

Index

Symbols

&& (and) 69
(cardinality) 80
- (difference) 52, 286
= (equals) 52
> (greater than) 80, 290
>= (greater than or equal to) 80, 290
<=> (iff) 69
=> (implies) 69
+ (in signature declaration) 94
& (intersection) 52, 286
. (join) 57, 286
[] (join) 61, 286
< (less than) 80, 290
=< (less than or equal to) 80, 290
! (not) 69, 290, 291
|| (or) 69
++ (override) 67–68, 286
-> (product) 55, 286
* (reflexive transitive closure) 65, 286
= (relational equals) 289
@ (suppress expansion) 120, 273, 285
^ (transitive closure) 63–65, 286
~ (transpose) 62, 286
+ (union) 52, 286

A

Abrial, Jean-Raymond 310, 330
Abstraction function 223
Abstractions
 not well expressed in code 2
 why key to software design xiv, 1
abstract keyword 86, 93, 94, 104, 260,
 273
Abstract signature 93, 94, 104, 273,
 283

Acyclicity
 constraint 35, 117, 133
 exercise 238
Address book
 informal description 5
Algebraic property 15, 212, 215
Alias
 for module 134
 in address book 5
all keyword 70, 260, 291
Alloy Analyzer 4, 152–154
Alloy grammar 261
AMN (Abstract Machine Notation)
 311
Analysis
 cf. manual review xiii, 30
 mechanism 152–154
 vs. theorem proving 15
Analysis constraint 146
Analysis variable 146
and keyword 69, 260
Arithmetic 136
Arity
 defined 36
 error 112, 266
 highest used in practice 43
Arrow product
 defined 55, 287
 universal relation 51
as keyword 134, 260, 270
Assertion
 anonymous 129
 defined 127
 first example 13
assert keyword 127, 260
Assignment
 modeled with override 68
Associativity 263

Atelier-B 316

Atom

defined 35

naming of 40

B

Backward execution 11

Barber Paradox 247

Bar, in quantification 292

BDD (Binary Decision Diagram) 154

Berkmin 152

bi-implication 69

Binary relation 36

Bjorner, Dines 322

Block (of expressions) 291

B method 310

Boolean

not a type in Alloy 137

Boolean expressions 289

Borgida, Alex 205

Bounding expression 70, 99, 100,
111, 122, 162, 274, 279, 285,
289, 296

Bounding expression, defined 75

Box join

defined 61

B-Toolkit 316

Bunch theory 44

but keyword 131, 260, 283

Butler, Michael 301

C

Canonicalization 219, 220, 222

Cardinality

constraint 80

operator 136

Cartesian product 168

Chaff 152

check keyword 130, 152, 260, 280

Classification hierarchy 17, 86, 94,
104, 110, 197, 272

Class invariant 122

Closure

not axiomatizable 238

symmetric 62

transitive 63–65, 287

Command

defined 130, 280

first example 6

Comment syntax 259

Composite objects

as language construct 42

Composite pattern 6, 17

Composition

with join 57

Comprehension

defined 74, 287

to define identity 51

Concurrency 181

Conditional expression 69

Conjunction

implicit 69, 291

Constants

expressive power 51

of Alloy logic 50

Constraint

analysis 146

defined 68

Containment

modeling with multirelation 38

Cook, Steve 316

Counterexample 142, 146, 280

first example 13

spurious 163

CTL (Computation tree logic) 186

D

Daniels, John 316

Day, Doris 247

- Declaration
 - defined 75, 274
 - dependent 100
 - no top-level 99
 - of fields 275
 - role in analysis 146, 148
 - signature 272
- Declaration formula
 - defined 75, 79, 277
 - examples 79, 174, 189
- Declarative
 - vs. operational 10
- Diagram
 - generated by Alloy Analyzer 32
 - model 103
 - use in modeling 32
- Diameter of state machine 185
- Difference operator 52, 287
- Dijkstra, E.W. 143
- disj keyword 70–71, 99, 260, 274, 288
 - in signature declarations 275
- Disjointness error 266
- Domain
 - in definition of override 67
 - of relation defined 47
 - related to restriction 67
- Domain restriction
 - defined 66, 287
 - resolve overloading 51, 117, 118
- Dot join
 - defined 57
- E**
- else keyword 69, 260
- Empty set
 - as constant in logic 50
- Equality
 - arithmetic 290
 - operator defined 52, 289
 - relational 289
 - structural vs. reference 54
 - vs. definitional symbol 54
- Errors 266
- Event-based idiom 195
- exactly keyword 131, 168, 260, 283
- Exact scope 183
- Example 146, 280
- Expression
 - defined 284
 - in model diagram 105
 - let 284
 - paragraph 278
 - quantified 291
 - redundant 112
 - sequence 291
 - sum 81, 289
- Expression,bounding 70, 99, 100, 111, 122, 162, 274, 279, 285, 289, 296
- Expression,bounding (defined) 75
- Expressions 284
 - boolean 289
 - integer 288
 - relational 285
- extends keyword 93, 104, 109, 260, 272
- Extreme programming 2
- F**
- Fact
 - defined 119, 278
 - first example 18
 - role in analysis 146
 - signature 19, 120–122, 122, 273
 - vs. predicate 125
- fact keyword 119, 260, 278
- Fairness 186
- Feynman, Richard 141
- Field
 - constraint implicit in declaration 121
 - declaration 275

