Name

Spezifikationsgesteuerte Abstraktionsverfeinerung für die formale Verifikation analoger Schaltungen (im Titel lassen sich umlaute nur auf die alte Weise mit slash schreiben)

Masterarbeit

Entwurfsmethodik
Institut für Informatik

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Masterarbeit

Institut für Informatik
Fachbereich Informatik und Mathematik

Spezifikationsgesteuerte Abstraktionsverfeinerung für die formale Verifikation analoger Schaltungen (im Titel lassen sich umlaute nur auf die alte Weise mit slash schreiben)

Name
Matrikel-Nr.: 1234567

Prüfer:
Prof. Dr. L. Hedrich
Prof. Dr. U. Brinkschulte

Betreuer:
M. Sc. Julius von Rosen

Abgabedatum:
14. Mai 2010

Frankfurt am Main, 29. Juni 2022

Danksagung

Hier könnte Ihre Werbung stehen! (A tribute to JD)

Eidesstattliche Versicherung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Hilfsmittel angefertigt habe.

Frankfurt am Main, 29. Juni 2022

Name

Aufgabenstellung

Verfahren zum Model-Checking analoger Schaltungen basieren auf einer vollständigen Diskretisierung des Zustandsraums. Diese Diskretisierung überführt den kontinuierlichen Zustandsraum in eine Graph-Datenstruktur, auf der temporallogische Model Checking - Algorithmen angewendet werden können. Diese vollständige Diskretisierung des Zustandsraums vor Anwendung der Verifikationsalgorithmen ist sehr rechenzeitintensiv und abhängig von der auszuwertenden Spezifikation wird nur ein kleiner Teil des erzeugten Modells untersucht.

Dementsprechend ist das Ziel dieser Arbeit, eine Methodik zu entwickeln, die abhängig von der zu klassifizierenden Spezifikation eine Verifikation nur auf den relevanten Teilen des Zustandsraums durchführt. Dies soll auf Basis einer Abstraktionsverfeinerung durch schrittweise Exploration des Zustandsraums erfolgen, womit eine on-demand Diskretisierung der relevanten Zustandsraumgebiete durch transiente Simulationstrajektorien erreicht wird.

Als Arbeitsumgebung wird eine Schnittstelle zu einem Simulationswerkzeug für analoge Schaltungen für die Abtastung des Zustandsraums sowie eine auf GNU Octave basierende Entwicklungsumgebung zur Verfügung gestellt.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AABB	*Axis-Aligned Bounding Box*
DEA	*Deterministischer endlicher Automat*
NEA	*Nichtdeterministischer endlicher Automat*
LTL	*Linear Temporal Logic*
CTL (-AT) ..	*Computation Tree Logic (- Analog Timed)*
ASL	*Analog Specification Language*
DAE	*Differential Algebraic Equation (dt. Algebro-Differentialgleichung)*
CMRR	*Common Mode Rejection Ratio (dt. Gleichtaktunterdrückungsverhältnis)*
PSRR	*Power Supply Rejection Ratio (dt. Netzstörungsunterdrückungsverhältnis)*
SR	*Slew Rate (dt. Flankensteilheit)*
VCO	*Voltage-Controlled Oscillator (dt. Spannungsgesteuerter Oszillator)*
OG	*Obergrenze eines Intervalls*
UG	*Untergrenze eines Intervalls*

Formelverzeichnis

$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\vec{x}$	Skalar oder Vektor
$\vec{x}_i$	i-te Komponente des Vektors x
t	Zeit
$[UG, OG]$	Intervall mit Untergrenze UG und Obergrenze OG
τ	Überschneidungsgrad zweier Bounding Boxen (in %)
dim	Dimension des Zustandsraums
sw_i	Schrittweite der Transition$_i$
sw_j^{OG}	Schrittweitenobergrenze der Punktmengentransition$_j$ (durchschnittliche Schrittweite der Transitionen der Punktmenge)
$f(x)$	Skalar- oder vektorwertige Funktion in Abhängigkeit von x
$\dot{x}(t) = \frac{dx}{dt}$	Erste Ableitung des Vektors x
$f\big(\dot{x}(t), x(t), t\big) = 0$ ...	Algebro-Differentialgleichungssystem
$\mathcal{A}$	Menge
A	Operator einer temporalen Logik
Φ	Ausdruck in temporaler Logik
KS	Zustandsgraph in Kripke-Struktur

