructor name can be omitted. If no constructor takes a parameter, the type is usually called an *enumeration*; for example:

```
datatype Friends = Agnes | Agatha | Jermaine | Jack
```

For every constructor `C`, Dafny defines a *discriminator* `C?`, which is a member that returns `true` if and only if the datatype value has been constructed using `C`. For every named parameter `p` of a constructor `C`, Dafny defines a *destructor* `p`, which is a member that returns the `p` parameter from the `C` call used to construct the datatype value; its use requires that `C?` holds. For example, for the standard `List` type

```
datatype List<T> = Nil | Cons(head: T, tail: List<T>)
```

the following holds:

```
Cons(5, Nil).Cons? && Cons(5, Nil).head == 5
```

Note that the expression

```
Cons(5, Nil).tail.head
```

is not well-formed, since `Cons(5, Nil).tail` does not satisfy `Cons?`.

A constructor can have the same name as the enclosing datatype; this is especially useful for single-constructor datatypes, which are often called *record types*. For example, a record type for black-and-white pixels might be represented as follows:

```
datatype Pixel = Pixel(x: int, y: int, on: bool)
```

To call a constructor, it is usually necessary only to mention the name of the constructor, but if this is ambiguous, it is always possible to qualify the name of constructor by the name of the datatype. For example, `Cons(5, Nil)` above can be written

```
List.Cons(5, List.Nil)
```

As an alternative to calling a datatype constructor explicitly, a datatype value can be constructed as a change in one parameter from a given datatype value using the *datatype update* expression. For any `d` whose type is a datatype that includes a constructor `C` that has a parameter (destructor) named `f` of type `T`, and any expression `t` of type `T`,

```
d.(f := t)
```

constructs a value like `d` but whose `f` parameter is `t`. The operation requires that `d` satisfies `C?`. For example, the following equality holds:

```
Cons(4, Nil).(tail := Cons(3, Nil)) == Cons(4, Cons(3, Nil))
```

The datatype update expression also accepts multiple field names, provided these are distinct. For example, a node of some inductive datatype for trees may be updated as follows:

```
node.(left := L, right := R)
```

19.2 Tuple types

```
TupleType_ = "(" [ Type { "," Type } ] ")"
```

Dafny builds in record types that correspond to tuples and gives these a convenient special syntax, namely parentheses. For example, what might have been declared as:

```
datatype Pair<T,U> = Pair(0: T, 1: U)
```

Dafny provides as the type `(T, U)` and the constructor `(t, u)`, as if the datatype's name were "" and its type arguments are given in round parentheses, and as if the constructor name were "". Note that the destructor names are `0` and `1`, which are legal identifier names for members. For example, showing the use of a tuple destructor, here is a property that holds of 2-tuples (that is, *pairs*):

```
(5, true).1 == true
```

Dafny declares n-tuples where n is 0 or 2 or up. There are no 1-tuples, since parentheses around a single type or a single value have no semantic meaning. The 0-tuple type, `()`, is often known as the *unit type* and its single value, also written `()`, is known as *unit*.

19.3 Co-inductive datatypes

```
CoinductiveDatatypeDecl_ = "codatatype" { Attribute } DatatypeName [ GenericParameters ]
  "=" DatatypeMemberDecl { "|" DatatypeMemberDecl } [ ";" ]
```

Whereas Dafny insists that there is a way to construct every inductive datatype value from the ground up, Dafny also supports *co-inductive datatypes*, whose constructors are evaluated lazily and hence allows infinite structures. A co-inductive datatype is declared using the keyword `codatatype`; other than that, it is declared and used like an inductive datatype.

For example,

```
codatatype IList<T> = Nil | Cons(head: T, tail: IList<T>)
codatatype Stream<T> = More(head: T, tail: Stream<T>)
codatatype Tree<T> = Node(left: Tree<T>, value: T, right: Tree<T>)
```

declare possibly infinite lists (that is, lists that can be either finite or infinite), infinite streams (that is, lists that are always infinite), and infinite binary trees (that is, trees where every branch goes on forever), respectively.

The paper [Co-induction Simply], by Leino and Moskal[@LEINO:Dafny:Coinduction], explains Dafny's implementation and verification of co-inductive types. We capture the key features from that paper in this section but the reader is referred to that paper for more complete details and to supply bibliographic references that we have omitted.

Mathematical induction is a cornerstone of programming and program verification. It arises in data definitions (e.g., some algebraic data structures can be described using induction), it underlies program semantics (e.g., it explains how to reason about finite iteration and recursion), and it gets used in proofs (e.g., supporting lemmas about data structures use inductive proofs). Whereas

induction deals with finite things (data, behavior, etc.), its dual, co-induction, deals with possibly infinite things. Co-induction, too, is important in programming and program verification, where it arises in data definitions (e.g., lazy data structures), semantics (e.g., concurrency), and proofs (e.g., showing refinement in a co-inductive big-step semantics). It is thus desirable to have good support for both induction and co-induction in a system for constructing and reasoning about programs.

Co-datatypes and co-recursive functions make it possible to use lazily evaluated data structures (like in Haskell or Agda). Co-predicates, defined by greatest fix-points, let programs state properties of such data structures (as can also be done in, for example, Coq). For the purpose of writing co-inductive proofs in the language, we introduce co-lemmas. Ostensibly, a co-lemma invokes the co-induction hypothesis much like an inductive proof invokes the induction hypothesis. Underneath the hood, our co-inductive proofs are actually approached via induction: co-lemmas provide a syntactic veneer around this approach.

The following example gives a taste of how the co-inductive features in Dafny come together to give straightforward definitions of infinite matters.

```
// infinite streams
codatatype IStream<T> = ICons(head: T, tail: IStream)

// pointwise product of streams
function Mult(a: IStream<int>, b: IStream<int>): IStream<int>
{ ICons(a.head * b.head, Mult(a.tail, b.tail)) }

// lexicographic order on streams
copredicate Below(a: IStream<int>, b: IStream<int>)
{ a.head <= b.head && ((a.head == b.head) ==> Below(a.tail, b.tail)) }

// a stream is Below its Square
colemma Theorem_BelowSquare(a: IStream<int>)
ensures Below(a, Mult(a, a))
{ assert a.head <= Mult(a, a).head;
  if a.head == Mult(a, a).head {
    Theorem_BelowSquare(a.tail);
  }
}

// an incorrect property and a bogus proof attempt
colemma NotATheorem_SquareBelow(a: IStream<int>)
  ensures Below(Mult(a, a), a); // ERROR
{
  NotATheorem_SquareBelow(a);
}
```

It defines a type `IStream` of infinite streams, with constructor `ICons` and destructors `head` and `tail`. Function `Mult` performs pointwise multiplication on infinite streams of integers, defined using a co-recursive call (which is evaluated lazily). Co-predicate `Below` is defined as a greatest fix-point, which intuitively means that the co-predicate will take on the value true if the recursion goes on forever without determining a different value. The co-lemma states the theorem `Below(a, Mult(a, a))`. Its body gives the proof, where the recursive invocation of the co-lemma corresponds to an invocation of the co-induction hypothesis.

The proof of the theorem stated by the first co-lemma lends itself to the following intuitive reading: To prove that `a` is below `Mult(a, a)`, check that their heads are ordered and, if the heads are equal, also prove that the tails are ordered. The second co-lemma states a property that does not always hold; the verifier is not fooled by the bogus proof attempt and instead reports the property as unproved.

We argue that these definitions in Dafny are simple enough to level the playing field between induction (which is familiar) and co-induction (which, despite being the dual of induction, is often perceived as eerily mysterious). Moreover, the automation provided by our SMT-based verifier reduces the tedium in writing co-inductive proofs. For example, it verifies `Theorem_BelowSquare` from the program text given above— no additional lemmas or tactics are needed. In fact, as a consequence of the automatic-induction heuristic in Dafny, the verifier will automatically verify Theorem_BelowSquare even given an empty body.

Just like there are restrictions on when an *inductive hypothesis* can be invoked, there are restriction on how a *co-inductive* hypothesis can be *used*. These are, of course, taken into consideration by our verifier. For example, as illustrated by the second co-lemma above, invoking the co-inductive hypothesis in an attempt to obtain the entire proof goal is futile. (We explain how this works in section [#sec-colemmas]) Our initial experience with co-induction in Dafny shows it to provide an intuitive, low-overhead user experience that compares favorably to even the best of today's interactive proof assistants for co-induction. In addition, the co-inductive features and verification support in Dafny have other potential benefits. The features are a stepping stone for verifying functional lazy programs with Dafny. Co-inductive features have also shown to be useful in defining language semantics, as needed to verify the correctness of a compiler, so this opens the possibility that such verifications can benefit from SMT automation.

19.3.1 Well-Founded Function/Method Definitions

The Dafny programming language supports functions and methods. A *function* in Dafny is a mathematical function (i.e., it is well-defined, deterministic, and pure), whereas a *method* is a body of statements that can mutate the state of the program. A function is defined by its given body, which is an expression. To ensure that function definitions are mathematically consistent, Dafny insists

that recursive calls be well-founded, enforced as follows: Dafny computes the call graph of functions. The strongly connected components within it are *clusters* of mutually recursive definitions arranged in a DAG. This stratifies the functions so that a call from one cluster in the DAG to a lower cluster is allowed arbitrarily. For an intra-cluster call, Dafny prescribes a proof obligation that gets taken through the program verifier's reasoning engine. Semantically, each function activation is labeled by a *rank*—a lexicographic tuple determined by evaluating the function's **decreases** clause upon invocation of the function. The proof obligation for an intra-cluster call is thus that the rank of the callee is strictly less (in a language-defined well-founded relation) than the rank of the caller. Because these well-founded checks correspond to proving termination of executable code, we will often refer to them as "termination checks". The same process applies to methods.

Lemmas in Dafny are commonly introduced by declaring a method, stating the property of the lemma in the *postcondition* (keyword **ensures**) of the method, perhaps restricting the domain of the lemma by also giving a *precondition* (keyword **requires**), and using the lemma by invoking the method. Lemmas are stated, used, and proved as methods, but since they have no use at run time, such lemma methods are typically declared as *ghost*, meaning that they are not compiled into code. The keyword **lemma** introduces such a method. Control flow statements correspond to proof techniques—case splits are introduced with if statements, recursion and loops are used for induction, and method calls for structuring the proof. Additionally, the statement:

```
forall x | P(x) { Lemma(x); }
```

is used to invoke `Lemma(x)` on all `x` for which `P(x)` holds. If `Lemma(x)` ensures `Q(x)`, then the forall statement establishes

```
forall x :: P(x) ==> Q(x).
```

19.3.2 Defining Co-inductive Datatypes

Each value of an inductive datatype is finite, in the sense that it can be constructed by a finite number of calls to datatype constructors. In contrast, values of a co-inductive datatype, or co-datatype for short, can be infinite. For example, a co-datatype can be used to represent infinite trees.

Syntactically, the declaration of a co-datatype in Dafny looks like that of a datatype, giving prominence to the constructors (following Coq). The following example defines a co-datatype Stream of possibly infinite lists.

```
codatatype Stream<T> = SNil | SCons(head: T, tail: Stream)
function Up(n: int): Stream<int> { SCons(n, Up(n+1)) }
function FivesUp(n: int): Stream<int>
  decreases 4 - (n - 1) % 5
{
```

```
  if (n % 5 == 0) then
    SCons(n, FivesUp(n+1))
  else
    FivesUp(n+1)
}
```

`Stream` is a co-inductive datatype whose values are possibly infinite lists. Function `Up` returns a stream consisting of all integers upwards of `n` and `FivesUp` returns a stream consisting of all multiples of 5 upwards of `n` . The self-call in `Up` and the first self-call in `FivesUp` sit in productive positions and are therefore classified as co-recursive calls, exempt from termination checks. The second self-call in `FivesUp` is not in a productive position and is therefore subject to termination checking; in particular, each recursive call must decrease the rank defined by the **decreases** clause.

Analogous to the common finite list datatype, Stream declares two constructors, `SNil` and `SCons`. Values can be destructed using match expressions and statements. In addition, like for inductive datatypes, each constructor `C` automatically gives rise to a discriminator `C?` and each parameter of a constructor can be named in order to introduce a corresponding destructor. For example, if `xs` is the stream `SCons(x, ys)`, then `xs.SCons?` and `xs.head == x` hold. In contrast to datatype declarations, there is no grounding check for co-datatypes—since a codatatype admits infinite values, the type is nevertheless inhabited.

19.3.3 Creating Values of Co-datatypes

To define values of co-datatypes, one could imagine a "co-function" language feature: the body of a "co-function" could include possibly never-ending self-calls that are interpreted by a greatest fix-point semantics (akin to a **CoFixpoint** in Coq). Dafny uses a different design: it offers only functions (not "co-functions"), but it classifies each intra-cluster call as either *recursive* or *co-recursive*. Recursive calls are subject to termination checks. Co-recursive calls may be never-ending, which is what is needed to define infinite values of a co-datatype. For example, function `Up(n )` in the preceding example is defined as the stream of numbers from `n` upward: it returns a stream that starts with `n` and continues as the co-recursive call `Up(n + 1)`.

To ensure that co-recursive calls give rise to mathematically consistent definitions, they must occur only in productive positions. This says that it must be possible to determine each successive piece of a co-datatype value after a finite amount of work. This condition is satisfied if every co-recursive call is syntactically guarded by a constructor of a co-datatype, which is the criterion Dafny uses to classify intra-cluster calls as being either co-recursive or recursive. Calls that are classified as co-recursive are exempt from termination checks.

A consequence of the productivity checks and termination checks is that, even in the absence of talking about least or greatest fix-points of self-calling functions,

all functions in Dafny are deterministic. Since there is no issue of several possible fix-points, the language allows one function to be involved in both recursive and co-recursive calls, as we illustrate by the function `FivesUp`.

19.3.4 Copredicates

Determining properties of co-datatype values may require an infinite number of observations. To that avail, Dafny provides *co-predicates* which are function declarations that use the `copredicate` keyword. Self-calls to a co-predicate need not terminate. Instead, the value defined is the greatest fix-point of the given recurrence equations. Continuing the preceding example, the following code defines a co-predicate that holds for exactly those streams whose payload consists solely of positive integers. The co-predicate definition implicitly also gives rise to a corresponding prefix predicate, `Pos#`. The syntax for calling a prefix predicate sets apart the argument that specifies the prefix length, as shown in the last line; for this figure, we took the liberty of making up a coordinating syntax for the signature of the automatically generated prefix predicate (which is not part of Dafny syntax).

```
copredicate Pos(s: Stream<int>)
{
  match s
  case SNil => true
  case SCons(x, rest) => x > 0 && Pos(rest)
}
// Automatically generated by the Dafny compiler:
predicate Pos#[_k: nat](s: Stream<int>)
  decreases _k
{ if _k = 0 then true else
  match s
  case SNil => true
  case SCons(x, rest) => x > 0 && Pos#[_k-1](rest)
}
```

Some restrictions apply. To guarantee that the greatest fix-point always exists, the (implicit functor defining the) co-predicate must be monotonic. This is enforced by a syntactic restriction on the form of the body of co-predicates: after conversion to negation normal form (i.e., pushing negations down to the atoms), intra-cluster calls of co-predicates must appear only in *positive* positions—that is, they must appear as atoms and must not be negated. Additionally, to guarantee soundness later on, we require that they appear in *co-friendly* positions—that is, in negation normal form, when they appear under existential quantification, the quantification needs to be limited to a finite range[9]. Since the evaluation of a co-predicate might not terminate, co-predicates are always ghost. There is

[9]Higher-order function support in Dafny is rather modest and typical reasoning patterns do not involve them, so this restriction is not as limiting as it would have been in, e.g., Coq.

also a restriction on the call graph that a cluster containing a co-predicate must contain only co-predicates, no other kinds of functions.

A **copredicate** declaration of `P` defines not just a co-predicate, but also a corresponding *prefix predicate* `P#`. A prefix predicate is a finite unrolling of a co-predicate. The prefix predicate is constructed from the co-predicate by

- adding a parameter _k of type nat to denote the prefix length,
- adding the clause "**decreases** `_k;`" to the prefix predicate (the co-predicate itself is not allowed to have a decreases clause),
- replacing in the body of the co-predicate every intra-cluster call `Q(args)` to a copredicate by a call `Q#[_k - 1](args)` to the corresponding prefix predicate, and then
- prepending the body with `if _k = 0 then true else`.

For example, for co-predicate `Pos`, the definition of the prefix predicate `Pos#` is as suggested above. Syntactically, the prefix-length argument passed to a prefix predicate to indicate how many times to unroll the definition is written in square brackets, as in `Pos#[k](s)`. In the Dafny grammar this is called a `HashCall`. The definition of `Pos#` is available only at clusters strictly higher than that of `Pos`; that is, `Pos` and `Pos#` must not be in the same cluster. In other words, the definition of `Pos` cannot depend on `Pos#`.

19.3.4.1 Co-Equality Equality between two values of a co-datatype is a built-in co-predicate. It has the usual equality syntax `s == t`, and the corresponding prefix equality is written `s ==#[k] t`. And similarly for `s != t` and `s !=#[k] t`.

19.3.5 Co-inductive Proofs

From what we have said so far, a program can make use of properties of co-datatypes. For example, a method that declares `Pos(s)` as a precondition can rely on the stream `s` containing only positive integers. In this section, we consider how such properties are established in the first place.

