Institut für Informatik
Universität Augsburg
D-86135 Augsburg

Nachwuchspreis der Universität Bayern e.V. (Bewerbung)

Algebraische Kalküle für hybride Systeme

von Dipl.-Math. Peter Höfner

Motivation und Überblick

Es ist allgemein bekannt, dass fehlerhafte Software in den letzten Jahrzehnten eine erschreckend hohe Zahl an Menschenleben gefordert, Umweltschäden hervorgerufen und regelmäßig zu enormen wirtschaftlichen Verlusten geführt hat. Besonders fehleranfällig sind hierbei Systeme, welche ständig mit ihrer Umwelt interagieren, da sie auf diese flexibel, aber dennoch vorhersagbar reagieren müssen. Anders als reine Softwaresysteme wie Büroanwendungen, sind Korrektheitsanforderungen in diesen Bereichen besonders hoch — ein Airbag, der sich zu spät öffnet, ist nicht akzepierbar.

Solche sicherheitskritische Systeme können meistens als so genannte *hybride Systeme* charakterisiert werden. Bei diesen Systemen besteht ein Wechselspiel zwischen *kontinuierlichem* Systemverhalten und Kontrollereignissen zu *diskreten* Zeitpunkten, die Zustandswechsel auslösen.

Anwendungsgebiete reichen von Steuerungselementen über Medizintechnik bis hin zu Avionik und Raumfahrt. Aber auch chemische und biologische Systeme können so mathematisch exakt beschrieben werden.

Hybride Systeme sind jedoch häufig so komplex, dass eine computergestützte Verifikation auch mit den heute verfügbaren großen Speicher- und Rechenkapazitäten nicht durchführbar ist. Daher wurden und werden im Forschungsvorhaben Untersuchungen zu einer kompakteren Behandlungsmöglichkeit von Verifikationsaufgaben angestellt. Zentrales Interesse finden hierbei algebraische Techniken, in denen Systeme durch Gleichungsregeln—ähnlich den aus der Schulalgebra bekannten—beschrieben werden. Die generellen Vorteile eines algebraischen Ansatzes sind vor allem Klarheit und Einfachheit, insbesondere im Hinblick auf (computerunterstützbare) Rechenregeln.

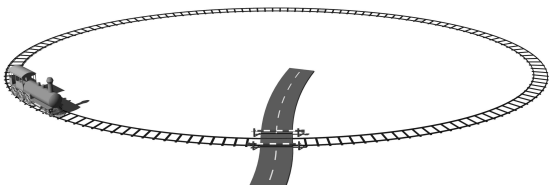

Abbildung 1: Ein einfaches hybrides System

Forschungsergebnisse

Zentraler Aspekt der hybriden Systeme ist die Interaktion mit ihrer Umgebung, d.h. die Beeinflussung durch und die Rückwirkung auf diese. Ein einfaches Beispiel für ein solches System ist die Steuerungskomponente für einen beschrankten Bahnübergang (vgl. Abb. 1). Zur Vereinfachung betrachtet man zunächst einen im Kreis fahrenden Zug, der regelmäßig den Bahnübergang quert. Der Zug und die Schranke bewegen sich nach vorgegeben mathematischen Gleichungen, welche die kontinuierlichen Komponenten beschreiben. Auch eine Veränderung der Geschwindigkeit des Zuges wird in Betracht gezogen. Die (diskrete) Steuerung des Schrankensystems übernimmt ein Computer. Selbstverständlich muss bei diesem System garantiert werden, dass die Bahnschranken geschlossen sind, sobald der Zug den Bahnübergang passiert.

Vorhandene Standardwerkzeuge für solche Verifikationsaufgaben basierten meist auf *hybriden Automaten*. Indem sie systematisch alle möglichen Abläufe des Systems modellieren, bieten sie einen allgemeinen und formalen Ansatz. Insbesondere bei der Modellierung hybrider Systeme spielen solche Automaten eine zentrale Rolle, da sie hybride Systeme visualisieren. Ein hybrider Automat, welcher das Systemverhalten des Bahnübergangs beschreibt, ist in Abbildung 2 gegeben.

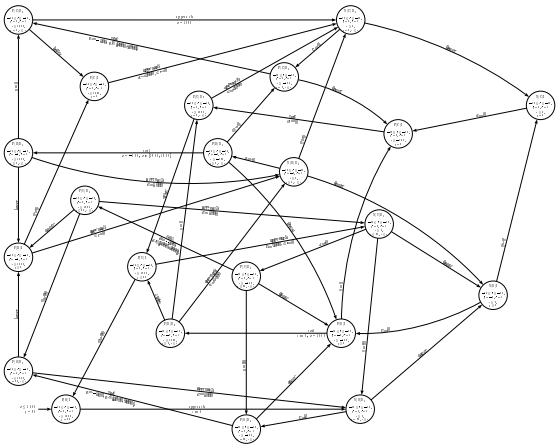

Abbildung 2: Hohe Komplexität bereits bei einfachen Beispielen

Rein formale Aussagen und Beweise über konkretes Systemverhalten, wie der zuvor beschriebene Sicherheitsaspekt, sind zwar möglich, meistens jedoch recht kompliziert und nur schwer nachvollziehbar, da die Automaten schon bei sehr kleinen Anwendungen unüberschaubar groß werden (vgl. Abb. 2). Zudem sind in den Knoten der Automaten komplexe und in ihrer Art unterschiedliche Eigenschaften beschrieben. Daher benötigen (halb)automatische Verifikationssysteme, die auf hybriden Automaten aufbauen, enorme Rechenleistung, um auch nur einfachste Ergebnisse zu erzielen. Aus diesem Grund wurden bisher bei der Automatisierung kaum Fortschritte erzielt.