1 Einleitung

Seit fast einem halben Jahrhundert existiert das von Gordon Moore formulierte Gesetz, dass sich die Transistoranzahl auf einem Chip innerhalb von zwei Jahren verdoppelt. Dieser rapide wachsenden Schaltungskomplexität versuchen seit jeher Industrie und Forschung mit verbesserten Entwurfsprozessen zu begegnen. Gerade der in der Industrie vorherrschende Innovationsdruck für neue Produkte und die immer kürzer werdende Lebensdauer eben dieser, fordern einen Schulterschluss. Doch in der Realität existiert ein sogenannter, stetig wachsender ‚Design Gap' zwischen der Schaltungskomplexität und dem Entwurfsprozess. Abstrakt formuliert, zeigt der ‚Design Gap' den Unterschied der theoretisch fertigbaren und der praktisch entwerfbaren Schaltungen.

...

Aufbau dieser Arbeit

Diese Arbeit betrachtet ...

2 Grundlagen

Dieses Kapitel beschreibt die Grundlagen, ...

2.1 Von der Spezifikation zur Verifikation

Bei der Herstellung von analogen, digitalen oder mixed-signal Schaltungen wird von der Idee bis zur Fertigstellung ein definierter Prozess durchlaufen. Dieser beinhaltet folgende Schritte:

1. die Spezifikation
2. den Entwurf
3. die Fertigung
4. den Test

...

Grammatik (2.1) repräsentiert die Erweiterung der CTL - Syntax um die Neuerungen von CTL-A und CTL-AT.

$$\begin{aligned} \Phi \;:=\; & a \mid z * v \mid \Phi \circ \Psi \mid \neg \Phi \\ & \mid \triangleright \diamond \Phi \mid \triangleright \Phi \, U \, \Psi \mid \triangleright \diamond^{-1} \Phi \mid \triangleright \Phi \, U^{-1} \, \Psi \\ & \mid \triangleright \diamond \Box \Phi \mid \triangleright \Phi \, U \, \Box \Psi \mid \triangleright \diamond^{-1} \Box \Phi \mid \triangleright \Phi \, U^{-1} \, \Box \Psi \end{aligned} \tag{2.1}$$

Zieht man [HaKl04] für die Beschreibung der CTL-AT - Syntax die Grundlage der CTL-Syntax auf Tabelle 2.1 , die Erweiterung aus Tabelle 2.1 auf Seite 3und die neu formulierten Zeitbedingungen hinzu, erhält man Tabelle 2.1. Die neuen Variablen und die analogen Operatoren reihen sich direkt nach der bool'schen Zustandsvariablen ein. Abgeschlossen wird die Syntaxbeschreibung nun von dem Vergangenheitsoperator und den Zeitbedingungen. Diese werden an die temporalen Operatoren, mit Ausnahme des X-Operators, als Zeitintervall angehängt, sodass eine minimale und maximale zeitliche Pfadlänge definiert ist. Eine Operatorenschreibweise $\triangleright \, X \, \Box \, \Phi$ bzw. $\triangleright \, X^{-1} \, \Box \, \Phi$ ist nicht zulässig.

...

Tabelle 2.1: Beschreibung der CTL-AT - Syntax (Quelle: [Plat04, S. 10])

a	Bool'sche Zustandsvariable	
z	Kontinuierliche Zustandsvariable	
v	Reeller Zahlenwert ($\mathbb{R}$)	
$*$	Analoge Operatoren	$>=$ größer
		$<=$ kleiner
$\circ$	Bool'sche Operatoren	$\vee$ = oder
		$\wedge$ = und
$\neg$		$\neg$ = nicht
$\triangleright$	Pfadquantoren	A = auf allen Pfaden
		E = auf mindestens einem Pfad
$\diamond$	Temporale Operatoren	X = nächster Zeitschritt (neXt)
		F = irgendwann (Finally)
		G = immer (Globally)
U		U = bis (Until)
$^{-1}$	Vergangenheit	Umkehrung der Zeit
$\square$	Zeitintervall	$[t_{low}, t_{high}]$ mit: $t_{low} \in \mathbb{R}_0^+,\ t_{high} \in \mathbb{R}^+$ $t_{low} \leq t_{high}$

3 Zusammenfassung und Ausblick

Im Rahmen dieser ...