19.3.5.1 Properties About Prefix Predicates Among other possible strategies for establishing co-inductive properties we take the time-honored approach of reducing co-induction to induction. More precisely, Dafny passes to the SMT solver an assumption `D(P)` for every co-predicate `P`, where:

```
D(P) = ? x • P(x) <==> ? k • P#[k](x)
```

In other words, a co-predicate is true iff its corresponding prefix predicate is true for all finite unrollings.

In Sec. 4 of the paper [Co-induction Simply] a soundness theorem of such assumptions is given, provided the co-predicates meet the co-friendly restrictions.

An example proof of `Pos(Up(n))` for every `n > 0` is here shown:

```
lemma UpPosLemma(n: int)
  requires n > 0
  ensures Pos(Up(n))
{
  forall k | 0 <= k { UpPosLemmaK(k, n); }
}

lemma UpPosLemmaK(k: nat, n: int)
  requires n > 0
  ensures Pos#[k](Up(n))
  decreases k
{
  if k != 0 {
    // this establishes Pos#[k-1](Up(n).tail)
    UpPosLemmaK(k-1, n+1);
  }
}
```

The lemma `UpPosLemma` proves `Pos(Up(n))` for every `n > 0`. We first show `Pos#[k](Up(n ))`, for `n > 0` and an arbitrary `k`, and then use the forall statement to show `? k • Pos#[k](Up(n))`. Finally, the axiom `D(Pos)` is used (automatically) to establish the co-predicate.

19.3.5.2 Colemmas As we just showed, with help of the `D` axiom we can now prove a co-predicate by inductively proving that the corresponding prefix predicate holds for all prefix lengths `k` . In this section, we introduce *co-lemma* declarations, which bring about two benefits. The first benefit is that co-lemmas are syntactic sugar and reduce the tedium of having to write explicit quantifications over `k` . The second benefit is that, in simple cases, the bodies of co-lemmas can be understood as co-inductive proofs directly. As an example consider the following co-lemma.

```
colemma UpPosLemma(n: int)
  requires n > 0
  ensures Pos(Up(n))
{
  UpPosLemma(n+1);
}
```

This co-lemma can be understood as follows: `UpPosLemma` invokes itself co-recursively to obtain the proof for `Pos(Up(n).tail)` (since `Up(n).tail` equals `Up(n+1)`). The proof glue needed to then conclude `Pos(Up(n))` is provided automatically, thanks to the power of the SMT-based verifier.

19.3.5.3 Prefix Lemmas To understand why the above `UpPosLemma` co-lemma code is a sound proof, let us now describe the details of the desugaring of co-lemmas. In analogy to how a **copredicate** declaration defines both a co-predicate and a prefix predicate, a **colemma** declaration defines both a co-lemma and *prefix lemma*. In the call graph, the cluster containing a co-lemma must contain only co-lemmas and prefix lemmas, no other methods or function. By decree, a co-lemma and its corresponding prefix lemma are always placed in the same cluster. Both co-lemmas and prefix lemmas are always ghosts.

The prefix lemma is constructed from the co-lemma by

- adding a parameter `_k` of type `nat` to denote the prefix length,
- replacing in the co-lemma's postcondition the positive co-friendly occurrences of co-predicates by corresponding prefix predicates, passing in `_k` as the prefix-length argument,
- prepending `_k` to the (typically implicit) **decreases** clause of the co-lemma,
- replacing in the body of the co-lemma every intra-cluster call `M(args)` to a colemma by a call `M#[_k - 1](args)` to the corresponding prefix lemma, and then
- making the body's execution conditional on `_k != 0`.

Note that this rewriting removes all co-recursive calls of co-lemmas, replacing them with recursive calls to prefix lemmas. These recursive call are, as usual, checked to be terminating. We allow the pre-declared identifier `_k` to appear in the original body of the co-lemma.[10]

We can now think of the body of the co-lemma as being replaced by a **forall** call, for every k , to the prefix lemma. By construction, this new body will establish the colemma's declared postcondition (on account of the `D` axiom, and remembering that only the positive co-friendly occurrences of co-predicates in the co-lemma's postcondition are rewritten), so there is no reason for the program verifier to check it.

The actual desugaring of our co-lemma `UpPosLemma` is in fact the previous code for the `UpPosLemma` lemma except that `UpPosLemmaK` is named `UpPosLemma#` and modulo a minor syntactic difference in how the `k` argument is passed.

In the recursive call of the prefix lemma, there is a proof obligation that the prefixlength argument `_k - 1` is a natural number. Conveniently, this follows from the fact that the body has been wrapped in an `if _k != 0` statement. This also means that the postcondition must hold trivially when `_k = 0`, or else a postcondition violation will be reported. This is an appropriate design

[10]Note, two places where co-predicates and co-lemmas are not analogous are: co-predicates must not make recursive calls to their prefix predicates, and co-predicates cannot mention _k.

for our desugaring, because co-lemmas are expected to be used to establish co-predicates, whose corresponding prefix predicates hold trivially when `_k = 0`. (To prove other predicates, use an ordinary lemma, not a co-lemma.)

It is interesting to compare the intuitive understanding of the co-inductive proof in using a co-lemma with the inductive proof in using the lemma. Whereas the inductive proof is performing proofs for deeper and deeper equalities, the co-lemma can be understood as producing the infinite proof on demand.

20 Newtypes

```
NewtypeDecl = "newtype" { Attribute } NewtypeName "="
  ( NumericTypeName [ ":" Type ] "|" Expression(allowLemma: false, allowLambda: true)
  | Type
  )
```

A new numeric type can be declared with the *newtype* declaration, for example:

```
newtype N = x: M | Q
```

where `M` is a numeric type and `Q` is a boolean expression that can use `x` as a free variable. If `M` is an integer-based numeric type, then so is `N`; if `M` is real-based, then so is `N`. If the type `M` can be inferred from `Q`, the "`: M`" can be omitted. If `Q` is just `true`, then the declaration can be given simply as:

```
newtype N = M
```

Type `M` is known as the *base type* of `N`.

A newtype is a numeric type that supports the same operations as its base type. The newtype is distinct from and incompatible with other numeric types; in particular, it is not assignable to its base type without an explicit conversion. An important difference between the operations on a newtype and the operations on its base type is that the newtype operations are defined only if the result satisfies the predicate `Q`, and likewise for the literals of the newtype.[11]

For example, suppose `lo` and `hi` are integer-based numerics that satisfy `0 <= lo <= hi` and consider the following code fragment:

```
var mid := (lo + hi) / 2;
```

If `lo` and `hi` have type `int`, then the code fragment is legal; in particular, it never overflows, since `int` has no upper bound. In contrast, if `lo` and `hi` are variables of a newtype `int32` declared as follows:

```
newtype int32 = x | -0x80000000 <= x < 0x80000000
```

[11] Would it be useful to also automatically define `predicate N?(x: M) { Q }`?

then the code fragment is erroneous, since the result of the addition may fail to satisfy the predicate in the definition of `int32`. The code fragment can be rewritten as

```
var mid := lo + (hi - lo) / 2;
```

in which case it is legal for both `int` and `int32`.

Since a newtype is incompatible with its base type and since all results of the newtype's operations are members of the newtype, a compiler for Dafny is free to specialize the run-time representation of the newtype. For example, by scrutinizing the definition of `int32` above, a compiler may decide to store `int32` values using signed 32-bit integers in the target hardware.

Note that the bound variable `x` in `Q` has type `M`, not `N`. Consequently, it may not be possible to state `Q` about the `N` value. For example, consider the following type of 8-bit 2's complement integers:

```
newtype int8 = x: int | -128 <= x < 128
```

and consider a variable `c` of type `int8`. The expression

```
-128 <= c < 128
```

is not well-defined, because the comparisons require each operand to have type `int8`, which means the literal `128` is checked to be of type `int8`, which it is not. A proper way to write this expression would be to use a conversion operation, described next, on `c` to convert it to the base type:

```
-128 <= int(c) < 128
```

If possible, Dafny will represent values of the newtype using a native data type for the sake of efficiency. This action can be inhibited or a specific native data type selected by using the `{:nativeType}` attribute, as explained in section [#sec-nativetype].

There is a restriction that the value `0` must be part of every newtype.[12]

Furthermore, for the compiler to be able to make an appropriate choice of representation, the constants in the defining expression as shown above must be known constants at compile-time. They need not be numeric literals; combinations of basic operations and symbolic constants are also allowed as described in Section: Compile-Time Constants.

20.1 Numeric conversion operations

For every numeric type `N`, there is a conversion function with the same name. It is a partial identity function. It is defined when the given value, which can be of any numeric type, is a member of the type converted to. When the conversion is

[12]The restriction is due to a current limitation in the compiler. This will change in the future and will also open up the possibility for subset types and non-null reference types.

from a real-based numeric type to an integer-based numeric type, the operation requires that the real-based argument has no fractional part. (To round a real-based numeric value down to the nearest integer, use the `.Floor` member, see Section [#sec-numeric-types].)

To illustrate using the example from above, if `lo` and `hi` have type `int32`, then the code fragment can legally be written as follows:

```
var mid := (int(lo) + int(hi)) / 2;
```

where the type of `mid` is inferred to be `int`. Since the result value of the division is a member of type `int32`, one can introduce yet another conversion operation to make the type of `mid` be `int32`:

```
var mid := int32((int(lo) + int(hi)) / 2);
```

If the compiler does specialize the run-time representation for `int32`, then these statements come at the expense of two, respectively three, run-time conversions.

21 Subset types

TO BE WRITTEN: add `-->` (subset of `~>`), `->` (subset of `-->`), non-null types subset of nullable types

```
NatType_ = "nat"
```

A *subset type* is a restricted use of an existing type, called the *base type* of the subset type. A subset type is like a combined use of the base type and a predicate on the base type.

An assignment from a subset type to its base type is always allowed. An assignment in the other direction, from the base type to a subset type, is allowed provided the value assigned does indeed satisfy the predicate of the subset type. (Note, in contrast, assignments between a newtype and its base type are never allowed, even if the value assigned is a value of the target type. For such assignments, an explicit conversion must be used, see Section [#sec-numeric-conversion-operations].)

Dafny supports one subset type, namely the built-in type `nat`, whose base type is `int`.[13] Type `nat` designates the non-negative subrange of `int`. A simple example that puts subset type `nat` to good use is the standard Fibonacci function:

```
function Fib(n: nat): nat
{
  if n < 2 then n else Fib(n-2) + Fib(n-1)
}
```

[13] A future version of Dafny will support user-defined subset types.

An equivalent, but clumsy, formulation of this function (modulo the wording of any error messages produced at call sites) would be to use type `int` and to write the restricting predicate in pre- and postconditions:

```
function Fib(n: int): int
  requires 0 <= n  // the function argument must be non-negative
  ensures 0 <= Fib(n)  // the function result is non-negative
{
  if n < 2 then n else Fib(n-2) + Fib(n-1)
}
```

Type inference will never infer the type of a variable to be a subset type. It will instead infer the type to be the base type of the subset type. For example, the type of `x` in

```
forall x :: P(x)
```

will be `int`, even if predicate `P` declares its argument to have type `nat`.

22 Type Inference

TO BE WRITTEN

23 Statements

```
Stmt = ( BlockStmt | AssertStmt | AssumeStmt | ExpectStmt | PrintStmt
  | UpdateStmt | UpdateFailureStmt
  | VarDeclStatement | IfStmt | WhileStmt | MatchStmt | ForallStmt
  | CalcStmt | ModifyStmt | LabeledStmt_ | BreakStmt_ | ReturnStmt
  | RevealStmt | YieldStmt
  )
```

Many of Dafny's statements are similar to those in traditional programming languages, but a number of them are significantly different. This grammar production shows the different kinds of Dafny statements. They are described in subsequent sections.

23.1 Labeled Statement

```
LabeledStmt_ = "label" LabelName ":" Stmt
```

A labeled statement is just the keyword `label` followed by an identifier which is the label, followed by a colon and a statement. The label may be referenced in a break statement that is within the labeled statement to transfer control to the location after the labeled statement. The label is not allowed to be the same as any previous dominating label.

The label may also be used in an `old` expression. In this case the label must have been encountered during the control flow in route to the `old` expression. That is, again, the label must dominate the use of the label.

23.2 Break Statement

```
BreakStmt_ = "break" ( LabelName | { "break" } ) ";"
```

A break statement provides a means to transfer control in a way different than the usual nested control structures. There are two forms of break statement: with and without a label.

If a label is used, the break statement must be enclosed in a statement with that label and the result is to transfer control to the statement after the labeled statement. For example, such a break statement can be used to exit a sequence of statements in a block statement before reaching the end of the block.

For example,

```
L: {
  var n := ReadNext();
  if n < 0  { break L; }
  DoSomething(n);
}
```

is equivalent to

```
{
  var n: ReadNext();
  if 0 <= n {
    DoSomething(n);
  }
}
```

If no label is specified and the statement lists `n` occurrences of `break`, then the statement must be enclosed in at least `n` levels of loops. Control continues after exiting `n` enclosing loops. For example,

```
var i := 0;
while i < 10 {
  var j := 0;
  while j < 10 {
    var k := 0;
    while k < 10 {
      if (j + k == 15) break break;
      k := k + 1;
    }
    j := j + 1;
  }
```

```
  // control continues here after the break
  i := i + 1;
}
```

23.3 Block Statement

```
BlockStmt = "{" { Stmt } "}"
```

A block statement is just a sequence of statements enclosed by curly braces. Local variables declared in the block end their scope at the end of the block.

23.4 Return Statement

```
ReturnStmt = "return" [ Rhs { "," Rhs } ] ";"
```

A return statement can only be used in a method. It is used to terminate the execution of the method.

To return a value from a method, the value is assigned to one of the named out-parameters sometime before a return statement. In fact, the out-parameters act very much like local variables, and can be assigned to more than once. Return statements are used when one wants to return before reaching the end of the body block of the method.

Return statements can be just the return keyword (where the current value of the out-parameters are used), or they can take a list of expressions to return. If a list is given, the number of expressions given must be the same as the number of named out-parameters. These expressions are evaluated, then they are assigned to the out-parameters, and then the method terminates.

23.5 Yield Statement

```
YieldStmt = "yield" [ Rhs { "," Rhs } ] ";"
```

A yield statement can only be used in an iterator. See section Iterator types for more details about iterators.

The body of an iterator is a *co-routine*. It is used to yield control to its caller, signaling that a new set of values for the iterator's yield parameters (if any) are available. Values are assigned to the yield parameters at or before a yield statement. In fact, the yield parameters act very much like local variables, and can be assigned to more than once. Yield statements are used when one wants to return new yield parameter values to the caller. Yield statements can be just the **yield** keyword (where the current value of the yield parameters are used), or they can take a list of expressions to yield. If a list is given, the number of expressions given must be the same as the number of named return yield

parameters. These expressions are then evaluated, then they are assigned to the yield parameters, and then the iterator yields.

23.6 Update and Call Statements

```
UpdateStmt =
    Lhs
    ( {Attribute} ";"
    |If more than one
left-hand side is used, these must denote different l-values, unless the
corresponding right-hand sides also denote the same value.
     { "," Lhs }
     ( ":=" Rhs { "," Rhs }
     | ":|" [ "assume" ]
                Expression(allowLemma: false, allowLambda: true)
     )
     ";"
    | ":"
    )
```

```
CallStmt_ =
    [ Lhs { , Lhs } ":=" ] Lhs ";"
```

The update statement serves several logical purposes.

1) The form

```
Lhs {Attribute} ";"
```

is assumed to be a call to a method with no out-parameters.

2) The form

```
    [ Lhs { , Lhs } ":=" ] Lhs ";"
```

can occur in the `UpdateStmt` grammar when there is a single Rhs that takes the special form of a `Lhs` that is a call; that is, this form matches the grammar of a `CallStmt_`, in which the `Lhs` after the `:=` references a method and the arguments to it, corresponding to a method call or a new allocation with an initializing method. This is the only case where the number of left-hand sides can be different than the number of right-hand sides in the `UpdateStmt`. In that case the number of left-hand sides must match the number of out-parameters of the method that is called or there must be just one `Lhs` to the left of the `:=`, which then is assigned a tuple of the out-parameters. Note that the result of a method call is not allowed to be used as an argument of another method call, as if it were an expression.

3) If no call is involved, the `UpdateStmt` can be a parallel assignment of right-hand-side values to the left-hand sides. For example, `x,y := y,x` swaps the values of `x` and `y`. If more than one left-hand side is used, these must denote different l-values, unless the corresponding right-hand sides also denote the same value. There must be an equal number of left-hand sides and right-hand sides in this case. Of course, the most common case will have only one `Rhs` and one `Lhs`.

4) The form that uses "`:|`" assigns some values to the left-hand side variables such that the boolean expression on the right hand side is satisfied. This can be used to make a choice as in the following example where we choose an element in a set.

```
method Sum(X: set<int>) returns (s: int)
{
  s := 0; var Y := X;
  while Y != {}
    decreases Y
  {
    var y: int;
    y :| y in Y;
    s, Y := s + y, Y - {y};
  }
}
```

Dafny will report an error if it cannot prove that values exist which satisfy the condition.

In addition, as the choice is arbitrary, assignment statements using `:|` may be non-deterministic when executed.

Note that the form

```
    Lhs ":"
```

is diagnosed as a label in which the user forgot the **label** keyword.

23.7 Update with Failure Statement (:-)

```
UpdateFailureStmt  =
    [ Lhs { "," Lhs } ]
    ":-"
    [ "expect" ]
    Expression(allowLemma: false, allowLambda: false) { "," Rhs }
```

A `:-` statement is similar to a `:=` statement, but allows for immediate return if a failure is detected. This is a language feature somewhat analogous to exceptions in other languages.