- defined 97
- inherited 273
- overloading 115, 267
- Filtering properties 186
- First-order logic
 - Alloy limited to 41
 - vs. temporal logics 186
- Fitzgerald, John 301
- for keyword 130, 260, 283
- Formal methods
 - lightweight xiii
 - not silver bullet xi
 - obstacles to adoption 2
- Formula
 - declaration 75, 277
 - quantified 291
- Frame condition 191
 - examples 210
 - Reiter style 205
- Function
 - Alloy construct 278
 - Alloy construct defined 123, 268
 - as relation 46
 - first example 13
 - higher-order 41
 - total and partial 48
- Functional relation 46
 - defined with identity 63
- Function application
 - with join 59
- fun keyword 123, 260, 278

G

- Generator axiom 158
- Generic module
 - first example 24
 - overview 133, 270
- Goat, cabbage, wolf 249
- Gogolla, Martin 301, 316, 322
- Grammar of Alloy 261
- Grandpa, self 85

- Gries, David 247
- Group, in address book 5
- Guttag, John xi, 31, 92

H

- Halmos, Paul 248, 249
- Handshaking problem 248
- Harel, David 144
- Hehner, Eric 44
- Higher-order
 - quantification 72
 - structures 41
- History variable 228
- Hoare, C.A.R. xiii
- Horning, James J. xi, 31, 92
- Hotel locking
 - example 187, 303
 - exercise 255

I

- iden keyword 50, 260, 285
- Identifiers 260
- Identity relation
 - definable 51
 - defined 50
 - over universe 50, 65
 - with restriction 67
- Idiom
 - event-based 195
 - explicit time 152, 173, 174, 181, 188
 - incremental state 207
 - not hardwired 31
 - traces 22, 179, 306
- IFAD 328
- iff keyword 69, 260
- if keyword 69
- if-then-else 69
- implies keyword 69, 260
- Importing modules 133

in

- choice of keyword 55
- in signature declaration 93, 272
- keyword 260, 289
- operator defined 52

Inductive analysis 179

Initial condition 178

Injection 47

Injective relation

- defined with identity 63

Instance

- choice by analyzer 7
- choice of term 144
- defined 146, 264
- first example 7
- from command 280

Instance finding 142

Int

- keyword 260
- signature 136, 271

Integer

- and interpreted set 42
- scope 137

Integer expressions 288

Integers 136

Interpreted set 39–40

Intersection operator 52, 287

Int (signature) 136

Invariant

- preservation 179, 211, 227, 302, 313, 323, 329
- preservation (exercise) 244

iView MediaPro 207

J

Jackson, Michael 195

Java

- metamodel (exercise) 251
- overloading in 118

Jaza 336

JML (Java Modeling Language) 323

Join

- by position not column name 43
- compared to database 61
- defined 57, 61, 287
- distributivity (exercise) 236
- higher arity 60
- not associative 60
- typing rule 112

Jones, Cliff 322

JSP xi

K

Khurshid, Sarfraz 176

Kleppe, Anneke 316

L

Lampson, Butler 61

Larch specification language xi, 92, 323

Larsen, Peter Gorm 301

Leader election example 171

Let

- constraint 73, 284
- expression 73
- expressoin 284
- not recursive 74

let keyword 260

Lexical issues 259

Library module 133

Lightweight formal methods xiii

List 159, 160

Logic

- first order 33, 41, 44, 137, 144, 146, 165, 186, 238
- higher order 41, 42, 72, 157, 265, 293, 302
- relational 264–265

London Underground (exercise) 241

lone keyword 260

- as multiplicity 34, 72, 76, 97, 103, 269, 272, 275
- as quantifier 70, 72, 291
- LTL (Linear temporal logic) 186