Ausblick

...

Literaturverzeichnis

[HaKl04] W. Hartong, R. Klausen, L. Hedrich, *Formal Verification for Nonlinear Analog Systems: Approaches to Model and Equivalence Checking*, S. 205–245, Kluwer Academic Publishers, Boston, 2004

[Plat04] D. Platte, *Model-Checking analoger Schaltungen unter Berücksichtigung von Zeitbedingungen*, Diplomarbeit, Institut für Mikroelektronische Systeme, Universität Hannover, 2004

A Die Operationen

...

A.1 Die Operatoren E und U

Die $E\,\Phi\,U\,\Psi$ - Operation

Die Operationen dienen dem Model-Checking als eine Prüfinstanz der Eigenschaften und der Spezifikation. Dazu werden der Schaltung mittels der Operatoren sinnbildlich Fragen gestellt, deren Antworten die Richtigkeit einer Eigenschaft/Bedingung widergeben. Die für die $E\,\Phi\,U\,\Psi$ - Operation formulierte Frage würde wie folgt aussehen:

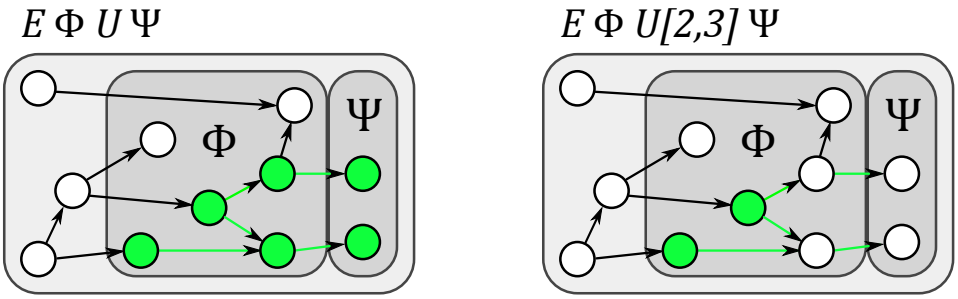
Auf welchen Pfaden gilt Φ, bis unmittelbar danach Ψ gilt?

Im **zeitunbeschränkten** Fall, werden durch $E\,\Phi\,U\,\Psi$ die Zustände in die Ergebnismenge eingefügt, die auf einem Pfad in Φ liegen, welcher unmittelbar nach Φ in Ψ landet. Für die gefundenen Zustände gilt somit, dass auf mindestens einem Pfad Ψ unmittelbar auf Φ folgt. Eine **Zeitbeschränkung** erschwert die Erfüllbarkeit von $E\,\Phi\,U\,\Psi$. Der Operator $E\ \Phi\ U\,[t_{low}, t_{high}]\ \Psi$ restriktiert die Erfüllung auf ein Zeitintervall. Nur Zustände von Pfaden, die innerhalb von $[t_{low}, t_{high}]$ von Φ unmittelbar nach Ψ kommen, werden zur Ergebnismenge hinzugefügt. Daraus lässt sich ableiten, dass folgende Teilmengenrelation zu gelten hat:

$$E\ \Phi\ U\,[t_{low}, t_{high}]\ \Psi\ \subseteq E\,\Phi\,U\,\Psi.$$

Abbildung A.1 zeigt einen Zustandsgraphen und die jeweilige Ergebnismenge, die aus der Fallunterscheidung ‚keine und eine zeitlichen Begrenzung' resultiert. Die grün markierten Knoten stellen die Zustände dar, die in der Ergebnismenge enthalten sind. Des Weiteren zeigen die grünen Kanten die Pfade an, anhand denen die Ergebnismenge zur Erfüllung der CTL-AT - Operationen bestimmt wurde. Diese Angaben gelten für das restliche Kapitel.

...



(a) (b)

Abbildung A.1: Beispielhafter Zustandsgraph für die $E\,\Phi\,U\,\Psi$ - Operation mit Fallunterscheidung in Zeitunbeschränkung A.1(a) und Zeitbeschränkung A.1(b)