An update-with-failure statement uses *failure-compatible* types. A failure-compatible type is a type that has the following members (each with no in-parameters and one out-parameter):

- a function method `IsFailure()` that returns a `bool`
- a function method `PropagateFailure()` that returns a value assignable to the first out-parameter of the caller
- an optional method or function `Extract()`

A failure-compatible type with an `Extract` member is called *value-carrying*.

To use this form of update,

- the caller must have a first out-parameter whose type matches the output of `PropagateFailure` applied to the first output of the callee
- if the RHS of the update-with-failure statement is a method call, the first out-parameter of the callee must be failure-compatible
- if instead the RHS of the update-with-failure statement is one or more expressions, the first of these expressions must be a value with a failure-compatible type
- if the failure-compatible type of the RHS does not have an `Extract` member, then the LHS of the `:-` statement has one less expression than the RHS (or than the number of out-parameters from the method call)
- if the failure-compatible type of the RHS does have an `Extract` member, then the LHS of the `:-` statement has the same number of expressions as the RHS (or as the number of out-parameters from the method call) and the type of the first LHS expression must be assignable from the return type of the `Extract` member
- the `IsFailure` and `PropagateFailure` methods may not be ghost
- the LHS expression assigned the output of the `Extract` member is ghost precisely if `Extract` is ghost

23.7.1 Failure compatible types

A simple failure-compatible type is the following:

```
datatype Status =
| Success
| Failure(error: string)
{
  predicate method IsFailure() { this.Failure?  }
  function method PropagateFailure(): Status
    requires IsFailure()
  {
    Failure(this.error)
  }
}
```

A commonly used alternative that carries some value information is something

like this generic type:

```
datatype Outcome<T> =
| Success(value: T)
| Failure(error: string)
{
  predicate method IsFailure() {
    this.Failure?
  }
  function method PropagateFailure<U>(): Outcome<U>
    requires IsFailure()
  {
    Failure(this.error) // this is Outcome<U>.Failure(...)
  }
  function method Extract(): T
    requires !IsFailure()
  {
    this.value
  }
}
```

23.7.2 Simple status return with no other outputs

The simplest use of this failure-return style of programming is to have a method call that just returns a non-value-carrying `Status` value:

```
method Callee(i: int) returns (r: Status)
{
  if i < 0 { return Failure("negative"); }
  return Success;
}

method Caller(i: int) returns (rr: Status)
{
  :- Callee(i);
  ...
}
```

Note that there is no LHS to the `:-` statement. If `Callee` returns `Failure`, then the caller immediately returns, not executing any statements following the call of `Callee`. The value returned by `Caller` (the value of `rr` in the code above) is the result of `PropagateFailure` applied to the value returned by `Callee`, which is often just the same value. If `Callee` does not return `Failure` (that is, returns a value for which `IsFailure()` is `false`) then that return value is forgotten and execution proceeds normally with the statements following the call of `callee` in the body of `Caller`.

The desugaring of the `:- Callee(i);` statement is

```
var tmp;
tmp := Callee(i);
if tmp.IsFailure() {
  rr := tmp.PropagateFailure();
  return;
}
```

In this and subsequent examples of desugaring, the `tmp` variable is a new, unique variable, unused elsewhere in the calling member.

23.7.3 Status return with additional outputs

The example in the previous subsection affects the program only through side effects or the status return itself. It may well be convenient to have additional out-parameters, as is allowed for `:=` updates; these out-parameters behave just as for `:=`. Here is an example:

```
method Callee(i: int) returns (r: Status, v: int, w: int)
{
  if i < 0 { return Failure("negative"), 0, 0; }
  return Success, i+i, i*i;
}

method Caller(i: int) returns (rr: Status, k: int)
{
  var j: int;
  j, k :- Callee(i);
  k := k + k;
  ...
}
```

Here `Callee` has two outputs in addition to the `Status` output. The LHS of the `:-` statement accordingly has two l-values to receive those outputs. The recipients of those outputs may be any sort of l-values; here they are a local variable and an out-parameter of the caller. Those outputs are assigned in the `:-` call regardless of the `Status` value:

- If `Callee` returns a failure value as its first output, then the other outputs are assigned, the *caller's* first out-parameter (here `rr`) is assigned the value of `PropagateFailure`, and the caller returns.
- If `Callee` returns a non-failure value as its first output, then the other outputs are assigned and the caller continues execution as normal.

The desugaring of the `j, k :- Callee(i);` statement is

```
var tmp;
tmp, j, k := Callee(i);
if tmp.IsFailure() {
```

```
  rr := tmp.PropagateFailure();
  return;
}
```

23.7.4 Failure-returns with additional data

The failure-compatible return value can carry additional data as shown in the `Outcome<T>` example above. In this case there is a (first) LHS l-value to receive this additional data.

```
method Callee(i: int) returns (r: Outcome<nat>, v: int)
{
  if i < 0 { return Failure("negative"), i+i; }
  return Success(i), i+i;
}

method Caller(i: int) returns (rr: Outcome<int>, k: int)
{
  var j: int;
  j, k := Callee(i);
  k := k + k;
  ...
}
```

Suppose `Caller` is called with an argument of `10`. Then `Callee` is called with argument `10` and returns `r` and `v` of `Outcome<nat>.Success(10)` and `20`. Here `r.IsFailure()` is `false`, so control proceeds normally. The `j` is assigned the result of `r.Extract()`, which will be `10`, and `k` is assigned `20`. Control flow proceeds to the next line, where `k` now gets the value `40`.

Suppose instead that `Caller` is called with an argument of `-1`. Then `Callee` is called with the value `-1` and returns `r` and `v` with values `Outcome<nat>.Failure("negative")` and `-2`. `k` is assigned the value of `v` (-2). But `r.IsFailure()` is `true`, so control proceeds directly to return from `Caller`. The first out-parameter of `Caller` (`rr`) gets the value of `r.PropagateFailure()`, which is `Outcome<int>.Failure("negative")`; `k` already has the value `-2`. The rest of the body of `Caller` is skipped. In this example, the first out-parameter of `Caller` has a failure-compatible type so the exceptional return will propagate up the call stack. It will keep propagating up the call stack as long as there are callers with this first special output type and calls that use `:-` and the return value keeps having `IsFailure()` true.

The desugaring of the `j, k :- Callee(i);` statement in this example is

```
var tmp;
tmp, k := Callee(i);
if tmp.IsFailure() {
  rr := tmp.PropagateFailure();
```

```
  return;
}
j := tmp.Extract();
```

23.7.5 RHS with expression list

Instead of a failure-returning method call on the RHS of the statement, the RHS can instead be a list of expressions. As for a `:=` statement, in this form, the expressions on the left and right sides of `:-` must correspond, just omitting a LHS l-value for the first RHS expression if its type is not value-carrying. The semantics is very similar to that in the previous subsection.

- The first RHS expression must have a failure-compatible type.
- All the assignments of RHS expressions to LHS values except for the first RHS value are made.
- If the first RHS value (say `r`) responds `true` to `r.IsFailure()`, then `r.PropagateFailure()` is assigned to the first out-parameter of the *caller* and the execution of the caller's body is ended.
- If the first RHS value (say `r`) responds `false` to `r.IsFailure()`, then
  - if the type of `r` is value-carrying, then `r.Extract()` is assigned to the first LHS value of the `:-` statement (if `r` is not value-carrying, then the corresponding LHS l-value is omitted)
  - execution of the caller's body continues with the statement following the `:-` statement.

A RHS with a method call cannot be mixed with a RHS containing multiple expressions.

For example, the desugaring of

```
method m(Status r) returns (rr: Status) {
  var j, k;
  j, k :- r, 7;
  ...
}
```

is

```
var j, k;
var tmp;
tmp, k := r, 7;
if tmp.IsFailure() {
  rr := tmp.PropagateFailure();
  return;
}
```

23.7.6 Failure with initialized declaration.

The `:-` syntax can also be used in initalization, as in

```
var s :- M();
```

This is equivalent to

```
var s;
s :- M();
```

with the semantics as described above.

23.7.7 Expect alternative

In any of the above described uses of `:-`, the `:-` token may be followed immediately by the keyword `expect`. This keyword states that the RHS evaluation is expected to be successful: if the failure-compatible value is a failure, then the program halts immediately (precisely as with the `expect` statement); if the return value is not a failure, the semantics is as described in previous sub-sections.

The equivalent desugaring replaces

```
if tmp.IsFailure() {
  rr := tmp.PropagateFailure();
  return;
}
```

with

```
expect !tmp.IsFailure(), tmp;
```

23.7.8 Key points

There are several points to note.

- The first out-parameter of the callee is special. It has a special type and that type indicates that the value is inspected to see if an immediate return from the caller is warranted. This type is often a datatype, as shown in the examples above, but it may be any type with the appropriate members.
- The restriction on the type of caller's first out-parameter is just that it must be possible (perhaps through generic instantiation and type inference, as in these examples) for `PropagateFailure` applied to the failure-compatible output from the callee to produce a value of the caller's first out-parameter type. If the caller's first out-parameter type is failure-compatible (which it need not be), then failures can be propagated up the call chain.
- In the statement `j, k :- callee(i);`, when the callee's return value has an `Extract` member, the type of `j` is not the type of the first out-parameter of `callee`. Rather it is a type assignable from the output type of `Extract` applied to the first out-value of `callee`.

- A method like `callee` with a special first out-parameter type can still be used in the normal way: `r, k := callee(i)`. Now `r` gets the first output value from callee, of type `Status` or `Outcome<nat>` in the examples above. No special semantics or exceptional control paths apply. Subsequent code can do its own testing of the value of `r` and whatever other computations or control flow are desired.
- The caller and callee can have any (positive) number of output arguments, as long as the callee's first out-parameter has a failure-compatible type and the caller's first out-parameter type matches `PropagateFailure`.
- If there is more than one LHS, the LHSs must denote different l-values, unless the RHS is a list of expressions and the corresponding RHS values are equal.
- The LHS l-values are evaluated before the RHS method call, in case the method call has side-effects or return values that modify the l-values prior to assignments being made.

It is important to note the connection between the failure-compatible types used in the caller and callee, if they both use them. They do not have to be the same type, but they must be closely related, as it must be possible for the callee's `PropagateFailure` to return a value of the caller's failure-compatible type. In practice this means that one such failure-compatible type should be used for an entire program. If a Dafny program uses a library shared by multiple programs, the library should supply such a type and it should be used by all the client programs (and, effectively, all Dafny libraries). It is also the case that it is inconvenient to mix types such as `Outcome` and `Status` above within the same program. If there is a mix of failure-compatible types, then the program will need to use `:=` statements and code for explicit handling of failure values.

23.7.9 Failure returns and exceptions

The `:-` mechanism is like the exceptions used in other programming languages, with some similarities and differences.

- There is essentially just one kind of 'exception' in Dafny, the variations of the failure-compatible data type.
- Exceptions are passed up the call stack whether or not intervening methods are aware of the possibility of an exception, that is, whether or not the intervening methods have declared that they throw exceptions. Not so in Dafny: a failure is passed up the call stack only if each caller has a failure-compatible first out-parameter, is itself called in a `:-` statement, and returns a value that responds true to `IsFailure()`.
- All methods that contain failure-return callees must explicitly handle those failures using either `:-` statements or using `:=` statements with a LHS to receive the failure value.

23.8 Variable Declaration Statement

```
VarDeclStatement = [ "ghost" ] "var" { Attribute }
  (
    LocalIdentTypeOptional
    { "," { Attribute } LocalIdentTypeOptional }
    [ ":=" Rhs { "," Rhs }
    | { Attribute } ":|" [ "assume" ]
                    Expression(allowLemma: false, allowLambda: true)
    | ":-" [ "expect" ] Expression { "," Rhs }
    ]
  |
    "(" CasePattern { "," CasePattern } ")"
    ":=" Expression(allowLemma: false, allowLambda: true)
  )
  ";"
```

A `VarDeclStatement` is used to declare one or more local variables in a method or function. The type of each local variable must be given unless its type can be inferred, either from a given initial value, or from other uses of the variable. If initial values are given, the number of values must match the number of variables declared.

Note that the type of each variable must be given individually. The following code

```
var x, y : int;
```

does not declare both `x` and `y` to be of type `int`. Rather it will give an error explaining that the type of `x` is underspecified if it cannot be inferred from uses of x.

What follows the `LocalIdentTypeOptional` optionally combines the variable declarations with an update statement (cf. Update and Call Statement). If the Rhs is a call, then any variable receiving the value of a formal ghost out-parameter will automatically be declared as ghost, even if the **ghost** keyword is not part of the variable declaration statement.

The left-hand side can also contain a tuple of patterns which will be matched against the right-hand-side. For example:

```
function returnsTuple() : (int, int)
{
    (5, 10)
}

function usesTuple() : int
{
```

```
    var (x, y) := returnsTuple();
    x + y
}
```

23.9 Guards

```
Guard = ( "*"
        | "(" "*" ")"
        | Expression(allowLemma: true, allowLambda: true)
        )
```

Guards are used in `if` and `while` statements as boolean expressions. Guards take two forms.

The first and most common form is just a boolean expression.

The second form is either `*` or `(*)`. These have the same meaning. An unspecified boolean value is returned. The value returned may be different each time it is executed.

23.10 Binding Guards

```
BindingGuard(allowLambda) =
  IdentTypeOptional { "," IdentTypeOptional } { Attribute }
  ":|" Expression(allowLemma: true, allowLambda)
```

`IfStmt`s can also take a `BindingGuard`. It checks if there exist values for the given variables that satisfy the given expression. If so, it binds some satisfying values to the variables and proceeds into the "then" branch; otherwise it proceeds with the "else" branch, where the bound variables are not in scope.

In other words, the statement

```
if x :| P { S } else { T }
```

has the same meaning as

```
if exists x :| P { var x :| P; S } else { T }
```

The identifiers bound by `BindingGuard` are ghost variables and cannot be assigned to non-ghost variables. They are only used in specification contexts.

Here is an example:

```
predicate P(n: int)
{
  n % 2 == 0
}
```

```
method M1() returns (ghost y: int)
    requires exists x :: P(x)
    ensures P(y)
{
  if x : int :| P(x) {
      y := x;
  }
}
```

23.11 If Statement

```
IfStmt = "if"
  ( IfAlternativeBlock
  | "{" IfAlternativeBlock "}"
  |
    ( BindingGuard(allowLambda: true)
    | Guard
    | "..."
    )
    BlockStmt [ "else" ( IfStmt | BlockStmt ) ]
  )
```

```
IfAlternativeBlock =
      { "case"
      (
        BindingGuard(allowLambda:false)
      | Expression(allowLemma: true, allowLambda: false)
      ) "=>" { Stmt } } .
```

The simplest form of an `if` statement uses a guard that is a boolean expression. It then has the same form as in C# and other common programming languages. For example,

```
  if x < 0 {
    x := -x;
  }
```

If the guard is an asterisk then a non-deterministic choice is made:

```
  if * {
    print "True";
  } else {
    print "False";
  }
```

The `if` statement using the `IfAlternativeBlock` form is similar to the `if ... fi` construct used in the book "A Discipline of Programming" by Edsger W.

Dijkstra. It is used for a multi-branch `if`.

For example:

```
if {
  case x <= y => max := y;
  case y <= x => max := x;
}
```

In this form, the expressions following the `case` keyword are called *guards*. The statement is evaluated by evaluating the guards in an undetermined order until one is found that is `true` and the statements to the right of `=>` for that guard are executed. The statement requires at least one of the guards to evaluate to `true`.

23.12 While Statement

```
WhileStmt = "while"
  ( LoopSpecWhile ( WhileAlternativeBlock | "{" WhileAlternativeBlock "}" )
  | ( Guard | "..." ) LoopSpec
      ( BlockStmt
      | "..."
      | /* go body-less */
      )
  )
```

```
WhileAlternativeBlock =
   "{"
   { "case" Expression(allowLemma: true, allowLambda: false)
   "=>" { Stmt } }
   "}
```

Loops need *loop specifications* (`LoopSpec` in the grammar) in order for Dafny to prove that they obey expected behavior. In some cases Dafny can infer the loop specifications by analyzing the code, so the loop specifications need not always be explicit. These specifications are described in the section on Loop Specifications.

The `while` statement is Dafny's only loop statement. It has two general forms.

The first form is similar to a while loop in a C-like language. For example:

```
var i := 0;
while i < 5 {
  i := i + 1;
}
```

In this form, the condition following the `while` is one of these:

- A boolean expression. If true it means execute one more iteration of the loop. If false then terminate the loop.
- An asterisk (`*`), meaning non-deterministically yield either `true` or `false` as the value of the condition

The second form uses the `WhileAlternativeBlock`. It is similar to the `do ... od` construct used in the book "A Discipline of Programming" by Edsger W. Dijkstra. For example:

```
while
  decreases if 0 <= r then r else -r;
{
  case r < 0 =>
    r := r + 1;
  case 0 < r =>
    r := r - 1;
}
```

For this form, the guards are evaluated in some undetermined order until one is found that is true, in which case the corresponding statements are executed. If none of the guards evaluates to true, then the loop execution is terminated. k

23.13 Loop Specifications

For some simple loops, such as those mentioned previously, Dafny can figure out what the loop is doing without more help. However, in general the user must provide more information in order to help Dafny prove the effect of the loop. This information is provided by a `LoopSpec`. A `LoopSpec` provides information about invariants, termination, and what the loop modifies. For additional tutorial information see [@KoenigLeino:MOD2011] or the online Dafny tutorial.

