Index

∃, 145
∀, 145
∈, 356

abstract data type, 73, 300
abstraction, 298
Ada reference manual, 18
Ada, interfacing with, 247
Addition, 142
aggregate
  array, 51
  record, 55
antecedent, 137
argument, 141
arithmetic operators, 44
array, 47
  attributes, 51
  constrained, 49
  unconstrained, 49
aspect, 13, 76
  Abstract_State, 111
  Address, 270, 271
  Async_Readers, 270
  Async_Writers, 270
  Contract_Cases, 184
  Convention, 264, 265, 345
  Default_Value, 125
  Depends, 105
  Effective_Reads, 270
  Effective_Writes, 270
  External_Name, 265, 268
  Ghost, 327
  Global, 31, 100, 265
  Import, 265, 331, 333, 345
  Initial_Condition, 171
  Initializes, 112
  Inline, 176, 346
  Post, 76, 167
  Pre, 77, 164
  Refined_Depends, 117
  Refined_Global, 117
  Refined_Post, 174
  Refined_State, 116
  Size, 271
  Spark_Mode, 101
  synthesized, 291
  Volatile, 270, 271
Assert pragma, 189
Assert_And_Cut pragma, 196
assertion policy, 163
assertions, 9, 155, 163
Assume pragma, 198, 333
Async_Readers, 270
Async_Writers., 270
asynchronous reader, 270
asynchronous writer, 270
attribute, 42, 51
  'First, 42, 51
  'Image, 42, 43
  'Last, 42, 51
  'Length, 51
  'Loop_Entry, 204
  'Old, 77, 169, 186
  'Pred, 42
  'Range, 51
  'Result, 78, 170, 186
  'Succ, 42
  'Value, 42, 107

binder, 95
binding
  thick, 265
  thin, 265
bound variable, 145
boundary variable abstraction package, 301
boundary variable package, 301

C, interfacing with, 261
call tree, 161
calling conventions, 261
Case Analysis, 142
case expression, 25
case statement, 23
casting. *See* type conversion
child package, 87
circular dependency, 95
clean room, 7
cohesion, 298
compilation unit, 68
concatenation, 50
conclusion, 141
conditional expression, 23
configuration pragma, 248
conjecture, 356
Conjunction, 142
connective, 136
consequent, 137
constituents, 115
Constraint_Error, 161
constructive analysis, 128, 291
context clause, 19
context item, 19
  limited with clause, 93
  private with clause, 92, 254
  use clause, 21, 68, 71
  use type clause, 71
  with clause, 19, 68
contract, 13, 76, 163
  data dependency, 100
  flow dependency, 105
  refined, 116
  synthesis, 127, 291
contract programming, 162
Contract_Cases aspect, 184
Contrapositive, 142
controlled variable, 303
Convention aspect, 264, 265, 345
conversion. *See* type conversion
correct by construction, 7
correct, definition of, 8
coupling, 298
cryptographic hash, 310
cut point, 196

data dependency contract, 100
data layout, 261
data type, 32
declarative part, 20, 29, 93
declarative region, 30
default value aspect, 125
definition package, 69, 301
dependent expression, 24
depends aspect, 105
digital signature, 311
discriminant
  private type, 80
  record, 56
Disjunctive Syllogism, 142
dynamic predicate, 180

effective computation, 99
Effective_Reads, 270
Effective_Writes, 270
elaboration, 86, 93
  circular dependency, 95
encapsulation, 68, 298
enumeration representation clause, 264
erroneous execution, 156
error
  external, 155
  logical, 155
  runtime, 156
exclusive or, 137
existential quantifier, 145
expression function, 31
external axiomatization, 352
external error, 155
External option, 274, 281
external property, 274
external state abstraction, 273
external subsystems, 269

false coupling, 121
flow dependency contract, 104
for loop, 26, 43
formal methods, 7
formal verification, 8
function, 31
  expression, 31

generic
  formal
    subprograms, 62
    types, 59
  package, 36, 80
  parameter, 59, 80
  proof of, 224
  subprogram, 59
ghost function, 173, 326
ghost variable, 330
global, 30
Global aspect, 31, 100
golden rule of refinement, 305

hash, cryptographic, 310
header files, 262
homograph, 30
Hypothetical Syllogism, 142

