Index

AKM, 121
ATA, 84
DFA, 9
KM, 10
KMLTS, 105
↔, 11
false, 104
⇌, 11
⊗, 16
⊗, 126
→, 52
⊠, 51
true, 104
↑, 104
ATL, 157
DEL, 15
ETL, 15
Mu, 84
MSO, 156
PAL, 17
PDL, 13
PDL, 39
PDL♯, 49

abstraction, 109
accelerated transitions, 120
Alloy Analyzer, 32
atomic observables, 69
automata
μ-, 86
accepting run of, 87

parity condition of, 87
alternating tree, 84
expression, 121
finite, 9
deterministic, 9
language of, 10
generalized, 121
on guarded strings, 46
on words, 9
Rabin tree, 84
bisimulation, 11
auto-, 12
contraction, 12
game, 12
restricted, 11
total, 11
with termination, 50

card cryptography, 155
characteristic formula, 83
commutative monoid, 63
compatible states, 61
concrete model, 105

decomposition
by agents, 60
by issues, 60

derivable message, 144
Dinning Cryptographer, 149

empty language, 10
empty string, 10
epistemic bisimulation invariance, 153
equivalence
  language, 10
  modal, 15
  pattern matching, 150
  permutation, 150
  simple deduction, 150
  static, 150
  event model, 16
fusion product, 44
generated temporal structure, 147
guarded automata, 46
  accept states of, 52
  action states of, 46
  deterministic, 46
  test states of, 46
  guarded string, 43
information state, 147
initial assumptions, 24
interpreted system, 2, 15
  global state of, 15
  local state of, 15
  pointed, 15
  run of, 15
  admissible, 146
  isomorphism, 84
Kleene Algebra, 121
Kleene’s Theorem, 10
knowledge
  algorithmic, 141
  certain, 141
  explicit data, 141
  levels of, 85
  propositional, 141
  states of, 84
knowledge-based program, 2
knowledge-based protocol, 153
Kripke model, 10
  \( \omega \)-branching, 11
  accelerated, 7
  normal, 131
  connected, 28
  decomposable, 68
  expansion of, 65
  finite, 11
  finitely branching, 11
  image-finite, 11
  labels of, 11
  locally generated, 69
  propositionally differentiated, 65
  signature of, 11
  unit, 61
  vocabulary of, 11
  with termination, 50
labelled transition system, 11
  accelerated modal, 120
  Kripke, 11
  Kripke modal, 105
left-simulation, 63
  total, 64
local proposition, 69
logic
  alternating time, 157
  dynamic epistemic, 15
  epistemic, 11
  epistemic temporal, 3, 15
  Kleene’s, 107
  monadic second order, 156
  normal modal, 132
  propositional dynamic, 13
  test-free, 14, 41
  propositional modal \( \mu \)-calculus, 84
  public announcement, 17
  3-valued semantics of, 106
  public event, 43
  update, 49
logical omniscience, 143
merging composition, 60
  on event models, 78
  on Kripke models, 61
Index

mode semantics, 40
model checking, 4, 5
Muddy Children, 4, 62, 114, 149
no miracle, 152
non-parallel run, 89
perfect recall, 152
precondition, 16
  propositionally differentiated, 75
product update, 16
  extended, 74
program test, 13
protocol
  DEL, 3
    explicit, 3, 21
    announcement, 38
    biased, 32
  complete verification, 25
  compliance, 40
  deterministic, 24
  epistemic, 3, 154
  extensional notion of, 3
goal, 24
knowledge of, 4, 37
  local, 146
meta-knowledge of, 21
  non-deterministic, 24
regular, 21
remaining, 40
roles in, 140
runs of, 23
security, 8
skip, 43
specification, 24, 26
unbiased, 33
public event, 43
refinement, 109
regenerating path, 95
regular expression, 120
  expansion of, 120
  guarded, 45
input derivatives of, 40
language of, 10
pre-derivatives of, 41
pre-sequences, 41
rewriting, 123
relation
  equivalence, 11
  may, 104, 119
  must, 104, 119
  reflexive, 11
  symmetric, 11
  transitive, 11
restricted invariance, 11
Russian Cards Problem, 3, 21, 26, 149
social software, 55
start state, 9
symbolic model checking, 6
synchronicity, 152
tree, 85
  alive, 95
  bisimulation-regular, 86
  image-finite, 89
  labelled, 85
  levels of, 86, 156
  root of, 85
  simple, 90
verification
  under common knowledge, 28
  universal, 25, 29