23.13.1 Loop Invariants

Loops present a problem for specification-based reasoning. There is no way to know in advance how many times the code will go around the loop and a tool cannot reason about every one of a possibly unbounded sequence of unrollings. In order to consider all paths through a program, specification-based program verification tools require loop invariants, which are another kind of annotation.

A loop invariant is an expression that holds just prior to the loop test, that is, upon entering a loop and after every execution of the loop body. It captures something that is invariant, i.e. does not change, about every step of the loop. Now, obviously we are going to want to change variables, etc. each time around the loop, or we wouldn't need the loop. Like pre- and postconditions, an invariant is a property that is preserved for each execution of the loop, expressed using the same boolean expressions we have seen. For example,

```
var i := 0;
while i < n
  invariant 0 <= i
{
  i := i + 1;
}
```

When you specify an invariant, Dafny proves two things: the invariant holds upon entering the loop, and it is preserved by the loop. By preserved, we mean that assuming that the invariant holds at the beginning of the loop, we must show that executing the loop body once makes the invariant hold again. Dafny can only know upon analyzing the loop body what the invariants say, in addition to the loop guard (the loop condition). Just as Dafny will not discover properties of a method on its own, it will not know any but the most basic properties of a loop are preserved unless it is told via an invariant.

23.13.2 Loop Termination

Dafny proves that code terminates, i.e. does not loop forever, by using `decreases` annotations. For many things, Dafny is able to guess the right annotations, but sometimes it needs to be made explicit. There are two places Dafny proves termination: loops and recursion. Both of these situations require either an explicit annotation or a correct guess by Dafny.

A `decreases` annotation, as its name suggests, gives Dafny an expression that decreases with every loop iteration or recursive call. There are two conditions that Dafny needs to verify when using a `decreases` expression:

- that the expression actually gets smaller, and
- that it is bounded.

That is, the expression must strictly decrease in a well-founded ordering (cf. Section Well-Founded Orders.

Many times, an integral value (natural or plain integer) is the quantity that decreases, but other things that can be used as well. In the case of integers, the bound is assumed to be zero. For example, the following is a proper use of `decreases` on a loop:

```
  while 0 < i
    invariant 0 <= i
    decreases i
  {
    i := i - 1;
  }
```

Here Dafny has all the ingredients it needs to prove termination. The variable i gets smaller each loop iteration, and is bounded below by zero. This is fine, except the loop is backwards from most loops, which tend to count up instead

of down. In this case, what decreases is not the counter itself, but rather the distance between the counter and the upper bound. A simple trick for dealing with this situation is given below:

```
  while i < n
    invariant 0 <= i <= n
    decreases n - i
  {
    i := i + 1;
  }
```

This is actually Dafny's guess for this situation, as it sees `i < n` and assumes that `n - i` is the quantity that decreases. The upper bound of the loop invariant implies that `0 <= n - i`, and gives Dafny a lower bound on the quantity. This also works when the bound `n` is not constant, such as in the binary search algorithm, where two quantities approach each other, and neither is fixed.

If the **decreases** clause of a loop specified "*", then no termination check will be performed. Use of this feature is sound only with respect to partial correctness.

23.13.3 Loop Framing

In some cases we also must specify what memory locations the loop body is allowed to modify. This is done using a `modifies` clause. See the discussion of framing in methods for a fuller discussion.

TO BE WRITTEN

23.14 Match Statement

```
MatchStmt = "match" Expression(allowLemma: true, allowLambda: true)
  ( "{" { CaseStatement } "}"
  | { CaseStatement }
  )

CaseStatement = CaseBinding_ "=>" { Stmt }
```

The `match` statement is used to do case analysis on a value of inductive or co-inductive datatype (which includes the built-in tuple types), a base type, or newtype. The expression after the `match` keyword is called the *selector*. The expression is evaluated and then matched against each clause in order until a matching clause is found.

The identifier after the `case` keyword in a case clause, if present, must be either the name of one of the datatype's constructors (when the selector is a value of a datatype), a literal (when the selector is a value of a base type or a newtype), or a variable, in which case the clause matches any constructors. If the constructor takes parameters then a parenthesis-enclosed list of patterns must

follow the constructor. There must be as many patterns as the constructor has parameters. If the optional type is given it must be the same as the type of the corresponding parameter of the constructor. If no type is given then the type of the corresponding parameter is the type assigned to the identifier. If the identifier represents a variable, it cannot be applied to arguments. If the variable is not used in a case, it can be replaced by an underscore.

When an inductive value that was created using constructor expression `C1(v1, v2)` is matched against a case clause `C2(x1, x2)`, there is a match provided that `C1` and `C2` are the same constructor. In that case `x1` is bound to value `v1` and `x2` is bound to `v2`. The identifiers in the case pattern are not mutable. Here is an example of the use of a `match` statement.

```
datatype Tree = Empty | Node(left: Tree, data: int, right: Tree)

// Return the sum of the data in a tree.
method Sum(x: Tree) returns (r: int)
{
  match x {
    case Empty => r := 0;
    case Node(t1, d, t2) =>
      var v1 := Sum(t1);
      var v2 := Sum(t2);
      r := v1 + d + v2;
 }
}
```

Note that the `Sum` method is recursive yet has no `decreases` annotation. In this case it is not needed because Dafny is able to deduce that `t1` and `t2` are *smaller* (structurally) than `x`. If `Tree` had been coinductive this would not have been possible since `x` might have been infinite.

23.15 Assert Statement

```
AssertStmt =
    "assert" { Attribute }
    ( Expression(allowLemma: false, allowLambda: true)
    | "..."
    ) ";"
```

`Assert` statements are used to express logical proposition that are expected to be true. Dafny will attempt to prove that the assertion is true and give an error if the assertion cannot be provenb. Once the assertion is proved, its truth is to aid in proving following deductions. Thus if Dafny is having a difficult time verifying a method, the user may help by inserting assertions that Dafny can prove, and whose truth may aid in the larger verification effort, much as lemmas might be used in mathematical proofs.

Using `...` as the argument of the statement is part of module refinement, as described here.

TO BE WRITTEN - assert by statements

23.16 Assume Statement

```
AssumeStmt =
    "assume" { Attribute }
    ( Expression(allowLemma: false, allowLambda: true)
    | "..."
    ) ";"
```

The `assume` statement lets the user specify a logical proposition that Dafny may assume to be true without proof. If in fact the proposition is not true this may lead to invalid conclusions.

An `assume` statement would ordinarily be used as part of a larger verification effort where verification of some other part of the program required the proposition. By using the `assume` statement the other verification can proceed. Then when that is completed the user would come back and replace the `assume` with `assert`.

An `assume` statement cannot be compiled. In fact, the compiler will complain if it finds an **assume** anywhere where it has not been replaced through a refinement step.

Using `...` as the argument of the statement is part of module refinement, as described here.

23.17 Expect Statement

```
ExpectStmt =
    "expect" { Attribute }
    ( Expression(allowLemma: false, allowLambda: true)
    | "..."
    )
    [ "," Expression(allowLemma: false, allowLambda: true) ]
    ";"
```

The `expect` statement states a boolean expression that is (a) assumed to be true by the verifier and (b) checked to be true at run-time. That is, the compiler inserts into the run-time executable a check that the given expression is true; if the expression is false, then the execution of the program halts immediately. If a second argument is given, it may be a value of any type. That value is converted to a string (just like the `print` statement) and the string is included in

the message emitted by the program when it halts; otherwise a default message is emitted.

Because the expect expression and optional second argument are compiled, they cannot be ghost expressions.

`assume` statements are ignored at run-time. The `expect` statement behaves like `assume` for the verifier, but also inserts a run-time check that the assumption is indeed correct (for the test cases used at run-time).

Here are a few use-cases for the `expect` statement.

A) To check the specifications of external methods.

Consider an external method `Random` that takes a `nat` as input and returns a `nat` value that is less than the input. Such a method could be specified as

```
method {:extern} Random(n: nat) returns (r: nat)
  ensures r < n
```

But because there is no body for `Random` (only the external non-dafny implementation), it cannot be verified that `Random` actually satisfies this specification.

To mitigate this situation somewhat, we can define a wrapper function, `Random'`, that calls `Random` but in which we can put some run-time checks:

```
method {:extern} Random(n: nat) returns (r: nat)

method Random'(n: nat) returns (r: nat)
  ensures r < n
{
  r := Random(n);
  expect r < n;
}
```

Here we can verify that `Random'` satisfies its own specification, relying on the unverified specification of `Random`. But we are also checking at run-time that any input-output pairs for `Random` encountered during execution do satisfy the specification, as they are checked by the `expect` statement.

Note, in this example, two problems are still remaining. One problem is that the out-parameter of the extern `Random` has type `nat`, but there is no check that the value returned really is non-negative. It would be better to declare the out-parameter of `Random` to be `int` and to include `0 <= r` in the condition checked by the `expect` statement in `Random'`. The other problem is that `Random` surely will need `n` to be strictly positive. This can be fixed by adding `requires n != 0` to `Random'` and `Random`.

B) Run-time testing

Verification and run-time testing are complementary and both have their role in assuring that software does what is intended. Dafny can produce executables

and these can be instrumented with unit tests. Annotating a method with the `{:test}` attribute indicates to the compiler that it should produce target code that is correspondingly annotated to mark the method as a unit test (e.g., an XUnit test) in the target language. Within that method one might use `expect` statements (as well as `print` statements) to insert checks that the target program is behaving as expected.

C) Compiler tests

If one wants to assure that compiled code is behaving at run-time consistently with the statically verified code, one can use paired assert/expect statements with the same expression:

```
assert _P_;
expect _P_;
```

The verifier will check that P is always true at the given point in a program (at the `assert` statement).

At run-time, the compiler will insert checks that the same predicate, in the `expect` statement is true. Any difference identifies a compiler bug. Note that the `expect` must be after the `assert`. If the `expect` is first, then the verifier will interpret the `expect` like an `assume`, in which case the `assert` will be proved trivially and potential unsoundness will be hidden.

Using `...` as the argument of the `expect` statement is part of module refinement, as described here.

23.18 Print Statement

```
PrintStmt =
    "print" Expression(allowLemma: false, allowLambda: true)
    { "," Expression(allowLemma: false, allowLambda: true) } ";"
```

The `print` statement is used to print the values of a comma-separated list of expressions to the console. The generated code uses target-language-specific idioms to perform this printing. The expressions may of course include strings that are used for captions. There is no implicit new line added, so to add a new line you should include `"\n"` as part of one of the expressions. Dafny automatically creates implementations of methods that convert values to strings for all Dafny data types. For example,

```
datatype Tree = Empty | Node(left: Tree, data: int, right: Tree)
method Main()
{
  var x : Tree := Node(Node(Empty, 1, Empty), 2, Empty);
  print "x=", x, "\n";
}
```

produces this output:

```
x=Tree.Node(Tree.Node(Tree.Empty, 1, Tree.Empty), 2, Tree.Empty)
```

Note that Dafny does not have method overriding and there is no mechanism to override the built-in value->string conversion. Nor is there a way to explicitly invoke this conversion.

23.19 Forall Statement

```
ForallStmt = "forall"
  ( "(" [ QuantifierDomain ] ")"
  | [ QuantifierDomain ]
  )
  { ForAllEnsuresClause_ }
  [ BlockStmt ]
```

The `forall` statement executes the body simultaneously for all quantified values in the specified range. There are several variant uses of the `forall` statement and there are a number of restrictions.

In particular, a `forall` statement can be classified as one of the following:

- *Assign* - the `forall` statement is used for simultaneous assignment. The target must be an array element or an object field.
- *Call* - The body consists of a single call to a ghost method without side effects
- *Proof* - The `forall` has `ensure` expressions which are effectively quantified or proved by the body (if present).

An *assign* `forall` statement performs simultaneous assignment. The left-hand sides must denote different l-values, unless the corresponding right-hand sides also coincide.

The following is an excerpt of an example given by Leino in *Developing Verified Programs with Dafny*. When the buffer holding the queue needs to be resized, the `forall` statement is used to simultaneously copy the old contents into the new buffer.

```
class {:autocontracts} SimpleQueue<Data>
{
  ghost var Contents: seq<Data>;
  var a: array<Data>  // Buffer holding contents of queue.
  var m: int          // Index head of queue.
  var n: int          // Index just past end of queue
  ...
  method Enqueue(d: Data)
    ensures Contents == old(Contents) + [d]
```

```
  {
    if n == a.Length {
      var b := a;
      if m == 0 { b := new Data[2 * a.Length]; }
      forall i | 0 <= i < n - m {
        b[i] := a[m + i];
      }
      a, m, n := b, 0, n - m;
    }
    a[n], n, Contents := d, n + 1, Contents + [d];
  }
}
```

Here is an example of a *call* `forall` statement and the callee. This is contained in the `CloudMake-ConsistentBuilds.dfy` test in the Dafny repository.

```
forall cmd', deps', e' |
       Hash(Loc(cmd', deps', e')) == Hash(Loc(cmd, deps, e)) {
  HashProperty(cmd', deps', e', cmd, deps, e);
}

lemma HashProperty(cmd: Expression, deps: Expression, ext: string,
    cmd': Expression, deps': Expression, ext': string)
  requires Hash(Loc(cmd, deps, ext)) == Hash(Loc(cmd', deps', ext'))
  ensures cmd == cmd' && deps == deps' && ext == ext'
```

The following example of a *proof* `forall` statement comes from the same file:

```
forall p | p in DomSt(stCombinedC.st) && p in DomSt(stExecC.st)
  ensures GetSt(p, stCombinedC.st) == GetSt(p, stExecC.st)
{
  assert DomSt(stCombinedC.st) <= DomSt(stExecC.st);
  assert stCombinedC.st == Restrict(DomSt(stCombinedC.st),
                                                  stExecC.st);
}
```

More generally, the statement

```
forall x | P(x) { Lemma(x); }
```

is used to invoke `Lemma(x)` on all `x` for which `P(x)` holds. If `Lemma(x)` ensures `Q(x)`, then the forall statement establishes

```
forall x :: P(x) ==> Q(x).
```

The `forall` statement is also used extensively in the de-sugared forms of co-predicates and co-lemmas. See section [#sec-co-inductive-datatypes].

23.20 Modify Statement

```
ModifyStmt =
  "modify" { Attribute }
  ( FrameExpression(allowLemma: false, allowLambda: true)
    { "," FrameExpression(allowLemma: false, allowLambda: true) }
  | "..."
  )
  ( BlockStmt | ";" )
```

The `modify` statement has two forms which have two different purposes.

When the `modify` statement ends with a semi-colon rather than a block statement its effect is to say that some undetermined modifications have been made to any or all of the memory locations specified by the frame expressions. In the following example, a value is assigned to field `x` followed by a `modify` statement that may modify any field in the object. After that we can no longer prove that the field `x` still has the value we assigned to it.

```
class MyClass {
  var x: int
  method N()
    modifies this
  {
    x := 18;
    modify this;
    assert x == 18;  // error: cannot conclude this here
  }
}
```

When the `modify` statement is followed by a block statement, we are instead specifying what can be modified in that block statement. Namely, only memory locations specified by the frame expressions of the block `modify` statement may be modified. Consider the following example.

```
class ModifyBody {
  var x: int
  var y: int
  method M0()
    modifies this
  {
    modify {} {
      x := 3;  // error: violates modifies clause of the modify statement
    }
  }

  method M1()
```

```
    modifies this
  {
    modify {} {
      var o := new ModifyBody;
      o.x := 3;  // fine
    }
  }

  method M2()
    modifies this
  {
    modify this {
      x := 3;
    }
  }
```

```
  method M3()
    modifies this
  {
    var k: int;
    modify {} { k := 4; } // fine. k is local
  }
}
```

The first `modify` statement in the example has an empty frame expression so it cannot modify any memory locations. So an error is reported when it tries to modify field `x`.

The second `modify` statement also has an empty frame expression. But it allocates a new object and modifies it. Thus we see that the frame expressions on a block `modify` statement only limit what may be modified in already allocated memory. It does not limit what may be modified in new memory that is allocated within the block.

The third `modify` statement has a frame expression that allows it to modify any of the fields of the current object, so the modification of field `x` is allowed.

Finally, the fourth example shows that the restrictions imposed by the modify statement do not apply to local variables, only those that are heap-based.

23.21 Calc Statement

```
CalcStmt = "calc" { Attribute } [ CalcOp ] "{" CalcBody "}"
CalcBody = { CalcLine [ CalcOp ] Hints }
CalcLine = Expression(allowLemma: false, allowLambda: true) ";"
Hints = { ( BlockStmt | CalcStmt ) }
CalcOp =
  ( "==" [ "#" "["
           Expression(allowLemma: true, allowLambda: true) "]" ]
  | "<" | ">"
  | "!=" | "<=" | ">="
  | "<==>" | "==>" | "<=="
  )
```

The `calc` statement supports *calculational proofs* using a language feature called *program-oriented calculations* (poC). This feature was introduced and explained in the [*Verified Calculations*] paper by Leino and Polikarpova[@LEINO:Dafny:Calc]. Please see that paper for a more complete explanation of the `calc` statement. We here mention only the highlights.

Calculational proofs are proofs by stepwise formula manipulation as is taught in elementary algebra. The typical example is to prove an equality by starting with a left-hand-side, and through a series of transformations morph it into the desired right-hand-side.

Non-syntactic rules further restrict hints to only ghost and side-effect free statements, as well as imposing a constraint that only chain-compatible operators can be used together in a calculation. The notion of chain-compatibility is quite intuitive for the operators supported by poC; for example, it is clear that "<" and ">" cannot be used within the same calculation, as there would be no relation to conclude between the first and the last line. See the paper for a more formal treatment of chain-compatibility.

