

# Inhaltsverzeichnis

<b>Einleitung</b>	<b>1</b>
<b>1 Mathematische Grundlagen</b>	<b>15</b>
1.1 Mengen . . . . .	15
1.2 Relationen . . . . .	16
1.3 Abbildungen . . . . .	17
1.4 Sequenzen . . . . .	17
<b>2 Die Logik TLDA</b>	<b>18</b>
2.1 Semantisches Modell . . . . .	18
2.1.1 Der Begriff des Ablaufs . . . . .	19
2.1.2 Strukturelle Eigenschaften der Abläufe . . . . .	23
2.2 Syntax . . . . .	35
2.2.1 Alphabet . . . . .	35
2.2.2 Terme . . . . .	37
2.2.3 Formeln . . . . .	37
2.2.4 Zustandsformeln . . . . .	38
2.2.5 Freie Variablen . . . . .	42
2.2.6 Notationen . . . . .	42
2.3 Semantik . . . . .	43
2.3.1 Informale Semantik . . . . .	43
2.3.2 Formale Semantik . . . . .	46
2.3.3 Modelle . . . . .	48
2.3.4 Erfüllbarkeit und Allgemeingültigkeit . . . . .	50
2.3.5 Logisches Folgern und logische Äquivalenz . . . . .	51
2.3.6 Koinzidenzlemma . . . . .	52
2.4 Semantische Eigenschaften . . . . .	60
2.4.1 Eigenschaften von Zustandsformeln . . . . .	61

2.4.2	Präfix- und Suffixeigenschaften . . . . .	64
<b>3</b>	<b>Umgebungsinvarianz</b>	<b>68</b>
3.1	Restriktion . . . . .	73
3.2	Umgebung . . . . .	78
3.3	Umgebungsinvariante Formeln . . . . .	89
3.3.1	Umgebungsinvariante Schrittformeln . . . . .	93
3.3.2	Schwach umgebungsinvariante Schrittformeln . . . . .	98
3.3.3	Umgebungsinvariante Ablaufformeln . . . . .	103
3.4	Eigenschaften umgebungsinvarianter Formeln . . . . .	111
<b>4</b>	<b>Spezifikation</b>	<b>117</b>
4.1	Der Begriff der Spezifikation . . . . .	121
4.2	Sicherheitseigenschaften . . . . .	122
4.2.1	Spezifikation von Sicherheitseigenschaften . . . . .	124
4.3	Lebendigkeitseigenschaften . . . . .	130
4.3.1	Progress und Fairness . . . . .	130
4.4	Zerlegung einer Eigenschaft . . . . .	136
<b>5</b>	<b>Komposition</b>	<b>144</b>
5.1	Komposition von Systemen . . . . .	150
5.2	Komposition von Spezifikationen . . . . .	151
5.2.1	Komposition umgebungsinvarianter Spezifikationen . . . . .	152
5.2.2	Komposition von Spezifikationen der Sicherheitseigen- schaften . . . . .	158
5.2.3	Komposition von Spezifikationen der Sicherheits- und Lebendigkeitseigenschaften . . . . .	159
5.2.4	Kompositionsschema . . . . .	161
<b>6</b>	<b>Verifikation</b>	<b>170</b>
6.1	Aussagenlogische Beweisregeln . . . . .	173
6.2	Beweisregeln für $\sim$ -Variablen . . . . .	174
6.3	Beweisregeln für $\square$ und $\diamond$ . . . . .	176
6.4	Invarianten . . . . .	180
6.4.1	Invarianten-Regeln in TLDA . . . . .	184
6.4.2	Korrektheit der Invarianten-Regeln . . . . .	185

6.5	Beweisregeln für Lebendigkeitsoperatoren . . . . .	201
<b>7</b>	<b>Fallstudien</b>	<b>206</b>
7.1	Das Produzenten-Konsumenten-System . . . . .	207
7.1.1	Spezifikation der Komponenten . . . . .	209
7.1.2	Verifikation der Komponenten . . . . .	211
7.1.3	Komposition . . . . .	214
7.2	Speisende Philosophen . . . . .	219
7.2.1	Spezifikation . . . . .	220
7.2.2	Verifikation der Sicherheitseigenschaften . . . . .	222
7.2.3	Verifikation der Lebendigkeitseigenschaften . . . . .	222
7.3	TLDA und TLA: ein Vergleich . . . . .	226
7.3.1	Stottersequenzen und stotterinvariante Formeln . . . . .	226
7.3.2	Syntax der Logiken . . . . .	228
7.3.3	Nichts ändern ist doch ändern . . . . .	230
7.3.4	Nicht-Aktualisieren vs. Lesen einer Variablen . . . . .	232
7.3.5	Nebenläufigkeit und Nichtdeterminismus . . . . .	234
7.3.6	Progress und Fairness . . . . .	236
7.3.7	Reflexion . . . . .	238
	<b>Zusammenfassung</b>	<b>240</b>
<b>A</b>		<b>243</b>
A.1	Quantifizierung über flexible Variablen . . . . .	243
A.2	Beweisregeln für $\square$ und $\diamond$ : Ableitungen . . . . .	246