if expression, 24
if statement, 22
inclusive or, 137
indexing, 47
inference rules, 142
  Addition, 142
  Case Analysis, 142
  Conjunction, 142
  Contrapositive, 142
  Disjunctive Syllogism, 142
  Hypothetical Syllogism, 142
  Modus Ponens, 142
  Modus Tolens, 142
  Simplification, 142
information hiding, 69, 78, 298
INFORMED, 297
  design elements, 299
  design steps, 303
  principles of, 302
Initial_Condition aspect, 171
Initializes aspect, 112
Inline aspect, 176, 346
interfacing with
  Ada, 247
  C, 261
Intrinsic, 345

key, public/private, 311

library unit, 68
limited with clause, 93
local, 30

logical equivalence, 140
logical error, 155
logical operators, 22, 44
logical statement, 11, 135
loop parameter, 27
loop statement, 25
  for scheme, 26, 43
  while scheme, 26
Loop_Invariant pragma, 201
Loop_Variant pragma, 212
loose coupling, 298

main procedure, 29
model number, 35, 38
Modus Ponens, 142
Modus Tolens, 142
monitored variable, 303
mutually dependent units, 93

name precedence, 30
Natural, 46
null range, 27
null statement, 160

option
  External, 274, 281
  Part_Of, 124, 281
or
  exclusive, 137
  inclusive, 137
overloading
  operators, 58
  subprograms, 57

package, 69
  boundary variable, 301
  boundary variable abstraction, 301
  child, 87
  definition, 69, 301
  generic, 36
  initialization of, 86
  nested, 121
  private child, 89, 124
  public child, 89
  type, 73, 300
  utility, 71, 301
  variable, 83, 300
package state, 110
parameter
  association, 20
  mode, 29

Part_Of option, 124, 281
Patriot missile, 38
Positive, 46
postcondition, 76, 167
poststate, 169
pragma, 13
  Assert, 189
  Assert_And_Cut, 196
  Assume, 198, 333
  Loop_Invariant, 201
  Loop_Variant, 212
  Spark_Mode, 101, 254
precondition, 77, 164
predefined exceptions
  constraint error, 161
  program error, 157
  storage error, 160
  tasking error, 160
predicate, 144
  dynamic, 180
  static, 181, 182
premise, 141
prestate, 169
private child package, 89, 124
private part, 80
private type, 69, 78
private with clause, 92, 254
procedure, 28
Program_Error, 157
programming language, C, 261
proof obligation, 162
property
  Async_Readers, 270
  Async_Writers, 270
  Effective_Reads, 270
  Effective_Write, 270
proposition, 135
propositional connective, 136
public child package, 89

range, 27
Refined_Depends aspect, 117
Refined_Global aspect, 117
Refined_Post aspect, 174
Refined_State aspect, 116
refinement, 115
  golden rule of, 305
relational operators, 22
representation clause, enumeration, 264
reserved word, 19
retrospective analysis, 128, 291
rules of inference. *See* inference rules
runtime error, 156

scope, 30
Simplification, 142
singleton, 83
slicing, 48
sound argument, 144
spark mode, 248
Spark_Mode aspect, 101
Spark_Mode pragma, 101, 254
state abstraction, 111
  external, 273
statement. *See* logical statement
static predicate, 181
static verification, 8
Storage_Error, 160
String, 53
subprogram, 27
subtype, 45
  Natural, 46
  Positive, 46
subtype predicate, 179
synthesis of contracts, 127, 291

Tasking_Error, 160
tautology, 139
test driven development, 296
thick binding, 265
thin binding, 265
transitivity, 333, 334
trusted computing base, 339
type
  array, 47
    constrained, 49
    unconstrained, 49
  atomic, 33
  composite, 33
  derived, 57
  discrete, 40
  enumeration, 40
  integer
    modular, 44
    signed, 43
  parent, 57
  private, 69, 78
  real, 35
    decimal, 39

fixed point, 37
floating point, 35
record, 55
scalar, 34
string, 53
type conversion, 20, 44
type invariant, 178
type package, 73, 300

unbound variable, 145
undefined behavior, 156
universal quantifier, 145
universe of discourse, 144
use clause, 21, 68, 71
use type clause, 71
utility package, 71, 301

valid argument, 141
variable package, 83, 300
VC. *See* verification condition
verification condition, 143, 162
verification driven development, 296, 305
verification goals, 313
visibility, 91
direct, 91
with clause, 91
visible part, 80

while loop, 26
with clause, 19, 68
limited, 93
private, 92, 254