Note that we allow a single occurrence of the intransitive operator "!=" to appear in a chain of equalities (that is, "!=" is chain-compatible with equality but not with any other operator, including itself). Calculations with fewer than two lines are allowed, but have no effect. If a step operator is omitted, it defaults to the calculation-wide operator, defined after the `calc` keyword. If that operator is omitted, it defaults to equality.

Here is an example using `calc` statements to prove an elementary algebraic identity. As it turns out, Dafny is able to prove this without the `calc` statements, but the example illustrates the syntax.

```
lemma docalc(x : int, y: int)
  ensures (x + y) * (x + y) == x * x + 2 * x * y + y * y
{
  calc {
```

```
    (x + y) * (x + y);
    ==
    // distributive law: (a + b) * c == a * c + b * c
    x * (x + y) + y * (x + y);
    ==
    // distributive law: a * (b + c) == a * b + a * c
    x * x + x * y + y * x + y * y;
    ==
    calc {
        y * x;
      ==
        x * y;
    }
    x * x + x * y + x * y + y * y;
    ==
    calc {
      x * y + x * y;
      ==
      // a = 1 * a
      1 * x * y + 1 * x * y;
      ==
      // Distributive law
      (1 + 1) * x * y;
      ==
      2 * x * y;
    }
    x * x + 2 * x * y + y * y;
  }
}
```

Here we started with `(x + y) * (x + y)` as the left-hand-side expressions and gradually transformed it using distributive, commutative and other laws into the desired right-hand-side.

The justification for the steps are given as comments, or as nested `calc` statements that prove equality of some sub-parts of the expression.

The `==` operators show the relation between the previous expression and the next. Because of the transitivity of equality we can then conclude that the original left-hand-side is equal to the final expression.

We can avoid having to supply the relational operator between every pair of expressions by giving a default operator between the `calc` keyword and the opening brace as shown in this abbreviated version of the above calc statement:

```
calc == {
  (x + y) * (x + y);
```

```
  x * (x + y) + y * (x + y);
  x * x + x * y + y * x + y * y;
  x * x + x * y + x * y + y * y;
  x * x + 2 * x * y + y * y;
}
```

And since equality is the default operator, we could have omitted it after the `calc` keyword. The purpose of the block statements or the `calc` statements between the expressions is to provide hints to aid Dafny in proving that step. As shown in the example, comments can also be used to aid the human reader in cases where Dafny can prove the step automatically.

23.22 Reveal Statement

TO BE WRITTEN

24 Expressions

The grammar of Dafny expressions follows a hierarchy that reflects the precedence of Dafny operators. The following table shows the Dafny operators and their precedence in order of increasing binding power.

operator	description
`;`	In LemmaCall;Expression
`<==>`,	equivalence (if and only if)
`==>`, `<==`,	implication (implies) reverse implication (follows from)
`&&`, `&` `||`, `|`	conjunction (and) disjunction (or)

`==`
`==#[k]`
`!=`
`!=#[k]`
`<`
`<=`
`>=`
`>`
`in`
`!in`
`!!`
	equality
	prefix equality (co-inductive)
	disequality
	prefix disequality (co-inductive)
	less than
	at most
	at least
	greater than
	collection membership
	collection non-membership
	disjointness

operator	description
`+`	addition (plus)
`-`	subtraction (minus)
`*`	multiplication (times)
`/`	division (divided by)
`%`	modulus (mod)
`-`	arithmetic negation (unary minus)
`!`, ¬	logical negation
Primary Expressions	

We are calling the `UnaryExpression`s that are neither arithmetic nor logical negation the *primary expressions*. They are the most tightly bound.

In the grammar entries below we explain the meaning when the operator for that precedence level is present. If the operator is not present then we just descend to the next precedence level.

24.1 Top-level expressions

```
Expression(allowLemma, allowLambda) =
    EquivExpression(allowLemma, allowLambda)
    [ ";" Expression(allowLemma, allowLambda) ]
```

The "allowLemma" argument says whether or not the expression to be parsed is allowed to have the form S;E where S is a call to a lemma. "allowLemma" should be passed in as "false" whenever the expression to be parsed sits in a context that itself is terminated by a semi-colon.

The "allowLambda" says whether or not the expression to be parsed is allowed to be a lambda expression. More precisely, an identifier or parenthesized-enclosed comma-delimited list of identifiers is allowed to continue as a lambda expression (that is, continue with a "reads", "requires", or "=>") only if "allowLambda" is true. This affects function/method/iterator specifications, if/while statements with guarded alternatives, and expressions in the specification of a lambda expression itself.

Sometimes an expression will fail unless some relevant fact is known. In the following example the `F_Fails` function fails to verify because the `Fact(n)` divisor may be zero. But preceding the expression by a lemma that ensures that the denominator is not zero allows function `F_Succeeds` to succeed.

```
function Fact(n: nat): nat
{
  if n == 0 then 1 else n * Fact(n-1)
```

```
}

lemma L(n: nat)
  ensures 1 <= Fact(n)
{
}

function F_Fails(n: nat): int
{
  50 / Fact(n)  // error: possible division by zero
}

function F_Succeeds(n: nat): int
{
  L(n); // note, this is a lemma call in an expression
  50 / Fact(n)
}
```

24.2 Equivalence Expressions

```
EquivExpression(allowLemma, allowLambda) =
  ImpliesExpliesExpression(allowLemma, allowLambda)
  { "<==>" ImpliesExpliesExpression(allowLemma, allowLambda) }
```

An `EquivExpression` that contains one or more "<==>"s is a boolean expression and all the contained `ImpliesExpliesExpression` must also be boolean expressions. In that case each "<==>" operator tests for logical equality which is the same as ordinary equality.

See section [#sec-equivalence-operator] for an explanation of the `<==>` operator as compared with the `==` operator.

24.3 Implies or Explies Expressions

```
ImpliesExpliesExpression(allowLemma, allowLambda) =
  LogicalExpression(allowLemma, allowLambda)
  [ (  "==>" ImpliesExpression(allowLemma, allowLambda)
    | "<==" LogicalExpression(allowLemma, allowLambda)
            { "<==" LogicalExpression(allowLemma, allowLambda) }
    )
  ]

ImpliesExpression(allowLemma, allowLambda) =
  LogicalExpression(allowLemma, allowLambda)
  [  "==>" ImpliesExpression(allowLemma, allowLambda) ]
```

See section [#sec-implication-and-reverse-implication] for an explanation of the `==>` and `<==` operators.

24.4 Logical Expressions

```
LogicalExpression(allowLemma, allowLambda) =
  RelationalExpression(allowLemma, allowLambda)
  [ ( "&&" RelationalExpression(allowLemma, allowLambda)
           { "&&" RelationalExpression(allowLemma, allowLambda) }
    | "||" RelationalExpression(allowLemma, allowLambda)
           { "||" RelationalExpression(allowLemma, allowLambda) }
    )
  ]
```

TO BE WRITTEN – prefixed && and ||

See section [#sec-conjunction-and-disjunction] for an explanation of the `&&` (or) and `||` (or) operators.

24.5 Relational Expressions

```
RelationalExpression(allowLemma, allowLambda) =
  Term(allowLemma, allowLambda)
  { RelOp Term(allowLemma, allowLambda) }

RelOp =
  ( "==" [ "#" "[" Expression(allowLemma: true, allowLambda: true) "]" ]
  | "<" | ">" | "<=" | ">="
  | "!=" [ "#" "[" Expression(allowLemma: true, allowLambda: true) "]" ]
  | "in"
  | "!in"
  | "!!"
  )
```

The relation expressions that have a `RelOp` compare two or more terms. As explained in section [#sec-basic-types], `==`, `!=`, `<`, `>`, `<=`, and `>=` and their corresponding Unicode equivalents are *chaining*.

The `in` and `!in` operators apply to collection types as explained in section [#sec-collection-types] and represent membership or non-membership respectively.

The `!!` represents disjointness for sets and multisets as explained in sections [#sec-sets] and [#sec-multisets].

Note that `x ==#[k] y` is the prefix equality operator that compares co-inductive values for equality to a nesting level of k, as explained in section [#sec-co-equality].

24.6 Terms

```
Term(allowLemma, allowLambda) =
  Factor(allowLemma, allowLambda)
  { AddOp Factor(allowLemma, allowLambda) }
AddOp = ( "+" | "-" )
```

`Terms` combine `Factors` by adding or subtracting. Addition has these meanings for different types:

- Arithmetic addition for numeric types (section [#sec-numeric-types]).
- Union for sets and multisets (sections [#sec-sets] and [#sec-multisets])
- Concatenation for sequences (section [#sec-sequences])

Subtraction is arithmetic subtraction for numeric types, and set or multiset difference for sets and multisets.

24.7 Factors

```
Factor(allowLemma, allowLambda) =
  UnaryExpression(allowLemma, allowLambda)
  { MulOp UnaryExpression(allowLemma, allowLambda) }
MulOp = ( "*" | "/" | "%" )
```

A `Factor` combines `UnaryExpression`s using multiplication, division, or modulus. For numeric types these are explained in section [#sec-numeric-types].

Only `*` has a non-numeric application. It represents set or multiset intersection as explained in sections [#sec-sets] and [#sec-multisets].

24.8 Unary Expressions

```
UnaryExpression(allowLemma, allowLambda) =
  ( "-" UnaryExpression(allowLemma, allowLambda)
  | "!" UnaryExpression(allowLemma, allowLambda)
  | PrimaryExpression_(allowLemma, allowLambda)
  )
```

A `UnaryExpression` applies either numeric (section [#sec-numeric-types]) or logical (section [#sec-booleans]) negation to its operand.

24.9 Primary Expressions

```
PrimaryExpression_(allowLemma, allowLambda) =
  ( NameSegment { Suffix }
  | LambdaExpression(allowLemma)
  | MapDisplayExpr { Suffix }
  | SeqDisplayExpr { Suffix }
  | SetDisplayExpr { Suffix }
  | MultiSetExpr { Suffix }
  | EndlessExpression(allowLemma, allowLambda)
  | ConstAtomExpression { Suffix }
  )
```

After descending through all the binary and unary operators we arrive at the primary expressions which are explained in subsequent sections. As can be seen, a number of these can be followed by 0 or more `Suffix`es to select a component of the value.

If the `allowLambda` is false then `LambdaExpression`s are not recognized in this context.

24.10 Lambda expressions

```
LambdaExpression(allowLemma) =
  ( WildIdent
  | "(" [ IdentTypeOptional { "," IdentTypeOptional } ] ")"
  )
  LambdaSpec_
  "=>" Expression(allowLemma, allowLambda: true)
```

See section [#sec-lambda-specification] for a description of `LambdaSpec`.

In addition to named functions, Dafny supports expressions that define functions. These are called *lambda (expression)s* (some languages know them as *anonymous functions*). A lambda expression has the form:

```
(\(_params_\)) \(_specification_\) => \(_body_\)
```

where `\(_params_\)` is a comma-delimited list of parameter declarations, each of which has the form `x` or `x: T`. The type `T` of a parameter can be omitted when it can be inferred. If the identifier `x` is not needed, it can be replaced by "`_`". If `\(_params_\)` consists of a single parameter `x` (or `_`) without an explicit type, then the parentheses can be dropped; for example, the function that returns the successor of a given integer can be written as the following lambda expression:

```
x => x + 1
```

The `\(_specification_\)` is a list of clauses `requires E` or `reads W`, where `E` is a boolean expression and `W` is a frame expression.

`\(_body_\)` is an expression that defines the function's return value. The body must be well-formed for all possible values of the parameters that satisfy the precondition (just like the bodies of named functions and methods). In some cases, this means it is necessary to write explicit `requires` and `reads` clauses. For example, the lambda expression

```
x requires x != 0 => 100 / x
```

would not be well-formed if the `requires` clause were omitted, because of the possibility of division-by-zero.

In settings where functions cannot be partial and there are no restrictions on reading the heap, the *eta expansion* of a function `F: T -> U` (that is, the wrapping of `F` inside a lambda expression in such a way that the lambda expression is equivalent to `F`) would be written `x => F(x)`. In Dafny, eta expansion must also account for the precondition and reads set of the function, so the eta expansion of `F` looks like:

```
x requires F.requires(x) reads F.reads(x) => F(x)
```

24.11 Left-Hand-Side Expressions

```
Lhs =
  ( NameSegment { Suffix }
  | ConstAtomExpression Suffix { Suffix }
  )
```

A left-hand-side expression is only used on the left hand side of an `UpdateStmt`.

An example of the first (`NameSegment`) form is:

```
    LibraryModule.F().x
```

An example of the second (`ConstAtomExpression`) form is:

```
    old(o.f).x
```

24.12 Right-Hand-Side Expressions

```
Rhs =
  ( ArrayAllocation_
  | ObjectAllocation_
  | Expression(allowLemma: false, allowLambda: true)
  | HavocRhs_
  )
  { Attribute }
```

An `Rhs` is either array allocation, an object allocation, an expression, or a havoc right-hand-side, optionally followed by one or more `Attribute`s.

Right-hand-side expressions appear in the following constructs: `ReturnStmt`, `YieldStmt`, `UpdateStmt`, or `VarDeclStatement`. These are the only contexts in which arrays or objects may be allocated, or in which havoc may be produced.

24.13 Array Allocation

```
ArrayAllocation_ = "new" Type "[" Expressions "]"
```

This allocates a new single or multi-dimensional array as explained in section [#sec-array-types].

TO BE WRITTEN - argument that describes how to initialize the array

24.14 Object Allocation

```
ObjectAllocation_ = "new" Type [ "(" [ Expressions ] ")" ]
```

This allocated a new object of a class type as explained in section [#sec-class-types].

24.15 Havoc Right-Hand-Side

```
HavocRhs_ = "*"
```

A havoc right-hand-side produces an arbitrary value of its associated type. To get a more constrained arbitrary value the "assign-such-that" operator (`:|`) can be used. See section [#sec-update-and-call-statements].

24.16 Constant Or Atomic Expressions

```
ConstAtomExpression =
  ( LiteralExpression_
  | FreshExpression_
  | OldExpression_
  | CardinalityExpression_
  | NumericConversionExpression_
  | ParensExpression
  )
```

A `ConstAtomExpression` represent either a constant of some type, or an atomic expression. A `ConstAtomExpression` is never an l-value. ## Literal Expressions

```
LiteralExpression_ =
 ( "false" | "true" | "null" | Nat | Dec |
   charToken | stringToken | "this")
```

A literal expression is a boolean literal, a null object reference, an unsigned integer or real literal, a character or string literal, or "this" which denote the current object in the context of an instance method or function.

24.17 Fresh Expressions

```
FreshExpression_ = "fresh" "(" Expression(allowLemma: true, allowLambda: true) ")"
```

`fresh(e)` returns a boolean value that is true if the objects referenced in expression `e` were all freshly allocated in the current method invocation. The argument of `fresh` must be either an object reference or a collection of object references.

24.18 Allocated expression

TO BE WRITTEN – allocated predicate

24.19 Old and Old@ Expressions

```
OldExpression_ = "old" [ "@" ident ] "(" Expression(allowLemma: true, allowLambda: true) ")"
```

An *old expression* is used in postconditions or in the body of a method or in the body or specification of any two-state function or two-state lemma; an *old* expression with a label is used only in the body of a method at a point where the label dominates its use in this expression.

`old(e)` evaluates the argument using the value of the heap on entry to the method; `old@ident(e)` evaluates the argument using the value of the heap at the given statement label.

Note that **old** and **old@** only affect heap dereferences, like `o.f` and `a[i]`. In particular, neither form has any effect on the value returned for local variables or out-parameters (as they are not on the heap).[14] If the value of an entire expression at a particular point in the method body is needed later on in the method body, the clearest means is to declare a ghost variable, initializing it to the expression in question.

The argument of an `old` expression may not contain nested `old`, `fresh`, or `unchanged` expressions, nor two-state functions or two-state lemmas.

Here are some explanatory examples. All `assert` statements verify to be true.

```
class A {

  var value: int

  method m(i: int)
    requires i == 6
    requires value == 42
    modifies this
  {
    var j: int := 17;
    value := 43;
    label L:
    j := 18;
    value := 44;
    label M:
    assert old(i) == 6; // i is local, but can't be changed anyway
    assert old(j) == 18; // j is local and not affected by old
    assert old@L(j) == 18; // j is local and not affected by old
    assert old(value) == 42;
    assert old@L(value) == 43;
    assert old@M(value) == 44 && this.value == 44;
```

[14] The semantics of `old` in dafny differs from similar constructs in other specification languages like ACSL or JML.

```
    // value is this.value; 'this' is the same
    // same reference in current and pre state but the
    // values stored in the heap as its fields are different;
    // '.value' evaluates to 42 in the pre-state, 43 at L,
    // and 44 in the current state
  }
}
```

```
class A {
  var value: int
  constructor ()
     ensures value == 10
  {
     value := 10;
  }
}

class B {
   var a: A
   constructor () { a := new A(); }

   method m()
     requires a.value == 11
     modifies this, this.a
   {
     label L:
     a.value := 12;
     label M:
     a := new A(); // Line X
     label N:
     a.value := 20;
     label P:

     assert old(a.value) == 11;
     assert old(a).value == 12; // this.a is from pre-state,
                                // but .value in current state
     assert old@L(a.value) == 11;
     assert old@L(a).value == 12; // same as above
     assert old@M(a.value) == 12; // .value in M state is 12
     assert old@M(a).value == 12;
     assert old@N(a.value) == 10; // this.a in N is the heap
                                  // reference at Line X
     assert old@N(a).value == 20; // .value in current state is 20
     assert old@P(a.value) == 20;
     assert old@P(a).value == 20;
```

```
  }
}
```

The next example demonstrates the interaction between `old` and array elements.

```
class A {
  var z1: array<nat>
  var z2: array<nat>

  method mm()
    requires z1.Length > 10 && z1[0] == 7
    requires z2.Length > 10 && z2[0] == 17
    modifies z2
  {
    var a: array<nat> := z1;
    assert a[0] == 7;
    a := z2;
    assert a[0] == 17;
    assert old(a[0]) == 17; // a is local with value z2
    z2[0] := 27;
    assert old(a[0]) == 17; // a is local, with current value of
                            // z2; in pre-state z2[0] == 17
    assert old(a)[0] == 27; // a is local, with current value of
                            // z2; z2[0] is currently 27
  }
}
```

24.20 Unchanged Expressions

TO BE WRITTEN – including with labels

24.21 Cardinality Expressions

```
CardinalityExpression_ = "|" Expression(allowLemma: true, allowLambda: true) "|"
```

For a finite-collection expression `c`, `|c|` is the cardinality of `c`. For a finite set or sequence, the cardinality is the number of elements. For a multiset, the cardinality is the sum of the multiplicities of the elements. For a finite map, the cardinality is the cardinality of the domain of the map. Cardinality is not defined for infinite sets or infinite maps. For more, see section [#sec-collection-types].

