Universität Rostock

Traditio et Innovatio

Literaturarbeit

Verifikation von Petrinetzen

Vorgelegt von:

Tom Meyer

Matrikel-Nr.: 8200839

Eingereicht am:

29. März 2019

Betreuer:

Karsten Wolf

UNIVERSITÄT ROSTOCK | FAKULTÄT FÜR INFORMATIK UND ELEKTROTECHNIK

Lehrstuhl für Theoretische Informatik

Albert-Einstein-Straße 22, 18059 Rostock | Tel: +49 381 498 7641

Abstract

Betreuer: Karsten Wolf

Tag der Ausgabe: 05.03.2019
Tag der Abgabe: 29.03.2019

Inhaltsverzeichnis

1 Einleitung

Eines der ältesten und verbreitetsten Modelle zur Beschreibung von, sowohl sequentiellen, als auch parallelen Rechnern, ist der endliche Automat.

Automaten eigenen sich um Aussagen über bestimmte Eigenschaften der beschriebenen Systeme zu treffen. Eine erschöpfende Analyse wird jedoch bei größeren Modellen immer schwieriger, da die Anzahl der möglichen Zustände die angenommen werden können, gewöhnlich exponentiell mit der Größe des Sytems wächst. Dieses Phänomen wird als Zustandsexplosion bezeichnet und ist eines der größten Hindernisse im Gebiet der Softwareverifikation.

Gerade bei Verteilten Systemen ist es aber selten nötig Auswirkungen von Aktionen über den gesamten Zustandsraum zu prüfen. Viele Aktionen haben nur einen sehr lokalen Einfluss und können nur bestimmte Teile des Zustands verändern. Die Konstruktion des kompletten Zustandsraums ist also nicht unbedingt notwendig um bestimmte Eigenschaften zu überprüfen.

Das war auch einer der Gedanken die Carl Adam Petri umtrieb und ihn dazu inspirierte einen anderen Fromalismus zur Beschreibung von Computern zu entwickeln. Die nach ihm benannten Petri Netze.

Petri Netze haben einigie interessante Eigenschaften die man in der Verifikation gut ausnutzen kann. Bevor wir allerdings zur Verifikation mit Petri netzen kommen, sehen wir uns im folgenden Kapitel diese Eigenschaften etwas genauer an.

2 Petri Netze

Petrinetze sind Bipartiete gerichtete Grafen mit Kanten. D.h. sie bestehen aus zwei Disjunkten Knotenmengen – **Stellen** und **Transitionen** – die nur mit der jeweils anderen Menge durch Kanten verbunden sind.

Die Stellen (oder auch Plätze) können mit einer beliebigen Menge an **Marken** belegt sein. Die Menge der Marken auf allen Stellen repräsentiert den aktuellen Zustand des Systems und wird **Markierung** genannt.

Transitionen repräsentieren die möglichen **Aktionen** des Systems. Eine Transition ist **aktiviert**, wenn auf allen Stellen die mit eingehenden kanten verbunden sind, mindestens eine Marke liegt (bzw. eine Menge entsprechend der Kantengewichte). Eine **aktivierte** Transition kann zu einem beliebigen Zeitpunkt **feuern**.

Feuert eine Transition werden auf allen Stellen, die mit eingehenden Kanten verbunden sind, Marken **konsumiert** und auf allen Stellen die mit einer Ausgehenden Kante verbunden sind werden Marken **produziert**. Auch hier ist die Menge der konsumierten und produzierten Marken gleich des Kantengewichts der dazugehörigen Kante.

Somit kann ein Petrinetz als Sechs-Tupel [S, T, F, W, m_0] definiert werden mit:

- S - Menge der Stellen
- T - Menge der Transitionen
- F $\subseteq \{S \times T\} \cup \{T \times S\}$ - Menge der Kanten
- W: $F \to \mathbb{N} \setminus \{0\}$ - Menge der Kantengewichte
- m_0: $S \to \mathbb{N} \cup \{0\}$ - Anfangsmarkierung der Stellen

Auf dieser Definition aufbauend können wie erwähnt einige wichtige Eigenschaften hergeleitet werden. Die Details sind außerhalb des Umfangs dieser Arbeit, deswegen beschränken wir uns auf eine Informale Beschreibung der drei Wichtigsten.

2.1 Linearität des Schaltens

Petrinetze lassen sich als lineare Gleichungssysteme darstellen. Dadurch können die Regeln der linearen Algebra auf das System anwenden.

Mittels der **Zustandsgleichung** kann durch einfache Lösung des Gleichungssystems z.B. bereits eine Aussage darüber getroffen werden welche Markierung `nicht` von der Anfangsmarkierung aus erreicht werden können.

Außerdem lassen sich durch Stellen- und Transitionsinvarianten Aussagen über die Lebendigkeit und Beschränktheit des Systems treffen. Ob ein System Deadlocks hat ist z.B. eng mit der Lebendigkeit des Netzes verbunden.

2.2 Monotonie des Schaltens

Im Gegensatz zu anderen Formalismen

monotonie -¿ Ein weg den man in einer markierung gehen kann, kann man auch in einer größeren markierung gehen
localität Aktionen betreffen jeweils nur einen Teil des Zustandsraumes “Lokalitätsprinzip”C.A.Petri(Dis
-¿ kann man beim explizieten modellchecking ausnutzen

3 Verifikation

explizit -¿ zustandsraum suche
zustandsraum klein halten
ünendlich -¿ überdeckungsgraph (monotonie)
strtukturtheorie -¿ Zustandsgleichung (linearität)
transitionsinvarianten (linearität)
sweepline (linearität)
symmetrie (localität)
stubborn sets (localität)
kann man teilweise zusammenführen für noch bessere ergebnisse

4 Verwandte Arbeiten

5 Zusammenfassung

Literaturverzeichnis