

Krzysztof R. Apt Ernst-Rüdiger Olderog

Programm- verifikation

Sequentielle, parallele und verteilte
Programme

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Inhaltsverzeichnis

| | | |
|-----|--|----|
| 1 | Einführung | 1 |
| 1.1 | Beispiel eines parallelen Programmes | 1 |
| | Lösung 1 | 2 |
| | Lösung 2 | 3 |
| | Lösung 3 | 4 |
| | Lösung 4 | 5 |
| | Lösung 5 | 6 |
| | Lösung 6 | 7 |
| 1.2 | Programmkorrektheit | 8 |
| 1.3 | Struktur dieses Buches | 11 |
| 2 | Vorbereitungen | 15 |
| 2.1 | Syntax | 15 |
| 2.2 | Getypte Ausdrücke | 16 |
| | Typen | 16 |
| | Variablen | 16 |
| | Konstanten | 17 |
| | Ausdrücke | 18 |
| | Indizierte Variablen | 19 |
| 2.3 | Semantik von Ausdrücken | 19 |
| | Feste Struktur | 19 |
| | Zustände | 20 |
| | Definition der Semantik | 21 |
| | Modifikation von Zuständen | 23 |
| 2.4 | Formale Beweissysteme | 24 |
| 2.5 | Logische Formeln | 25 |

| | | |
|------|---|-----|
| 2.6 | Semantik von logischen Formeln | 27 |
| 2.7 | Substitution | 28 |
| 2.8 | Substitutions-Lemma | 31 |
| 2.9 | Übungsaufgaben | 32 |
| 2.10 | Bibliographische Anmerkungen | 33 |
| 3 | Deterministische Programme | 35 |
| 3.1 | Syntax | 35 |
| 3.2 | Semantik | 36 |
| | Eigenschaften der Semantiken | 40 |
| 3.3 | Verifikation | 42 |
| | Partielle Korrektheit | 43 |
| | Totale Korrektheit | 49 |
| | Korrektheit der Beweissysteme | 51 |
| 3.4 | Beweisskizzen | 57 |
| | Partielle Korrektheit | 58 |
| | Totale Korrektheit | 62 |
| | Programmdokumentation | 63 |
| 3.5 | Vollständigkeit | 64 |
| 3.6 | Zusätzliche Axiome und Regeln | 70 |
| 3.7 | Systematische Entwicklung korrekter Programme | 72 |
| | Summations-Problem | 73 |
| 3.8 | Fallstudie: Minimale Abschnittssumme | 75 |
| 3.9 | Übungsaufgaben | 79 |
| 3.10 | Bibliographische Anmerkungen | 83 |
| 4 | Disjunkte parallele Programme | 85 |
| 4.1 | Syntax | 85 |
| 4.2 | Semantik | 86 |
| | Determinismus | 88 |
| | Sequentialisierung | 91 |
| 4.3 | Verifikation | 92 |
| | Parallele Komposition | 93 |
| | Hilfsvariablen | 95 |
| | Korrektheit der Beweissysteme | 98 |
| 4.4 | Fallstudie: Finde Positives Element | 100 |
| 4.5 | Übungsaufgaben | 104 |
| 4.6 | Bibliographische Anmerkungen | 105 |
| 5 | Parallele Programme mit gemeinsamen Variablen | 107 |
| 5.1 | Zugriff auf gemeinsame Variablen | 107 |
| 5.2 | Syntax | 109 |
| 5.3 | Semantik | 110 |
| | Atomarität | 112 |
| 5.4 | Verifikation: Partielle Korrektheit | 113 |
| | Komponenten-Programme | 113 |