Ziel des Forschungsvorhabens war es, Vorteile algebraischer Ansätze für den Bereich der hybriden Systeme nutzbar zu machen. Tatsächlich gelang es, eine algebraische Charakterisierung hybrider Systeme zu entwickeln. Diese ermöglicht es, Sicherheitsaspekte mittels einfacher algebraischer Umformungen zu überprüfen. Das System der Bahnschranke lässt sich durch den algebraischen Term

$$\big(O||(P_1 \cdot T_1 \cdot P_2)\big)\cdot \Big(\big((M_1 \cdot C)||(T_2 \cdot P_3)\big)\cdot\big(C||(T_2 \cdot P_4)_{\asymp}\big)\cdot\big((M_2 \cdot O)||(T_1 \cdot P_2)\big)\Big)^{\omega}$$

präzise und kompakt beschreiben. Aktuelle Computersysteme können mit solchen Ausdrücken wesentlich besser umgehen als mit hybriden Automaten.

Wir wollen hier nicht auf die Details des Beispiels eingehen. Es stellt sich heraus, dass für fast alle hybride Systeme die grundlegenden Operationen die Auswahl[1] (+), die sequentielle Ausführung ($\cdot$), die parallele Ausführung ($||$) und die unendliche Iteration ($^{\omega}$) sind. Mit diesen Operatoren konnten allgemeingültige Kalküle für hybride Systeme entwickelt werden. Sie ermöglichen insbesondere Aussagen über Sicherheit und Lebendigkeit. Während sich die Sicherheit mit Geschehnissen beschäftigt, die nicht eintreten sollten (z.B.: offene Schranke), versucht man mittels Aussagen über Lebendigkeit zu beweisen, dass das System immer auf Änderungen der Umwelt reagieren kann und nie in einen Blockadezustand gerät. Im oben beschriebenen Kontrollbeispiel sollte die Bahnschranke nicht nur bei der ersten Durchfahrt des Zuges geschlossen sein, sondern auch bei der 100ten oder 10.000ten Durchfahrt. Gerade in diesem Bereich hat die Algebra mit ihren einfachen Rechen- und Transformationsregeln ihre Stärke. Auch Aussagen über Invarianten (Größen die unverändert bleiben) und andere Eigenschaften, wie Stabilität von hybriden Systemen, können getroffen werden.

Ferner stellte sich heraus, dass Terme der Form $P_1 \cdot T \cdot P_2$ eine zentrale Rolle spielen. P_1 und P_2 stellen hierbei *Systemkonfigurationen* dar (z.B.: Der Zug fährt 50 $\frac{\text{km}}{\text{h}}$ und die Schranke ist geschlossen.). T hingegen beschreibt eine *Systemveränderung* über einen gegebenen Zeitpunkt (z.B.: die Schranke öffnet sich innerhalb der nächsten Minuten oder der Zug beschleunigt für 5 Minuten). Eine solche Hintereinanderausführung kann deshalb auf folgende Weise verstanden werden: Falls das hybride System die Konfiguration P_1 vor der Ausführung von T erfüllt, dann gilt danach P_2. Ein Beispiel: Fährt der Zug 50 $\frac{\text{km}}{\text{h}}$ und beschleunigt er 5 Minuten, so fährt er danach 100 $\frac{\text{km}}{\text{h}}$.

Ähnliche Konstrukte kommen auch in einem zweiten Ansatz zur Beschreibung hybrider Systeme vor. Dieser bedient sich logischer Kalküle. Ein Hauptmerkmal sind hierbei "Wenn–Dann"-Konstrukte:

– *Wenn* ein Zug 50 $\frac{\text{km}}{\text{h}}$ fährt und 5 Minuten beschleunigt, *dann* fährt er danach 100 $\frac{\text{km}}{\text{h}}$.
– *Wenn* ein Zug eine offene Bahnschranke passiert, *dann* ist das System nicht sicher.

Im letzten Jahrzehnt wurden mehr als 10 unterschiedliche Logiken für hybride Systeme eingesetzt: Angefangen von klassischer Aussagenlogik, über modale und temporale Logiken bis hin

[1] Dieser Operator kommt im Beispiel nicht vor, da beispielsweise keine Weiche modelliert wurde.

zu eigens für diese Systeme entwickelte Logiken. Die meisten dieser Logiken sind für sich wohlverstanden. Aber auf Grund der Vielzahl von verwendeten Begriffe, sowie ihrer unterschiedlichen Notation und Bedeutung ist eine uniforme Behandlung der Logiken und ihrer Beziehungen zueinander sehr schwierig.