24.22 Numeric Conversion Expressions

```
NumericConversionExpression_ =
    ( "int" | "real" ) "(" Expression(allowLemma: true, allowLambda: true) ")"
```

Numeric conversion expressions give the name of the target type followed by the expression being converted in parentheses. This production is for `int` and `real` as the target types but this also applies more generally to other numeric types, e.g. `newtypes`. See section [#sec-numeric-conversion-operations].

24.23 Parenthesized Expression

```
ParensExpression =
  "(" [ Expressions ] ")"
```

A `ParensExpression` is a list of zero or more expressions enclosed in parentheses.

If there is exactly one expression enclosed then the value is just the value of that expression.

If there are zero or more than one, the result is a `tuple` value. See section [#sec-tuple-types].

24.24 Sequence Display Expression

```
SeqDisplayExpr = "[" [ Expressions ] "]"
```

A sequence display expression provide a way to constructing a sequence with given values. For example

```
[1, 2, 3]
```

is a sequence with three elements in it. See section [#sec-sequences] for more information on sequences.

24.25 Set Display Expression

```
SetDisplayExpr = [ "iset" ] "{" [ Expressions ] "}"
```

A set display expression provides a way of constructing a set with given elements. If the keyword `iset` is present, then a potentially infinite set (with the finiite set of given elements) is constructed.

For example

```
{1, 2, 3}
```

is a set with three elements in it. See section [#sec-sets] for more information on sets.

TO BE WRITTEN - use of initializing display expression in new-array allocation

24.26 Multiset Display or Cast Expression

```
MultiSetExpr =
    "multiset"
    ( "{" [ Expressions ] "}"
    | "(" Expression(allowLemma: true, allowLambda: true) ")"
    )
```

A multiset display expression provides a way of constructing a multiset with given elements and multiplicities. For example

```
multiset{1, 1, 2, 3}
```

is a multiset with three elements in it. The number 1 has a multiplicity of 2, the others a multiplicity of 1.

On the other hand, a multiset cast expression converts a set or a sequence into a multiset as shown here:

```
var s : set<int> := {1, 2, 3};
var ms : multiset<int> := multiset(s);
ms := ms + multiset{1};
var sq : seq<int> := [1, 1, 2, 3];
var ms2 : multiset<int> := multiset(sq);
assert ms == ms2;
```

See section [#sec-multisets] for more information on multisets.

24.27 Map Display Expression

```
MapDisplayExpr = ("map" | "imap" ) "[" [ MapLiteralExpressions ] "]"
MapLiteralExpressions =
    Expression(allowLemma: true, allowLambda: true)
    ":=" Expression(allowLemma: true, allowLambda: true)
    { "," Expression(allowLemma: true, allowLambda: true)
          ":=" Expression(allowLemma: true, allowLambda: true)
    }
```

A map display expression builds a finite or potentially infinite map from explicit `MapLiteralExpressions`. For example:

```
var m := map[1 := "a", 2 := "b"];
ghost var im := imap[1 := "a", 2 := "b"];
```

See section [#sec-finite-and-infinite-maps] for more details on maps and imaps.

24.28 Endless Expression

```
EndlessExpression(allowLemma, allowLambda) =
  ( IfExpression_(allowLemma, allowLambda)
  | MatchExpression(allowLemma, allowLambda)
  | QuantifierExpression(allowLemma, allowLambda)
  | SetComprehensionExpr(allowLemma, allowLambda)
  | StmtInExpr Expression(allowLemma, allowLambda)
  | LetExpr(allowLemma, allowLambda)
  | MapComprehensionExpr(allowLemma, allowLambda)
  )
```

`EndlessExpression` gets it name from the fact that all its alternate productions have no terminating symbol to end them, but rather they all end with an `Expression` at the end. The various `EndlessExpression` alternatives are described below.

24.29 If Expression

```
IfExpression_(allowLemma, allowLambda) =
    "if" Expression(allowLemma: true, allowLambda: true)
    "then" Expression(allowLemma: true, allowLambda: true)
    "else" Expression(allowLemma, allowLambda)
```

The `IfExpression` is a conditional expression. It first evaluates the expression following the `if`. If it evaluates to `true` then it evaluates the expression following the `then` and that is the result of the expression. If it evaluates to `false` then the expression following the `else` is evaluated and that is the result of the expression. It is important that only the selected expression is evaluated as the following example shows.

```
var k := 10 / x; // error, may divide by 0.
var m := if x != 0 then 10 / x else 1; // ok, guarded
```

24.30 Binding If Expression

TO BE WRITTEN

24.31 Case Bindings, Patterns, and Extended Patterns

```
CaseBinding_ =
  "case"
  ( ExtendedPattern
  | "(" [ ExtendedPattern { "," ExtendedPattern } ] ")"
  )

CasePattern =
  ( Ident "(" [ CasePattern { "," CasePattern } ] ")"
  | "(" [ CasePattern { "," Casepattern } ] ")"
  | IdentTypeOptional
  )


ExtendedPattern =
  ( LiteralExpression_
  ( Ident [ "(" ExtendedPattern { "," ExtendedPattern } ")" ]
```

Case bindings and extended patterns are used for (possibly nested) pattern matching on inductive, coinductive or base type values. The `CaseBinding_` construct is used in `CaseStatement` and `CaseExpression`s. `CasePattern`s are used in `LetExpr`s and `VarDeclStatement`s.

When matching an inductive or coinductive value in a `MatchStmt` or `MatchExpression`, the `ExtendedPattern` must either correspond to a constructor of the type of the value, or a bound variable. A tuple is considered to have a single constructor. The `Ident` of the `CaseBinding_` must either match the name of a constructor (or in the case of a tuple, the `Ident` is absent and the second alternative is chosen), or not be applied to a tuple of `ExtendedPattern`. The `ExtendedPattern`s inside the parentheses are then matched against the arguments that were given to the constructor when the value was constructed. The number of `ExtendedPattern` must match the number of parameters to the constructor (or the arity of the tuple). When matching a value of base type, the `ExtendedPattern` should either be a `LiteralExpression_` of the same type as the value, or a single identifier matching all values of this type.

The `CasePattern`s may be nested. The set of non-constructor-name identifiers contained in a `CaseBinding_` must be distinct. They are bound to the corresponding values in the value being matched.

24.32 Match Expression

```
MatchExpression(allowLemma, allowLambda) =
  "match" Expression(allowLemma, allowLambda)
  ( "{" { CaseExpression(allowLemma: true, allowLambda: true) } "}"
  | { CaseExpression(allowLemma, allowLambda) }
  )

CaseExpression(allowLemma, allowLambda) =
    CaseBinding_ "=>" Expression(allowLemma, allowLambda)
```

A `MatchExpression` is used to conditionally evaluate and select an expression depending on the value of an algebraic type, i.e. an inductive type, a co-inductive type, or a base type.

The `Expression` following the `match` keyword is called the *selector*. The selector is evaluated and then matched against each `CaseExpression` in order until a matching clause is found. An `Ident` following the `case` keyword in a `CaseExpression` is either the name of a constructor of the selector's type, or a bound variable. It may be absent if the expression being matched is a tuple since these have no constructor name.

If the constructor has parameters then in the `CaseExpression` the constructor name must be followed by a parenthesized list of `CasePatterns` with one `CasePattern` for each constructor parameter.

If the constructor has no parameters then the `CaseExpression` must not have a following `CasePattern` list (though optional empty parentheses are allowed).

All of the variables in the `CasePatterns` must be distinct. If types for the identifiers are not given then types are inferred from the types of the constructor's parameters. If types are given then they must agree with the types of the corresponding parameters.

A `MatchExpression` is evaluated by first evaluating the selector. The `ExtendedPattern` of each `CaseClause` are then compared in order with the resulting value until a matching pattern is found. If the constructor had parameters then the actual values used to construct the selector value are bound to the identifiers in the identifier list. The expression to the right of the `=>` in the `CaseClause` is then evaluated in the environment enriched by this binding. The result of that evaluation is the result of the `MatchExpression`.

Note that the braces enclosing the `CaseClauses` may be omitted.

24.33 Quantifier Expression

```
QuantifierExpression(allowLemma, allowLambda) =
    ( "forall" | "exists" ) QuantifierDomain "::"
    Expression(allowLemma, allowLambda)

QuantifierDomain =
  IdentTypeOptional { "," IdentTypeOptional } { Attribute }
  [ "|" Expression(allowLemma: true, allowLambda: true) ]
```

A `QuantifierExpression` is a boolean expression that specifies that a given expression (the one following the `::`) is true for all (for **forall**) or some (for **exists**) combination of values of the quantified variables, namely those in the `QuantifierDomain`.

Here are some examples:

```
assert forall x : nat | x <= 5 :: x * x <= 25;
(forall n :: 2 <= n ==> (exists d :: n < d < 2*n))
```

or using the Unicode symbols:

The quantifier identifiers are *bound* within the scope of the expressions in the `QuantifierExpression`.

If types are not given for the quantified identifiers, then Dafny attempts to infer their types from the context of the expressions. It this is not possible, the program is in error.

24.34 Set Comprehension Expressions

```
SetComprehensionExpr(allowLemma, allowLambda) =
  [ "set" | "iset" ]
  IdentTypeOptional { "," IdentTypeOptional } { Attribute }
  "|" Expression(allowLemma, allowLambda)
  [ "::" Expression(allowLemma, allowLambda) ]
```

A set comprehension expression is an expressions that yields a set (possibly infinite if `iset` is used) that satisfies specified conditions. There are two basic forms.

If there is only one quantified variable, the optional `"::" Expression` need not be supplied, in which case it is as if it had been supplied and the expression consists solely of the quantified variable. That is,

```
set x : T | P(x)
```

is equivalent to

```
set x : T | P(x) :: x
```

For the full form

```
var S := set x1:T1, x2:T2 ... | P(x1, x2, ...) :: Q(x1, x2, ...)
```

the elements of `S` will be all values resulting from evaluation of `Q(x1, x2, ...)` for all combinations of quantified variables `x1, x2, ...` such that predicate `P(x1, x2, ...)` holds. For example,

```
var S := set x:nat, y:nat | x < 2 && y < 2 :: (x, y)
```

yields `S == {(0, 0), (0, 1), (1, 0), (1,1) }`

The types on the quantified variables are optional and if not given Dafny will attempt to infer them from the contexts in which they are used in the `P` or `Q` expressions.

If a finite set was specified ("set" keyword used), Dafny must be able to prove that the result is finite otherwise the set comprehension expression will not be accepted.

Set comprehensions involving reference types such as

```
set o: object | true
```

are allowed in ghost contexts. In particular, in ghost contexts, the check that the result is finite should allow any set comprehension where the bound variable is of a reference type. In non-ghost contexts, it is not allowed, because–even though the resulting set would be finite–it is not pleasant or practical to compute at run time.

24.35 Statements in an Expression

```
StmtInExpr = ( AssertStmt | AssumeStmt | ExpectStmt | CalcStmt )
```

A `StmtInExpr` is a kind of statement that is allowed to precede an expression in order to ensure that the expression can be evaluated without error. For example:

```
assume x != 0; 10/x
```

`Assert`, `assume` and `calc` statements can be used in this way.

24.36 Let Expression

```
LetExpr(allowLemma, allowLambda) =
    [ "ghost" ] "var" CasePattern { "," CasePattern }
    ( ":=" | { Attribute } ":|" )
    Expression(allowLemma: false, allowLambda: true)
    { "," Expression(allowLemma: false, allowLambda: true) } ";"
    Expression(allowLemma, allowLambda)
```

A `let` expression allows binding of intermediate values to identifiers for use in an expression. The start of the `let` expression is signaled by the `var` keyword. They look much like a local variable declaration except the scope of the variable only extends to the enclosed expression.

For example:

```
var sum := x + y; sum * sum
```

In the simple case, the `CasePattern` is just an identifier with optional type (which if missing is inferred from the rhs).

The more complex case allows destructuring of constructor expressions. For example:

```
datatype Stuff = SCons(x: int, y: int) | Other
function GhostF(z: Stuff): int
  requires z.SCons?
{
  var SCons(u, v) := z; var sum := u + v; sum * sum
}
```

24.37 Map Comprehension Expression

```
MapComprehensionExpr(allowLemma, allowLambda) =
  ( "map" | "imap" ) IdentTypeOptional { Attribute }
  [ "|" Expression(allowLemma: true, allowLambda: true) ]
  "::" Expression(allowLemma, allowLambda)
```

A `MapComprehensionExpr` defines a finite or infinite map value by defining a domain (using the `IdentTypeOptional` and the optional condition following the "|") and for each value in the domain, giving the mapped value using the expression following the "::".

For example:

```
function square(x : int) : int { x * x }
method test()
{
```

```
  var m := map x : int | 0 <= x <= 10 :: x * x;
  ghost var im := imap x : int :: x * x;
  ghost var im2 := imap x : int :: square(x);
}
```

Dafny finite maps must be finite, so the domain must be constrained to be finite. But imaps may be infinite as the example shows. The last example shows creation of an infinite map that gives the same results as a function.

24.38 Name Segment

```
NameSegment = Ident [ GenericInstantiation | HashCall ]
```

A `NameSegment` names a Dafny entity by giving its declared name optionally followed by information to make the name more complete. For the simple case, it is just an identifier.

If the identifier is for a generic entity, it is followed by a `GenericInstantiation` which provides actual types for the type parameters.

To reference a prefix predicate (see section [#sec-copredicates]) or prefix lemma (see section [#sec-prefix-lemmas]), the identifier must be the name of the co-predicate or colemma and it must be followed by a `HashCall`.

24.39 Hash Call

```
HashCall = "#" [ GenericInstantiation ]
  "[" Expression(allowLemma: true, allowLambda: true) "]"
  "(" [ Expressions ] ")"
```

A `HashCall` is used to call the prefix for a copredicate or colemma. In the non-generic case, just insert `"#[k]"` before the call argument list where k is the number of recursion levels.

In the case where the `colemma` is generic, the generic type argument is given before. Here is an example:

```
codatatype Stream<T> = Nil | Cons(head: int, stuff: T, tail: Stream)

function append(M: Stream, N: Stream): Stream
{
  match M
  case Nil => N
  case Cons(t, s, M') => Cons(t, s, append(M', N))
}
```

```
function zeros<T>(s : T): Stream<T>
{
  Cons(0, s, zeros(s))
}

function ones<T>(s: T): Stream<T>
{
  Cons(1, s, ones(s))
}

copredicate atmost(a: Stream, b: Stream)
{
  match a
  case Nil => true
  case Cons(h,s,t) => b.Cons? && h <= b.head && atmost(t, b.tail)
}

colemma {:induction false} Theorem0<T>(s: T)
  ensures atmost(zeros(s), ones(s))
{
  // the following shows two equivalent ways to getting essentially the
  // co-inductive hypothesis
  if (*) {
    Theorem0#<T>[_k-1](s);
  } else {
    Theorem0(s);
  }
}
```

where the `HashCall` is `"Theorem0#<T>[_k-1](s);"`. See sections [#sec-copredicates] and [#sec-prefix-lemmas].

24.40 Suffix

```
Suffix =
  ( AugmentedDotSuffix_
  | DatatypeUpdateSuffix_
  | SubsequenceSuffix_
  | SlicesByLengthSuffix_
  | SequenceUpdateSuffix_
  | SelectionSuffix_
  | ArgumentListSuffix_
  )
```

The `Suffix` non-terminal describes ways of deriving a new value from the en-

tity to which the suffix is appended. There are six kinds of suffixes which are described below.

24.40.1 Augmented Dot Suffix

```
AugmentedDotSuffix_ = ". " DotSuffix [ GenericInstantiation | HashCall ]
```

An augmented dot suffix consists of a simple `DotSuffix` optionally followed by either

- a `GenericInstantiation` (for the case where the item selected by the `DotSuffix` is generic), or
- a `HashCall` for the case where we want to call a prefix copredicate or colemma. The result is the result of calling the prefix copredicate or colemma.