M

- Machine diameter 185
- Manna, Zohar 187
- McCarthy, John 152
- McMillan, Ken xi
- Media asset management example 205
- Memory example 219
- Metamodels
 - exercises 250
- Meyer, Bertrand 1
- Milgram, Stanley 66
- minus (integer operator) 80
- Model
 - meaning of term 4
 - term avoided 144
- Model checking 144, 187
 - not suitable for software xii
 - scope implicit 132
 - SMV xi
- Model diagram
 - defined 103
 - examples 17, 108, 121, 177, 189, 190, 211
 - first example 18
- Modifies clause 205
- Module
 - alias 134
 - defined 133
 - import 133, 270–272
 - parametric 134, 270–272
 - rationale 173
 - structure 85, 270
- module keyword 133, 260, 270
- Multiple inheritance 96
- Multiplicity
 - default in diagram 109
 - defined 75, 269
 - in diagrams 103, 104
 - in field declaration 97
 - in signature declaration 94
 - nested 79

- Multiplicity keywords 275

Multirelation

- Alloy-specific term 44
- defined 36
- in model diagram 105
- useful in practice 43

Mutation 38–39

- atoms immutable 35

Mylopoulos, John 205

N

Namespace 260

Navigation

- backward 59
- exercise 236
- expression style 34–35
- with join 59

Negation 69, 260

Nelson, Greg 154

Nitpick 154

no keyword 70, 260, 291

none keyword 50, 260, 267, 285

not keyword 69, 260, 290, 291

Null values 44

O

OCL (Object Constraint Language) 47, 316

Octopus tool 322

OMT (Object Modeling Technique) xii

one keyword 260

- as multiplicity 76, 97, 103, 269, 272, 275, 283

- as quantifier 70, 291
- open keyword 133, 260, 270
- Operation 10, 124
- Operational
 - vs. declarative 10
- Operators
 - logical 69, 291
 - precedence 68, 263
 - relational 50
- Option
 - Alloy-specific term 44
 - defined 37
 - describes variable not value 45
 - in Alloy compared to ML 44
- Ordering
 - symmetry breaking 154, 173, 183
 - with library module 24
- or keyword 69, 260
- Overapproximation 111
- Overlapping 109
- Overlapping signatures 273
- Overlapping types 115
- Overloading 266, 267
 - compared to Java 118
 - field 109, 115
 - field names 116, 273
 - of functions and predicates 127
 - resolve with restriction 117, 118
- Override
 - defined 67–68, 287
- Overture initiative 328

P

- Pair 55
- Paradox, Russell's 247
- Parametric module 134, 270
- Parentheses 285
- Partial function 48
 - no undefined application 59
- plus (integer operator) 80
- Pnueli, Amir 187

- Polymorphism 134
- Postcondition 191
- Poststate 10, 32, 150, 197, 226
- Praxis Critical Systems 2, 328
- Precedence 68, 263
- Precondition
 - examples 26, 28, 191, 209, 210, 220
 - implicit 192
 - not computable 163
- Predicate
 - Alloy construct 123, 268, 278
 - first example 6
 - invoking 11
 - operation 124
 - vs. fact 125
- Predicate calculus 33–35
 - exercise 234
- pred keyword 123, 124, 260, 278
- Prerequisites example 41
- Prestate 10, 32, 150, 197, 226
- Problem frames 195
- ProB tool 313, 316
- Product operator 55, 287
- Progress
 - predicate 182
 - property 186
- Projection
 - defined 48–49
 - example 150
 - of Book instance 7
- ProofPower 335

Q

- Qualified name 134, 271
- Quantification 70, 291
 - higher order 72
 - implicit in signature fact 122
 - nested 293
- Skolemized away 154
- unbounded universal 157

R

Railway switching (exercise) 253

Range

- of relation defined 47
- related to restriction 67

Range restriction

- defined 66, 287

Reachability

- expressed with closure 64

Receiver

- object-oriented 19
- syntax in Alloy 124, 126, 280

Recodable lock 187

Redundancy error 112, 266

Refactoring xiii, 91

Reflexive

- relation 64
- transitive closure 65, 287

Refutation 142

Regression testing

- with assertions 17

Reiter, Raymond 205

Relation

- as table 36
- declared as field 97
- defined 36–48
- empty 37
- functional 46, 63
- higher-order 41
- infinite 43
- injective 46, 47, 63
- in model diagram 104
- naming of columns 43
- properties (exercise) 234, 235
- reflexive 64
- size 36
- total and partial 48
- transitive 63
- undirected (exercise) 238
- universal 94
- unordered 43