Daher wurden im Forschungsprojekt Untersuchungen zu einer kompakteren und einheitlichen Behandlung angestellt. Zentrales Interesse finden hierbei dieselben algebraischen Techniken wie zur Beschreibung von hybriden Systemen.

Durch Algebraisierung ist es möglich, Beziehungen zwischen Logiken aufzuzeigen und, für dieses Projekt von besonderer Bedeutung, diese Logiken in einer einheitlichen und systematischen Weise auf hybride Systeme anzuwenden.

Die Forschungsergebnisse umfassen bis jetzt hauptsächlich grundlegende Methoden, münden jedoch bereits in eine kohärente Familie *algebraischer Kalküle für hybride Systeme*. Die Anwendbarkeit und Relevanz der Theorie ist durch erste Fallstudien belegt. Der entwickelte algebraische Ansatz bietet neben seiner Klarheit auch den Vorteil, dass Standard-Computer-Algebrasysteme verwendet werden können. So war es beispielsweise möglich *Theorembeweiser* einzusetzen, um fundamentale Eigenschaften hybrider Systeme automatisch herzuleiten. Theorembeweiser sind eine Softwarefamilie, die maschinengestütztes Beweisen mittels deduktiver Schlussfolgerungen ermöglichen. Der Einsatz von Standardsoftware bietet dabei die Vorteile, dass keine Entwicklungszeit für Spezialsoftware benötigt wird und keine Entwicklungskosten entstehen. Ferner könnten etwaige Fehler in einer neu entwickelten Beweis-Software Fehler in der Verifikation hybrider Systeme verursachen, welche dann wiederum Menschenleben gefährden, Umweltschäden hervorrufen oder zu enormen wirtschaftlichen Verlusten führen.

Weitere Forschungsvorhaben

Trotz der bisher erzielten Ergebnisse über hybride Systeme im Allgemeinen und hinsichtlich einer algebraischen Beschreibung im Speziellen bestehen noch viele offene Fragen.

Neben den dargestellten Beschreibungen hybrider Systeme mittels hybrider Automaten und Logiken hat sich in letzter Zeit ein dritter Ansatz herauskristallisiert: Hybride Systeme können als Spiele aufgefasst werden. Im einfachsten Fall wird das System als 2-Personen-Spiel dargestellt, in dem ein Spieler die Kontrolleinheit und der andere das System repräsentiert. Insbesondere muss sich die Kontrolleinheit zu jedem Zeitpunkt in einer Gewinnstellung befinden. In Vorstudien hat sich gezeigt, dass der algebraische Ansatz auch eine einfache Einbeziehung von 2-Personen-Spielen erlaubt. Bei feinerer Untergliederung des Systems in mehrere Subsysteme, oder bei Existenz mehrerer Kontrolleinheiten, muss das System als Mehr-Personen-Spiel aufgefasst werden, dessen Spieler zum Teil kooperieren. Algebraische Sichtweisen von Mehr-Personen-Spielen sind bisher kaum untersucht. Wir wollen konsequent Ergebnisse aus der Spieltheorie in die Theorie hybrider Systeme einbringen. Dieser Ansatz wurde bisher lediglich in sehr beschränktem Ausmaß realisiert. Wir erwarten dadurch neue Ergebnisse und Analysemethoden für hybride Systeme.

Fragen nach Lebendigkeit und Sicherheit sind nicht nur für die Informatik von Interesse, sondern spielen auch in allen Gebieten eine zentrale Rolle, in denen hybride Systeme zum Einsatz kommen, wie Physik, Ingenieurwissenschaften, Biologie, etc. So möchten wir unsere Ergebnisse als Grundlage für weitere interdisziplinäre Fallstudien verwenden.

Ausgewählte eigene Literatur

Die bisher erzielten Ergebnisse wurden bereits auf international angesehenen Tagungen präsentiert und in Zeitschriften publiziert. Desweiteren folgten Vortragseinladungen der Universitäten von Sheffield (Großbritannien) und Queensland (Australien).

[1] Höfner, P. und B. Möller: *An Algebra of Hybrid Systems.* J. Logic and Algebraic Programming, 2008. (im Druck).

[2] Höfner, P. und B. Möller: *Algebraic Neighbourhood Logic.* J. Logic and Algebraic Programming 76, Seiten 35–59, 2008.

[3] Höfner, P.: *Automated Reasoning for Hybrid Systems — Two Case Studies.* In: Berghammer, R., B. Möller und G. Struth (Herausgeber): *Relations and Kleene Algebra in Computer Science*, Band 4988 der Reihe *LNCS*, Seiten 191–205. Springer, 2008.

[4] Höfner, P. und G. Struth: *Automated Reasoning in Kleene Algebra.* In: Pfennig, F. (Herausgeber): *Automated Deduction — CADE-21*, Band 4603 der Reihe *LNAI*, Seiten 279–294. Springer, 2007.