24.40.2 Datatype Update Suffix

```
DatatypeUpdateSuffix_ =
  "." "(" MemberBindingUpdate { "," MemberBindingUpdate } ")"

MemberBindingUpdate =
  ( ident | digits ) ":=" Expression(allowLemma: true, allowLambda: true)
```

A datatype update suffix is used to produce a new datatype value that is the same as an old datatype value except that the value corresponding to a given destructor has the specified value. In a `MemberBindingUpdate`, the `ident` or `digits` is the name of a destructor (i.e. formal parameter name) for one of the constructors of the datatype. The expression to the right of the `:=` is the new value for that formal.

All of the destructors in a `DatatypeUpdateSuffix_` must be for the same constructor, and if they do not cover all of the destructors for that constructor then the datatype value being updated must have a value derived from that same constructor.

Here is an example:

```
module NewSyntax {
datatype MyDataType = MyConstructor(myint:int, mybool:bool)
                    | MyOtherConstructor(otherbool:bool)
                    | MyNumericConstructor(42:int)

method test(datum:MyDataType, x:int)
    returns (abc:MyDataType, def:MyDataType, ghi:MyDataType, jkl:MyDataType)
    requires datum.MyConstructor?;
    ensures abc == datum.(myint := x + 2);
```

```
    ensures def == datum.(otherbool := !datum.mybool);
    ensures ghi == datum.(myint := 2).(mybool := false);
    // Resolution error: no non_destructor in MyDataType
    //ensures jkl == datum.(non_destructor := 5);
    ensures jkl == datum.(42 := 7);
{
    abc := MyConstructor(x + 2, datum.mybool);
    abc := datum.(myint := x + 2);
    def := MyOtherConstructor(!datum.mybool);
    ghi := MyConstructor(2, false);
    jkl := datum.(42 := 7);

    assert abc.(myint := abc.myint - 2) == datum.(myint := x);
}
}
```

24.40.3 Subsequence Suffix

```
SubsequenceSuffix_ =
  "[" [ Expression(allowLemma: true, allowLambda: true) ]
      ".." [ Expression(allowLemma: true, allowLambda: true) ]
  "]"
```

A subsequence suffix applied to a sequence produces a new sequence whose elements are taken from a contiguous part of the original sequence. For example, expression `s[lo..hi]` for sequence `s`, and integer-based numerics `lo` and `hi` satisfying `0 <= lo <= hi <= |s|`. See section [#sec-other-sequence-expressions] for details.

24.40.4 Slices By Length Suffix

```
SlicesByLengthSuffix_ =
  "[" Expression(allowLemma: true, allowLambda: true) ":"
      [
        Expression(allowLemma: true, allowLambda: true)
        { ":" Expression(allowLemma: true, allowLambda: true) }
        [ ":" ]
      ]
  "]"
```

Applying a `SlicesByLengthSuffix_` to a sequence produces a sequence of subsequences of the original sequence. See section [#sec-other-sequence-expressions] for details.

24.40.5 Sequence Update Suffix

```
SequenceUpdateSuffix_ =
  "[" Expression(allowLemma: true, allowLambda: true)
      ":=" Expression(allowLemma: true, allowLambda: true)
  "]"
```

For a sequence `s` and expressions `i` and `v`, the expression `s[i := v]` is the same as the sequence `s` except that at index `i` it has value `v`.

If the type of `s` is `seq<T>`, then `v` must have type `T`. The index `i` can have any integer- and bitvector-based type. The expression `s[i := v]` has the same type as `s`.

24.40.6 Selection Suffix

```
SelectionSuffix_ =
  "[" Expression(allowLemma: true, allowLambda: true)
      { "," Expression(allowLemma: true, allowLambda: true) }
  "]"
```

If a `SelectionSuffix_` has only one expression in it, it is a zero-based index that may be used to select a single element of a sequence or from a single-dimensional array.

If a `SelectionSuffix_` has more than one expression in it, then it is a list of indices to index into a multi-dimensional array. The rank of the array must be the same as the number of indices.

If the `SelectionSuffix_` is used with an array or a sequence, then each index expression can have any integer- or bitvector-based type.

24.40.7 Argument List Suffix

```
ArgumentListSuffix_ = "(" [ Expressions ] ")"
```

An argument list suffix is a parenthesized list of expressions that are the arguments to pass to a method or function that is being called. Applying such a suffix causes the method or function to be called and the result is the result of the call.

24.41 Expression Lists

```
Expressions =
    Expression(allowLemma: true, allowLambda: true)
    { "," Expression(allowLemma: true, allowLambda: true) }
```

The `Expressions` non-terminal represents a list of one or more expressions separated by a comma.

24.42 Compile-Time Constants

In certain situations in Dafny it is helpful to know what the value of a constant is during program analysis, before verification or execution takes place. For example, a compiler can choose an optimized representation of a `newtype` that is a subset of `int` if it knows the range of possible values of the subset type: if the range is within 0 to less than 256, then an unsigned 8-bit representation can be used.

To continue this example, suppose a new type is defined as

```
const MAX := 47
newtype mytype = x | 0 <= x < MAX*4
```

In this case, we would prefer that Dafny recognize that `MAX*4` is known to be constant with a value of `188`. The kinds of expressions for which such an optimization is possible are called *compile-time constants*. Note that the representation of `mytype` makes no difference semantically, but can affect how compiled code is represented at run time. In addition, though, using a symbolic constant (which may well be used elsewhere as well) improves the self-documentation of the code.

In Dafny, the following expressions are compile-time constants[15], recursively (that is, the arguments of any operation must themselves be compile-time constants): - int, bitvector, real, boolean, char and string literals - int operations: `+ - * / %` and unary `-` and comparisons `< <= > >= == !=` - real operations: `+ - *` and unary `-` and comparisons `< <= > >= == !=' - bool operations:`&& || ==> <== <==> == !=`and unary '!' - bitvector operations:`+ - * / % « » & | ^`and unary! -and comparisons`< <= > >= == !=- char operations:< <= > >= == !=- string operations: length:|…|, concatenation:+, comparisons< <= == !=, indexing[]- conversions between: int real char bitvector - newtype operations: newtype arguments, but not newtype results - symbolic values that are declared`const‘ and have an explicit initialization value that is a compile-time constant - conditional (if-then-else) expressions - parenthesized expressions

24.43 Map comprehensions

TO BE WRITTEN

[15] This set of operations that are constant-folded may be enlarged in future versions of Dafny.

25 Variable Initialization and Definite Assignment

TO BE WRITTEN – rules for default initialization; resulting rules for constructors; definite assignment rules

26 Well-founded Orders

TODO: Write this section

27 Module Refinement

TODO: Write this section.

28 Attributes

```
Attribute = "{" ":" AttributeName [ Expressions ] "}"
```

Dafny allows many of its entities to be annotated with *Attributes*. The grammar shows where the attribute annotations may appear.

Here is an example of an attribute from the Dafny test suite:

```
{:MyAttribute "hello", "hi" + "there", 57}
```

In general an attribute may have any name the user chooses. It may be followed by a comma separated list of expressions. These expressions will be resolved and type-checked in the context where the attribute appears.

28.1 Dafny Attribute Implementation Details

In the Dafny implementation the `Attributes` type holds the name of the attribute, a list of `Expression` arguments and a link to the previous Attributes object for that Dafny entity. So for each Dafny entity that has attributes we have a list of them.

Dafny stores attributes on the following kinds of entities: Declaration (base class), ModuleDefinition, Statement, AssignmentRhs, LocalVariable, LetExpr, ComprehensionExpr, MaybeFreeExpression, Specification.

TODO: Dafny internals information should go into a separate document on Dafny internals.

28.2 Dafny Attributes

All entities that Dafny translates to Boogie have their attributes passed on to Boogie except for the `{:axiom}` attribute (which conflicts with Boogie usage) and the `{:trigger}` attribute which is instead converted into a Boogie quantifier *trigger*. See Section 11 of [@Leino:Boogie2-RefMan].

Dafny has special processing for some attributes. For some attributes, the setting is only looked for on the entity with the attribute. For others, we start at the entity and if the attribute is not there, look up in the hierarchy (enclosing class and enclosing modules). The latter case is checked by the `ContainsBoolAtAnyLevel` method in the Dafny source. The attribute declaration closest to the entity overrides those further away.

For attributes with a single boolean expression argument, the attribute with no argument is interpreted as if it were true.

The attributes that are processed specially by Dafny are described in the following sections.

28.2.1 assumption

This attribute can only be placed on a local ghost bool variable of a method. Its declaration cannot have a rhs, but it is allowed to participate as the lhs of exactly one assignment of the form: `b := b && expr;`. Such a variable declaration translates in the Boogie output to a declaration followed by an `assume b` command. See [@LeinoWuestholz2015], Section 3, for example uses of the `{:assumption}` attribute in Boogie.

28.2.2 autoReq boolExpr

For a function declaration, if this attribute is set true at the nearest level, then its `requires` clause is strengthed sufficiently so that it may call the functions that it calls.

For following example

```
function f(x:int) : bool
  requires x > 3
{
  x > 7
}

// Should succeed thanks to auto_reqs
function {:autoReq} g(y:int, b:bool) : bool
{
  if b then f(y + 2) else f(2*y)
}
```

the `{:autoReq}` attribute causes Dafny to deduce a `requires` clause for g as if it had been declared

```
function g(y:int, b:bool) : bool
  requires if b then y + 2 > 3 else 2 * y > 3
{
  if b then f(y + 2) else f(2*y)
}
```

28.2.3 autocontracts

Dynamic frames [@Kassios:FM2006;@SmansEtAl:VeriCool;@SmansEtAl:ImplicitDynamicFrames; @LEINO:Dafny:DynamicFrames] are frame expressions that can vary dynamically during program execution. AutoContracts is an experimental feature that will fill much of the dynamic-frames boilerplate into a class.

From the user's perspective, what needs to be done is simply:

- mark the class with {:autocontracts}
- declare a function (or predicate) called Valid()

AutoContracts will then:

- Declare:

```
ghost var Repr: set<object>
```

- For function/predicate Valid(), insert:

```
reads this, Repr
```

- Into body of Valid(), insert (at the beginning of the body):

```
this in Repr && null !in Repr
```

- and also insert, for every array-valued field A declared in the class:

```
(A != null ==> A in Repr) &&
```

- and for every field F of a class type T where T has a field called Repr, also insert:

```
(F != null ==> F in Repr && F.Repr <= Repr && this !in Repr)
```

Except, if A or F is declared with `{:autocontracts false}`, then the implication will not be added.

- For every constructor, add:

```
modifies this
ensures Valid() && fresh(Repr - {this})
```

- At the end of the body of the constructor, add:

```
Repr := {this};
if (A != null) { Repr := Repr + {A}; }
if (F != null) { Repr := Repr + {F} + F.Repr; }
```

- For every method, add:

```
requires Valid()
modifies Repr
ensures Valid() && fresh(Repr - old(Repr))
```

- At the end of the body of the method, add:

```
if (A != null) { Repr := Repr + {A}; }
if (F != null) { Repr := Repr + {F} + F.Repr; }
```

28.2.4 axiom

The `{:axiom}` attribute may be placed on a function or method. It means that the post-condition may be assumed to be true without proof. In that case also the body of the function or method may be omitted.

The `{:axiom}` attribute is also used for generated `reveal_*` lemmas as shown in Section [#sec-opaque].

28.2.5 compile

The `{:compile}` attribute takes a boolean argument. It may be applied to any top-level declaration. If that argument is false, then that declaration will not be compiled into .Net code.

28.2.6 decl

The `{:decl}` attribute may be placed on a method declaration. It inhibits the error message that has would be given when the method has an `ensures` clauses but no body. It has been used to declare Dafny interfaces in the MSR IronClad and IronFleet projects. Instead the `extern` keyword should be used (but that is soon to be replaced by the `{:extern}` attribute).

28.2.7 fuel

The fuel attributes is used to specify how much "fuel" a function should have, i.e., how many times Z3 is permitted to unfold it's definition. The new {:fuel} annotation can be added to the function itself, it which case it will apply to all uses of that function, or it can overridden within the scope of a module, function, method, iterator, calc, forall, while, assert, or assume. The general format is:

```
{:fuel functionName,lowFuel,highFuel}
```

When applied as an annotation to the function itself, omit functionName. If highFuel is omitted, it defaults to lowFuel + 1.

The default fuel setting for recursive functions is 1,2. Setting the fuel higher, say, to 3,4, will give more unfoldings, which may make some proofs go through with less programmer assistance (e.g., with fewer assert statements), but it may also increase verification time, so use it with care. Setting the fuel to 0,0 is similar to making the definition opaque, except when used with all literal arguments.

28.2.8 heapQuantifier

The `{:heapQuantifier}` attribute may be used on a `QuantifierExpression`. When it appears in a quantifier expression, it is as if a new heap-valued quantifier variable was added to the quantification. Consider this code that is one of the invariants of a while loop.

```
invariant forall u {:heapQuantifier} :: f(u) == u + r
```

The quantifier is translated into the following Boogie:

```
(forall q$heap#8: Heap, u#5: int ::
    {:heapQuantifier}
    $IsGoodHeap(q$heap#8) && ($Heap == q$heap#8 || $HeapSucc($Heap, q$heap#8))
       ==> $Unbox(Apply1(TInt, TInt, f#0, q$heap#8, $Box(u#5))): int == u#5 + r#0);
```

What this is saying is that the quantified expression, `f(u) == u + r`, which may depend on the heap, is also valid for any good heap that is either the same as the current heap, or that is derived from it by heap update operations.

28.2.9 imported

If a `MethodDecl` or `FunctionDecl` has an `{:imported}` attribute, then it is allowed to have a empty body even though it has an **ensures** clause. Ordinarily a body would be required in order to provide the proof of the **ensures** clause (but the `(:axiom)` attribute also provides this facility, so the need for `(:imported)` is not clear.) A method or function declaration may be given the `(:imported)` attribute. This suppresses the error message that would be given if a method or function with an `ensures` clause does not have a body.

This seems to duplicate what `extern` and `{:decl}` do and would be a good candidate for deprecation.

28.2.10 induction

The `{:induction}` attribute controls the application of proof by induction to two contexts. Given a list of variables on which induction might be applied, the `{:induction}` attribute selects a sub-list of those variables (in the same order) to which to apply induction.

Dafny issue 34 proposes to remove the restriction that the sub-list be in the same order, and would apply induction in the order given in the `{:induction}` attribute.

The two contexts are:

- A method, in which case the bound variables are all the in-parameters of the method.
- A quantifier expression, in which case the bound variables are the bound variables of the quantifier expression.

The form of the `{:induction}` attribute is one of the following:

- `{:induction}` – apply induction to all bound variables
- `{:induction false}` – suppress induction, that is, don't apply it to any bound variable
- `{:induction L}` where `L` is a list consisting entirely of bound variables – apply induction to the specified bound variables
- `{:induction X}` where `X` is anything else – treat the same as {:induction}, that is, apply induction to all bound variables. For this usage conventionally `X` is `true`.

Here is an example of using it on a quantifier expression:

```
lemma Fill_J(s: seq<int>)
  requires forall i :: 1 <= i < |s| ==> s[i-1] <= s[i]
  ensures forall i,j {:induction j} :: 0 <= i < j < |s| ==> s[i] <= s[j]
{
}
```

28.2.11 layerQuantifier

When Dafny is translating a quantified expression, if it has a `{:layerQuantifier}` attribute an additional quantifier variable is added to the quantifier bound variables. This variable as the predefined *LayerType*. A `{:layerQuantifier}` attribute may be placed on a quantifier expression. Translation of Dafny into Boogie defines a *LayerType* which has defined zero and successor constructors.

The Dafny source has the comment that "if a function is recursive, then make the reveal lemma quantifier a layerQuantifier." And in that case it adds the attribute to the quantifier.

There is no explicit user of the `{:layerQuantifier}` attribute in the Dafny tests. So I believe this attribute is only used internally by Dafny and not externally.

TODO: Need more complete explanation of this attribute. Dafny issue 35 tracks further effort for this attribute.

28.2.12 nativeType

The `{:nativeType}` attribute may only be used on a `NewtypeDecl` where the base type is an integral type. It can take one of the following forms:

- `{:nativeType}` - With no parameters it has no effect and the `NewtypeDecl` have its default behavior which is to choose a native type that can hold any value satisfying the constraints, if possible, otherwise BigInteger is used.
- `{:nativeType true}` - Also gives default `NewtypeDecl` behavior, but gives an error if base type is not integral.
- `{:nativeType false}` - Inhibits using a native type. BigInteger is used for integral types and BitRational for real types.
- `{:nativeType "typename"}` - This form has an native integral type name as a string literal. Acceptable values are: "byte", "sbyte", "ushort", "short", "uint", "int", "ulong" and "long". An error is reported if the given datatype cannot hold all the values that satisfy the constraint.

28.2.13 opaque

Ordinarily the body of a function is transparent to its users but sometimes it is useful to hide it. If a function `f` is given the `{:opaque}` attribute then Dafny hides the body of the function, so that it can only be seen within its recursive clique (if any), or if the programmer specifically asks to see it via the `reveal_f()` lemma.

We create a lemma to allow the user to selectively reveal the function's body That is, given:

```
function {:opaque} foo(x:int, y:int) : int
  requires 0 <= x < 5
  requires 0 <= y < 5
  ensures foo(x, y) < 10
{ x + y }
```

We produce:

```
lemma {:axiom} reveal_foo()
  ensures forall x:int, y:int {:trigger foo(x,y)} ::
       0 <= x < 5 && 0 <= y < 5 ==> foo(x,y) == foo_FULL(x,y)
```

where `foo_FULL` is a copy of `foo` which does not have its body hidden. In addition `foo_FULL` is given the `{:opaque_full}` and `{:auto_generated}` attributes in addition to the `{:opaque}` attribute (which it got because it is a copy of `foo`).

