

12. Entwicklung zuverlässiger Informationssysteme

H. D. Ehrich, Technische Universität Braunschweig

Innerhalb des KORSO-Projektes befaßt sich diese Gruppe damit, die Entwicklung zuverlässiger Informationssysteme auf der Basis formaler Spezifikationen zu unterstützen. Dazu konzentriert sich die Arbeit auf die Spezifikationssprache TROLL *light*, die es erlaubt, Teile der zu modellierenden Welt als eine Gemeinschaft nebeneinander bestehender und miteinander kommunizierender Objekte zu beschreiben. Auf diese Weise bestimmen wir sowohl die Struktur als auch das Verhalten konzeptioneller Objekte. Die Spezifikationsumgebung für TROLL *light* erlaubt die Animation von Spezifikationen ebenso wie das Beweisen von Eigenschaften der Spezifikationen unter Verwendung von Theorembeispielen.

TROLL *light* ist eine Sprache zur Beschreibung von strukturellen und dynamischen Eigenschaften von Objekten. Die Beschreibung von strukturellen Eigenschaften orientiert sich in weiten Teilen an semantischen Datenmodellen.

- Die in einem Zustand beobachtbaren Eigenschaften eines Objektes werden durch Attribute beschrieben. Einfache Attribute sind daten- oder objektwertig. Darüber hinaus erlauben vordefinierte Sortenkonstruktoren wie *set* oder *tuple* auch die Spezifikation komplexer Attributbereiche.
- TROLL *light*-Objekte sind in Objekthierarchien, die sich aus Unterobjektbeziehungen ergeben, organisiert. Eine Unterobjektbeziehung ist hierbei als eine exklusive „Teil von“ – bzw. Komponentenbeziehung zu verstehen.
- Normalerweise werden Attributwerte direkt durch das Eintreten gewisser Ereignisse bestimmt. Daneben ist es auch möglich, abgeleitete Attribute zu spezifizieren, d.h. Attribute, deren Inhalte sich aus anderer gespeicherter oder abgeleiteter Information bestimmen. Zur Formulierung von Ableitungsregeln stellt TROLL *light* einen SQL-ähnlichen Anfragekalkül zur Verfügung.
- Der Anfragekalkül von TROLL *light* unterstützt auch die Spezifikation statischer Integritätsbedingungen.

Die Beschreibung von dynamischen Eigenschaften basiert auf der Spezifikation von Ereignissen. Ereignisse sind Abstraktionen von zustandsverändernden Operationen auf Objekten.

- Objekt ereignisse werden durch eine endliche Menge von Ereignisgeneratoren beschrieben. Jeder Ereignisgenerator kann mit einer Liste von Parametersorten

versehen sein. Ein Ereignisgenerator mit aktuellen Parameterwerten liefert ein Ereignis.

- Die Auswirkung von Ereignissen auf Attribute werden durch Auswertungsregeln beschrieben.
- Ereignisse in verschiedenen Objekten können durch Interaktionsregeln synchronisiert werden.
- Die möglichen Ereignisfolgen können mit Hilfe CSP-ähnlicher Prozeßbeschreibungen auf zulässige Folgen eingeschränkt werden.

Neben den Bemühungen, allgemeine theoretische Grundlagen für objektorientierte Sprachkonzepte zu entwickeln, sind auch speziell für TROLL *light* semantische Untersuchungen gemacht worden. Vielversprechend erscheinen die Arbeiten, die auf dem Gebiet der Nebenläufigkeit im Zusammenhang mit Objektorientierung von Meseguer erstellt wurden. Auf dieser Basis wurde von Meseguer die logische Programmiersprache Maude entwickelt, die auf einer fundierten Modelltheorie basiert. In Maude sind wesentliche Merkmale der Nebenläufigkeit geeignet umgesetzt worden. Einer unserer Ansätze zur Semantik von TROLL *light* beschäftigt sich deshalb mit der Übersetzung von TROLL *light*-Konzepten nach Maude, um die Vorteile der zugrundeliegenden Theorie auszunutzen.

Für die Unterstützung der Spezifikation von Informationssystemen mit TROLL *light* ist eine integrierte CASE-Umgebung wünschenswert. Einer der wichtigsten Zwecke der TROLL *light*-Entwicklungsumgebung ist die Zertifizierung, die Validierung und Verifikation beinhaltet. Ein anderer Zweck, der in Zukunft betrachtet werden soll, ist die Transformation von TROLL *light*-Spezifikationen in ausführbaren Programm-Code.

Im ersten Schritt des Software-Entwicklungsprozesses, der Anforderungsanalyse, wird im wesentlichen informal gearbeitet. Dieser Schritt führt zu einer Entwurfsphase, in der ein realer Weltausschnitt in einer abstrakten TROLL *light*-Spezifikation modelliert wird. Von nun an kann die TROLL *light*-Entwicklungsumgebung für die folgenden Schritte der Entwicklung verwendet werden.

- *Validierung/Animation*: Die TROLL *light*-Spezifikation wird mit einem Animator prototypisch ausgeführt. Der Animator stellt Objektfenster zur Verfügung, die es den Benutzern ermöglichen, Objekte zu beobachten, neue Objektfenster durch Verfolgen der Unterobjektbeziehungen oder der objektwertigen Attribute zu öffnen, Zustandsübergänge durch Anklicken von Ereignissen zu initiieren, Anfragen an Objektzustände zu stellen, etc. Dies soll den Entwicklern helfen, die informale Sicht auf den realen Weltausschnitt mit der aktuellen Spezifikation zu vergleichen.
- *Verifikation*: Die TROLL *light*-Spezifikation wird bzgl. Inkonsistenzen, Mängeln und Zusicherungen geprüft.
- *Modifikation*: Validierung und Verifikation können Ergebnisse liefern, die es nötig machen, die TROLL *light*-Spezifikation zu verändern.
- *Transformation*: Die Spezifikation wird in möglicherweise mehreren Schritten in Richtung eines ausführbaren Programm-Codes transformiert.