Epistemic modelling and protocol dynamics

Wang, Y.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (http://dare.uva.nl)
<table>
<thead>
<tr>
<th>Page</th>
<th>Term</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>121</td>
<td>AKM</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>ATA</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>DFA</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>KM</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>KMLTS</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>Θ</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>⊠</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>↑</td>
<td></td>
</tr>
<tr>
<td>157</td>
<td>ATL</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>DEL</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>ETL</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>Mu</td>
<td></td>
</tr>
<tr>
<td>156</td>
<td>MSO</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>PAL</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>PDL</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>PDL*</td>
<td></td>
</tr>
</tbody>
</table>

- Abstract, 109
- Accelerated transitions, 120
- Alloy Analyzer, 82
- 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, 71
  - By issues, 60, 71
- Derivable message, 144
- Dinning Cryptographer, 149

- Empty language, 10
empty string, 10
epistemic bisimulation invariance, 153
equivalence
language, 10
modal, 13
pattern matching, 150
permutation, 150
simple deduction, 150
static, 150
event model, 16
fusion product, 44
genenerated 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
Kleene Algebra, 121
Kleene’s Theorem, 10
knowledge
algorithmic, 141
certain, 141, 145, 147
explicit data, 141
events of, 85
levels of, 85
propositional, 141, 145
states of, 84
knowledge-based program, 2
knowledge-based protocol, 153
Kripke model, 10
$\omega$-branching, 11
accelerated, 7, 121

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
modality, 104
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, 122
propositional modal $\mu$-calculus, 84
public announcement, 17, 29
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, 43
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