

Thesen zur Diplomarbeit
„Ein Kalkül paralleler Prozesse,
Bisimulationen und Korrektheit“
von Sebastian Wilhelmi

Die lokale und weltweite Vernetzung von Rechnern gewinnt gegenwärtig explosionsartig an Bedeutung und Verbreitung. Bekanntestes Beispiel dafür ist sicherlich das Internet.

Zur Untersuchung der dabei auftretenden Phänomene, besonders bei der Untersuchung der Korrektheit von Protokollen, sind parallele Kalküle sehr gut geeignet.

Parallele Kalküle sind z.B. CSP (**C**ommunicating **S**equential **P**rocesses) von C.A.R. Hoare und CCS (**C**alculus of **C**ommunicating **S**ystems) von Robin Milner.

Ein etwas neuerer, nicht wie CSP und CCS auf Handshaking, sondern auf Broadcasting basierender Kalkül ist TCBS (**T**imed **C**alculus of **B**roadcasting **S**ystems) von K.V.S. Prasad.

Auf diesem Kalkül, wie auf vielen anderen parallelen Kalkülen, lassen sich Äquivalenzrelationen wie die starke und die schwache Bisimulation definieren.

Mit Hilfe solcher Äquivalenzen ist der Vergleich verschiedener Prozesse aus dem Kalkül möglich.

Wenn man Spezifikation und Implementation eines Problems in Form von TCBS-Prozessen vorzuliegen hat, kann man formal die Äquivalenz dieser beiden und damit die Korrektheit der Implementation beweisen. Diese Technik ist besonders gut auf Protokolle anwendbar, deren Spezifikation sehr einfach ist und deren Implementation beliebig kompliziert sein kann.

Da bei Protokollen sehr häufig keine Aussage über die Geschwindigkeit der Übertragung möglich ist, muß ein Weg gefunden werden, von der Zeit, die ein Protokoll benötigt, abzusehen. Dieses wird durch die Einführung eines neuen, leicht abgewandelten Kalküls erreicht.

Mit Hilfe dieses neuen Kalküls, der schwachen Bisimulation, der Spezifikation eines perfekten Mediums und der Implementation eines unsicheren Mediums wird plausibilisiert und definiert, wann ein Protokoll als korrekt zu gelten hat.

Das Alternating-Bit-Protokoll wird kurz eingeführt und der Beweis der Korrektheit im vorher definierten Sinne vorgestellt.