Relational calculus 34–35, 44

- exercise 234
- hints on using 91

Relational composition

- with join 57

Relational expressions 285

Relational logic 264

Relational operators 55

Requirements

- vs. specification 195

Resource limits 145

Restriction

- domain 287
- range 287

Restriction operator

- defined 66
- resolve overloading 51, 117, 118

Richters, Mark 316

Ring (exercise) 237

run keyword 130, 152, 260, 281

Russell, Bertrand 247

Russell's Paradox 247

S

Sanity check 211

SAT solvers xii, 152, 187

Scalar

- as unary relation 36
- describes variable not value 45
- modeled as relations 44

Scope 142, 282

- and generator axioms 158–165
- default 87, 130, 131, 165, 167, 283
- defined 130
- exact 131, 168, 183
- first example 6
- monotonicity 167, 183
- of zero 169
- selecting 31, 165
- small scope hypothesis 15, 146
- specification 282

- Self-grandpa 85
 - Semantics 295
 - Set
 - as unary relation 36, 44
 - in model diagram 104
 - operators 52
 - universal 94
 - set keyword 76, 97, 103, 260, 275
 - not applicable to signature 273
 - Shlyakhter, Ilya 154
 - sig keyword 93, 260, 269, 272, 273
 - Signature
 - abstract 93, 94, 104, 273, 283
 - bounds in scope 130
 - declaration 272
 - defined 93, 272
 - extension 93, 109
 - fact 122, 273
 - first example 6
 - overlapping 109, 273
 - singleton 96
 - subset 94, 104, 109, 117, 272
 - subsignature 93, 272
 - top-level 93, 94, 130
 - type 272
 - Simon, Paul 247
 - Simplicity xiv
 - Situation calculus 152
 - Size of relation 36
 - Skolem constant 10, 149, 282
 - Skolemization 154, 265, 293
 - Small model theorem 146
 - Small scope hypothesis 15, 143, 146
 - Smalltalk 318
 - Snapshots 48
 - some keyword 260
 - as multiplicity 72, 76, 97, 103, 269, 272, 275
 - as quantifier 70, 72, 291
 - Spanning tree (exercise) 237
 - Specification
 - vs. requirements 195
 - Spivey, J. Michael 328
 - State machine
 - meta model (exercise) 250
 - simulation (exercise) 250
 - subsection
 - Function
 - invocation 279
 - overloading 279
 - Predicate
 - invocation 279
 - overloading 279
 - Subset
 - signature 272
 - Subset
 - operator 52
 - operator defined 289
 - Subsignature 93, 272
 - Subtype 109, 114, 115, 267, 272
 - sum keyword 81, 260, 289
 - Supertype 114
 - Surgeon's gloves problem 249
 - Symmetric
 - closure 62
 - relation 62
 - Symmetry breaking 32, 153, 173, 183
 - Syntropy xii, 316
- ## T
- Tanaka, Akira 215
 - Tarski, Alfred 44
 - Temporal logic 186
 - Ternary relation 36
 - Test cases 3, 30
 - Testing
 - inadequacy of 143
 - less effective than analysis 15
 - Theorem proving
 - limitations xi, 2
 - role in analysis 143
 - vs. instance finding 141
 - this keyword 97, 101, 122, 124

Time

- arguments to operation 181
- as column of relation 152, 173, 174–178, 188

Together Designer tool 322

Torlak, Emina 154

Total function 48

Trace

- analysis 22–28, 179
- constraint 24, 29, 192, 197, 305, 306
- inclusion 225
- order of states 32

Tractability 132

Transitive

- closure defined 63–65, 287
- closure not axiomatizable 238
- relation 63

Transpose 62, 287

Tree properties (exercise) 236

Tuple 55

- defined 37

Type 109, 266

- basic 109
- checking of predicate 126
- error 112, 266
- overlap 109
- redundancy 54, 112
- relational 111
- union 44, 54, 267

U

UML (Unified Modeling Language)

47

- bug in closure definition 239
- diagram notation 107

Unary relation 36

Unbounded universals 157

Undecidability 141, 144

Undefined expressions avoided 59

Uninterpreted sets 35

Union operator 52, 287

Union type 44, 54, 267

Universal set 94

- defined 50
- not definable 51

univ keyword 50, 260, 265, 267, 285

Unix file system (exercise) 252

USE tool 31, 316

Utting, Mark 336

V

Validity 141

Variable, analysis 146, 150

VDM++ 323

VDM-SL 323

VDMTools 31, 328, 336

VDM (Vienna Development Method)

xi, 31, 42, 178, 322

W

Warmer, Jos 316

Website 4

Witness 154

Woodcock, Jim 301, 329

Z

Zermelo-Fraenkel set theory 46, 330

Z/Eves 335

Z notation xi, 31, 42, 46, 47, 51, 54, 152, 178