| | | |
|------|--|-----|
| | Keine Kompositionalität des Ein/Ausgabe-Verhaltens | 115 |
| | Parallele Komposition: Interferenz-Freiheit | 115 |
| | Notwendigkeit von Hilfsvariablen | 118 |
| | Korrektheit des Beweissystems | 121 |
| 5.5 | Verifikation: Totale Korrektheit | 123 |
| | Komponenten-Programme | 123 |
| | Parallele Komposition: Interferenz-Freiheit | 126 |
| | Korrektheit des Beweissystems | 128 |
| | Diskussion | 129 |
| 5.6 | Fallstudie: Finde positives Element schneller | 131 |
| 5.7 | Verändern von Interferenzpunkten | 134 |
| 5.8 | Fallstudie: Parallele Nullstellensuche | 139 |
| | Schritt 1. Vereinfachung des Programms | 139 |
| | Schritt 2. Beweis der partiellen Korrektheit | 140 |
| 5.9 | Übungsaufgaben | 143 |
| 5.10 | Bibliographische Anmerkungen | 145 |
| 6 | Parallele Programme mit Synchronisation | 147 |
| 6.1 | Syntax | 148 |
| 6.2 | Semantik | 149 |
| 6.3 | Verifikation | 150 |
| | Partielle Korrektheit | 150 |
| | Korrektheit des Beweissystems | 152 |
| | Schwache totale Korrektheit | 153 |
| | Totale Korrektheit | 154 |
| | Korrektheit des Beweissystems | 156 |
| 6.4 | Fallstudie: Erzeuger/Verbraucher-Problem | 158 |
| 6.5 | Fallstudie: Wechselweiser Ausschluß | 163 |
| | Formulierung des Problems | 163 |
| | Verifikation | 166 |
| | Peterson's Lösung | 166 |
| | Dijkstra's Lösung | 170 |
| 6.6 | Verändern von Interferenzpunkten | 173 |
| 6.7 | Fallstudie: Synchronisierte Nullstellensuche | 175 |
| | Schritt 1. Vereinfachung des Programms | 175 |
| | Schritt 2. Zerlegung der Verifikationsaufgabe | 176 |
| | Schritt 3. Beweis der Terminierung | 177 |
| | Schritt 4. Beweis der partiellen Korrektheit | 181 |
| 6.8 | Übungsaufgaben | 183 |
| 6.9 | Bibliographische Anmerkungen | 185 |
| 7 | Nichtdeterministische Programme | 187 |
| 7.1 | Syntax | 187 |
| 7.2 | Semantik | 188 |
| | Eigenschaften der Semantiken | 189 |
| 7.3 | Vorteile nichtdeterministischer Programme | 191 |

| | | |
|----------------------|--|-----|
| | Symmetrie | 191 |
| | Laufzeitfehler | 192 |
| | Nichtdeterminismus | 192 |
| | Modellierung von Parallelität | 193 |
| 7.4 | Verifikation | 193 |
| 7.5 | Fallstudie: Wohlfahrtsbetrüger | 196 |
| 7.6 | Transformation paralleler Programme | 199 |
| 7.7 | Übungsaufgaben | 202 |
| 7.8 | Bibliographische Anmerkungen | 204 |
| 8 | Verteilte Programme | 207 |
| 8.1 | Syntax | 208 |
| | Sequentielle Prozesse | 208 |
| | Verteilte Programme | 210 |
| 8.2 | Semantik | 212 |
| 8.3 | Transformation verteilter Programme | 214 |
| | Semantische Beziehung zwischen S und T(S) | 215 |
| 8.4 | Verifikation | 217 |
| | Partielle Korrektheit | 217 |
| | Schwache Totale Korrektheit | 218 |
| | Totale Korrektheit | 219 |
| | Beweissysteme | 220 |
| 8.5 | Fallstudie: Übertragungsproblem | 222 |
| | Schritt 1. Zerlegung der Verifikationsaufgabe | 223 |
| | Schritt 2. Partielle Korrektheit | 223 |
| | Schritt 3. Kein Laufzeitfehler und keine Divergenz | 226 |
| | Schritt 4. Deadlock-Freiheit | 227 |
| 8.6 | Übungsaufgaben | 228 |
| 8.7 | Bibliographische Anmerkungen | 231 |
| Anhang | | 233 |
| A. | Semantik | 233 |
| B. | Beweisregeln | 235 |
| C. | Beweissysteme | 241 |
| D. | Beweisskizzen | 243 |
| Literaturverzeichnis | | 245 |
| Autorenverzeichnis | | 251 |
| Stichwortverzeichnis | | 253 |
| Symbolverzeichnis | | 257 |