28.2.14 opaque_full

The `{:opaque_full}` attribute is used to mark the *full* version of an opaque function. See Section [#sec-opaque].

28.2.15 tailrecursion

This attribute is used on method declarations. It has a boolean argument.

If specified with a false value, it means the user specifically requested no tail recursion, so none is done.

If specified with a true value, or if no argument is specified, then tail recursive optimization will be attempted subject to the following conditions:

- It is an error if the method is a ghost method and tail recursion was explicitly requested.
- Only direct recursion is supported, not mutually recursive methods.
- If `{:tailrecursion true}` was specified but the code does not allow it, an error message is given.

28.2.16 timeLimitMultiplier

This attribute may be placed on a method or function declaration and has an integer argument. If `{:timeLimitMultiplier X}` was specified a `{:timelimit Y}` attributed is passed on to Boogie where `Y` is `X` times either the default verification time limit for a function or method, or times the value specified by the Boogie `timelimit` command-line option.

28.2.17 trigger

Trigger attributes are used on quantifiers and comprehensions. They are translated into Boogie triggers.

28.2.18 typeQuantifier

The `{:typeQuantifier}` attribute must be used on a quantifier if it quantifies over types.

28.3 Boogie Attributes

Use the Boogie "/attrHelp" option to get the list of attributes that Boogie recognizes and their meaning. Here is the output at the time of this writing. Dafny passes attributes that have been specified to Boogie.

```
Boogie: The following attributes are supported by this implementation.

  ---- On top-level declarations ------------------------------------------

    {:ignore}
      Ignore the declaration (after checking for duplicate names).

    {:extern}
      If two top-level declarations introduce the same name (for example, two
      constants with the same name or two procedures with the same name), then
      Boogie usually produces an error message.  However, if at least one of
      the declarations is declared with :extern, one of the declarations is
      ignored.  If both declarations are :extern, Boogie arbitrarily chooses
      one of them to keep; otherwise, Boogie ignore the :extern declaration
      and keeps the other.

    {:checksum <string>}
      Attach a checksum to be used for verification result caching.

  ---- On implementations and procedures ----------------------------------

     {:inline N}
       Inline given procedure (can be also used on implementation).
       N should be a non-negative number and represents the inlining depth.
       With /inline:assume call is replaced with "assume false" once inlining depth is reach
       With /inline:assert call is replaced with "assert false" once inlining depth is reach
       With /inline:spec call is left as is once inlining depth is reached.
       With the above three options, methods with the attribute {:inline N} are not verified
       With /inline:none the entire attribute is ignored.

     {:verify false}
       Skip verification of an implementation.

     {:vcs_max_cost N}
     {:vcs_max_splits N}
     {:vcs_max_keep_going_splits N}
       Per-implementation versions of
       /vcsMaxCost, /vcsMaxSplits and /vcsMaxKeepGoingSplits.

     {:selective_checking true}
       Turn all asserts into assumes except for the ones reachable from
       assumptions marked with the attribute {:start_checking_here}.
       Thus, "assume {:start_checking_here} something;" becomes an inverse
       of "assume false;": the first one disables all verification before
       it, and the second one disables all verification after.

     {:priority N}
       Assign a positive priority 'N' to an implementation to control the order
       in which implementations are verified (default: N = 1).

     {:id <string>}
       Assign a unique ID to an implementation to be used for verification
       result caching (default: "<impl. name>:0").

     {:timeLimit N}
       Set the time limit for a given implementation
```

However a scan of Boogie's sources shows it checks for the following attributes.

- {:$}
- {:$renamed$}
- {:InlineAssume}
- {:PossiblyUnreachable}
- {:__dominator_enabled}
- {:__enabled}
- {:a##post##}
- {:absdomain}
- {:ah}
- {:assumption}
- {:assumption_variable_initialization}
- {:atomic}
- {:aux}
- {:both}
- {:bvbuiltin}
- {:candidate}
- {:captureState}
- {:checksum}
- {:constructor}
- {:datatype}
- {:do_not_predicate}
- {:entrypoint}
- {:existential}
- {:exitAssert}
- {:expand}
- {:extern}
- {:hidden}
- {:ignore}
- {:inline}
- {:left}
- {:linear}
- {:linear_in}
- {:linear_out}
- {:msg}
- {:name}
- {:originated_from_invariant}
- {:partition}
- {:positive}
- {:post}
- {:pre}
- {:precondition_previous_snapshot}
- {:qid}
- {:right}
- {:selective_checking}

- {:si_fcall}
- {:si_unique_call}
- {:sourcefile}
- {:sourceline}
- {:split_here}
- {:stage_active}
- {:stage_complete}
- {:staged_houdini_tag}
- {:start_checking_here}
- {:subsumption}
- {:template}
- {:terminates}
- {:upper}
- {:verified_under}
- {:weight}
- {:yields}

29 Dafny User's Guide

29.1 Introduction

The dafny tool implements the following capabilities:

- checking that the input files represent a valid dafny program (i.e., syntax, grammar and type checking);
- verifying that the program meets its specifications, by translating the program to verification conditions and checking those with Boogie and an SMT solver, typically Z3;
- compiling the program to a target language, such as C#, Java, Javascript, Go (and others in development);
- running the executable produced by the compiler.

Using various command-line flags, the tool can perform various combinations of the last three actions (the first action is always performed).

The development of the dafny language and tool is a GitHub project at https://github.com/dafny-lang/dafny. The project is open source, with collaborators from various organizations and additional contributors welcome. The software itself is licensed under the MIT license.

29.2 Installing Dafny From Binaries

Windows: To install Dafny on your own machine, download Dafny.zip and **save** it to your disk. Then, before you open or unzip it, right-click on it and select Properties; at the bottom of the dialog, click the Unblock button and then the OK button. Now, open Dafny.zip and copy its contents into a directory on your machine. (You can now delete the Dafny.zip file.)

Then:

- To run Dafny from the command line, simply run Dafny.exe from the `Binaries` directory.
- There is also a Dafny mode for Emacs.

Linux and Mac: Make sure you have Mono version 4. Then save the contents of the Dafny.zip for the appropriate version of your platform. You can now run Dafny from the command line by invoking the script file `dafny`. For an IDE, use the Dafny mode for Emacs.

Mac using brew: On a Mac, you can install dafny, along with its dependencies, mono and z3, using the `brew` package manager.

29.3 Building Dafny from Source

The current version of the Dafny executable builds and runs with Visual Studio 2012 or later.

First, install the following external dependencies:

- Visual Studio
- Code contract extension
- NUnit test adapter
- To install lit (for test run):
  - first, install python
  - second, install pip
  - last, run "pip install lit" and "pip install OutputCheck"

Second, clone source code (into sibling directories)

- Dafny
- Boogie

Last, follow the conventions:

- Visual Studio
  - Set "General:Tab" to "2 2"
  - For `"C\#:Formatting:NewLines` Turn everything off except the first option.

Dafny performs its verification by translating the Dafny source into the Boogie intermediate verification language. So Dafny references data structures defined in the Boogie project. So the first step is to clone and build Boogie from sources. See https://github.com/boogie-org/boogie.

Follow these steps.

Let *work* be a working directory.

Clone Boogie using

```
cd work
git clone https://github.com/boogie-org/boogie.git
```

Build Boogie using the directions from the Boogie web site, which for Windows currently are:

1. Open Source\Boogie.sln in Visual Studio
2. Right click the Boogie solution in the Solution Explorer and click Enable NuGet Package Restore. You will probably get a prompt asking to confirm this. Choose Yes.
3. Click BUILD > Build Solution.

Clone Dafny using git. The Dafny directory must be a sibling of the Boogie directory in order for it to find the Boogie files it needs.

```
cd work
git clone https://github.com/Microsoft/dafny.git
```

Build the command-line Dafny executables. 1. Open dafny/Source/Dafny.sln in Visual Studio 2. Click BUILD > Build Solution.

29.4 Using Dafny From Visual Studio

To test your installation, you can open Dafny test files from the dafny/Test subdirectory in Visual Studio 2012. You will want to use "VIEW/Error List" to ensure that you see any errors that Dafny detects, and "VIEW/Output" to see the result of any compilation.

An example of a valid Dafny test is

```
dafny\Test\vstte2012\Tree.dfy
```

You can choose "Dafny/Compile" to compile the Dafny program to C#. Doing that for the above test produces `Tree.cs` and `Tree.dll` (since this test does not have a main program).

The following file in the Dafny repository:

```
dafny\Test\dafny0\Array.dfy
```

is an example of a Dafny file with verification errors. The source will show red squiggles or dots where there are errors, and the Error List window will describe the errors.

29.5 The Dafny Server

TO BE WRITTEN

29.6 Using Dafny From the Command Line

29.6.1 Main method

TO BE WRITTEN

29.6.2 extern declarations

TO BE WRITTEN

29.6.3 Dafny Command Line Options

The command `Dafny.exe /?` gives the following description of options that can be passed to Dafny.

As a command-line tool, Dafny operates just like other command-line tools in Windows and Unix-like systems.

- The format of a command-line is determined by the shell program that is executing the command-line (.e.g. bash, the windows shell, COMMAND, etc.). The command-line typically consists of file names and options, in any order, separated by spaces.
- Files are designated by absolute paths or paths relative to the current working directory. Command-line argument not matching a known option is considered a filepath.
- Files containing dafny code must have a `.dfy` suffix.
- There must be at least one .dfy file.
- The command-line may contain other kinds of files appropriate to the language that the dafny files are being compiled to.

The command-line options are documented here.

- Options may begin with either a `/` (as is typical on Windows) or a `-` (as is typical on Linux)
- If an option is repeated (e.g. with a different argument), then the later instance on the command-line supercedes the earlier instance.
- If an option takes an argument, the option name is followed by a `:` and then by the argument value, with no intervening white space; if the argument itself contains white space, the argument must be enclosed in quotes.
- Escape characters are determined by the shell executing the command-line.

The dafny tool performs several tasks:

- Checking the form of the text in a .dfy file. This step is always performed, unless the tool is simply asked for help information or version number.
- Running the verification engine to check all implicit and explicit specifications. This step is performed by default, but can be skipped by using the `-noVerify` or `-dafnyVerify:0` option
- Compiling the dafny program to a target language. This step is performed by default if the verification is successful but can be skipped or always executed by using variations of the `-compile` option.
- Whether the source code of the compiled target is written out is controlled by `-spillTargetCode`
- The particular target language used is chosen by `-compileTarget`
- Whether or not the dafny tool attempts to run the compiled code is controlled by `-compile`

29.7 Verification

There are a great many options that control various aspects of verifying dafny programs. Here we mention only a few:

- Control of output: `-nologo`, `-dprint`, `-rpiomnt`, `-stats`, `-compileVerbose`

- Whether to print warnings: `-proverWarnings`
- Control of time: `-timeLimit`
- Control of the prover used: `-prover`

TO BE WRITTEN - advice on use of verifier, debugging verification problems

29.8 Compilation

The dafny tool can compile a dafny program to one of several target languages. Details and idiosyncracies of each of these are described in the following subsections. In general note that,

- the compiled code originating from dafny can be compiled with other source and binary code, but only the dafny-originated code is verified
- the output file names can be set using `-out`
- for each target language, there is a runtime library that must be used with the dafny-generated code when executing that code
- names in dafny are written out as names in the target language. In some cases this can result in naming conflicts. Thus if dafny program is intended to be compiled to a target language X, you should avoid using dafny identifiers that are not legal identifiers in X or that conflict with reserved words in X.

TODO - location of DafnyRuntime files

29.8.1 C

TO BE WRITTEN

29.8.2 Java

TO BE WRITTEN

29.8.3 Javascript

TO BE WRITTEN

29.8.4 Go

TO BE WRITTEN

29.8.5 C++

The C++ back-end is still very preliminary and is available for experimentation only.

TO BE WRITTEN

29.9 Dafny Command Line Options

The command `Dafny.exe /?` gives the following description of options that can be passed to Dafny.

```
---- Dafny options ------------------------------------------------------

Multiple .dfy files supplied on the command line are concatenated into one
Dafny program.

/dprelude:<file>
              choose Dafny prelude file
/dprint:<file>
              print Dafny program after parsing it
              (use - as <file> to print to console)
/printMode:<Everything|DllEmbed|NoIncludes|NoGhost>
              Everything is the default.
              DllEmbed prints the source that will be included in a compiled dll.
              NoIncludes disables printing of {:verify false} methods incorporated via the
              include mechanism, as well as datatypes and fields included from other files
              NoGhost disables printing of functions, ghost methods, and proof statements
              implementation methods.  It also disables anything NoIncludes disables.
/rprint:<file>
              print Dafny program after resolving it
              (use - as <file> to print to console)
/titrace      print type-inference debug info
/view:<view1, view2>
              print the filtered views of a module after it is resolved (/rprint).
              if print before the module is resolved (/dprint), then everthing in the modu
              if no view is specified, then everything in the module is printed.

/dafnyVerify:<n>
              0 - stop after typechecking
              1 - continue on to translation, verification, and compilation
/compile:<n>  0 - do not compile Dafny program
              1 (default) - upon successful verification of the Dafny
                  program, compile Dafny program to .NET assembly
                  Program.exe (if the program has a Main method) or
                  Program.dll (othewise), where Program.dfy is the name
                  of the last .dfy file on the command line
              2 - always attempt to compile Dafny program to C# program
                  out.cs, regardless of verification outcome
              3 - if there is a Main method and there are no verification
                  errors, compiles program in memory (i.e., does not write
                  an output file) and runs it
              4 - like (3), but attempts to compile and run regardless of
                  verification outcome
/compileTarget:<lang>
              cs (default) - Compilation to .NET via C#
              go - Compilation to Go
              js - Compilation to JavaScript
/compileVerbose:<n>
              0 - don't print status of compilation to the console
              1 (default) - print information such as files being written by
                  the compiler to the console
/spillTargetCode:<n>
              0 (default) - don't write the compiled Dafny program (but
                  still compile it, if /compile indicates to do so)
              1 - write the compiled Dafny program as a .cs file, if it
                  is being compiled
              2 - write the compiled Dafny program as a .cs file, provided
```

30 TODO

– const, static const

– declarations

– inference of array sizes

– witness, ghost witness clauses

– customizable error messages

– opaque types

– the !new type parameter characteristic

– traits, object

– non-null types

– abstemious functions

– labels (for program locations)

– updates to shared destructors

– labelled assertion statements, labelled preconditions

31 References

[BIB]

Sample math B: $a \to b$ or

$$a \to \pi$$

or (a) or [a $\to$]

Colors

```
integer literal:  10
hex literal:      0xDEAD
real literal:     1.1
boolean literal:  true false
char literal:     'c'
string literal:   "abc"
verbatim string:  @"abc"
ident:            ijk
type:             int
generic type:     map<int,T>
operator:         <=
punctuation:      { }
keyword:          while
spec:             requires
comment:          // comment
attribute         {: name }
error:            $
```

Syntax color tests:

```
integer: 0 00 20 01 0_1
float:   .0 1.0 1. 0_1.1_0
bad:     0_
hex:     0x10_abcdefABCDEF
string:    "string \n \t \r \0" "a\"b" "'" "\'" ""
string:    "!@#$%^&*()_-+={}[]|:;\\<>,.?/~`"
string:    "\u1234 "
string:    "     " : "\0\n\r\t\'\"\\"
notstring: "abcde
notstring: " \u123 " : "x \Z z" : "x \u x"
vstring:  @"" @"a" @""""" @"'\" @"\u"
vstring:  @"xx""y y""zz "
vstring:  @" " @"       "
vstring:  @"x
x"
bad:      @!
char:    'a' '\n' '\'' '"' '\"' ' ' '\\'
char:    '\0' '\r' '\t'  '\u1234'
badchar:  $ `
```

```
ids:  '\u123'   '\Z'  '\u'  '\u2222Z'
ids:  '\u123ZZZ'     '\u2222Z'
ids: 'a : a' : 'ab' :  'a'b' : 'a''b'
ids:  a_b _ab ab? _0
id-label:  a@label
literal:  true false null
op:       - ! ~ x  -!~x
op:       a + b - c * d / e % f a+b-c*d/e%f
op:       <= >= < > == != b&&c || ==> <==> <==
op:       .. ==# !=# !! in !in
op:       !in   !iné
not op:   !inx
punc:     . , :: | :| := ( ) [ ] { }
types:    int real string char bool nat ORDINAL
types:    object object?
types:    bv1 bv10 bv0
types:    array array2 array20 array10
types:    array? array2? array20? array10?
ids:      array1 array0 array02 bv02
ids:      intx natx int0 int_ int? bv1_ bv1x array2x
types:    seq<int>  set < bool >
types:    map<bool,bool>  imap < bool , bool >
types:    seq<Node> seq< Node >
types:    seq<set< real> >
types:    map<set<int>,seq<bool>>
types:    G<A,int> G<G<A>,G<bool>>
ids:      seqx mapx
no <:     seq  map  imap  set  iset  multiset  .
no arg:   seq < >  seq < , >  seq <bool , , bool >  seq<bool,>
keywords: if while assert assume
spec:     requires  reads modifies
attribute:  {: MyAttribute "asd", 34 }
attribute:  {: MyAttribute }
comment:  // comment
comment:  /* comment */ after
comment:  // comment /* asd */ dfg
comment:  /* comment /* embedded */ tail */ after
comment:  /* comment // embedded */ after
comment: /* comment
   /* inner comment
   */
   outer comment
   */ after
   more after
```