TECHNISCHE UNIVERSITÄT WIEN

DISSERTATION

Distribution Recovery in Probabilistic Loops

ausgeführt zum Zwecke der Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften unter der Leitung von

Univ. Prof. Ph.D Efstathia Bura
E105-08 – Institut für Stochastik und Wirtschaftsmathematik, TU Wien

und

Univ. Prof. Dott. Ric. Ezio Bartocci
E191-01 – Cyber-Physical Systems, Fakultät für Informatik, TU Wien

eingereicht an der Technischen Universität Wien
Fakultät für Mathematik und Geoinformation

von

Andrey Kofnov
Matrikelnummer: 12124539
Steinbruchstraße 4/4/9
1160 Wien

Diese Dissertation haben begutachtet:

1. **Univ. Prof., Ph.D. Efstathia Bura**
   Institut für Stochastik und Wirtschaftsmathematik, Technische Universität Wien, Österreich
2. **Univ. Prof., Dott. Ric. Ezio Bartocci**
   Fakultät für Informatik, Technische Universität Wien, Österreich
3. **Prof., Ph.D. Mirco Tribastone**
   Systems Security Modelling and Analysis research unit, School for Advenced Studies Lucca, Italy
4. **Prof., Ph.D. Max Tschaikowski**
   Department of Computer Science, Aalborg University, Denmark

Wien, am 27. März 2025

Kurzfassung

Diese kumulative Dissertation behandelt die Wiederherstellung von Verteilungen in probabilistischen Schleifen (Kapitel 2 & 3) sowie die Berechnung von oberen und unteren Schranken der kumulativen Verteilungsfunktion für die Ausgabe neuronaler Netze mit zufälligen Eingaben (Kapitel 4).

Viele stochastische dynamische Systeme mit kontinuierlichem Zustandsraum lassen sich als probabilistische Programme mit nichtlinearen, nicht-polynomialen Aktualisierungen in nicht verschachtelten Schleifen modellieren. Wir präsentieren zwei Methoden – eine approximative und eine exakte – zur automatischen Berechnung von momentenbasierten Invarianten für solche probabilistischen Programme in geschlossener Form als Funktion der Schleifeniteration, ohne auf Stichproben zurückzugreifen. Die exakte Methode ist für probabilistische Programme mit trigonometrischen und exponentiellen Aktualisierungen anwendbar und in das Tool Polar eingebettet. Die approximative Methode zur Momentenberechnung ist für beliebige nichtlineare Zufallsfunktionen geeignet, da sie die Theorie der polynomialen Chaos-Entwicklung nutzt, um nicht-polynomiale Aktualisierungen durch eine Summe orthogonaler Polynome zu approximieren. Dadurch wird das dynamische System in eine nicht-verschachtelte Schleife mit polynomialen Aktualisierungen überführt und somit mit dem Polar-Tool kompatibel, das die Momente beliebiger Ordnung der Zustandsvariablen berechnet. Wir evaluieren unsere Methoden anhand zahlreicher Beispiele, die von der Modellierung der Geldpolitik bis hin zu physikalischen Bewegungssystemen in unsicheren Umgebungen reichen. Die experimentellen Ergebnisse belegen die Vorteile unseres Ansatzes im Vergleich zum aktuellen Stand der Technik.

In Kapitel 3 stellen wir die K-Serien-Methode vor, um die Verteilung aller Zufallsvariablen, die in jeder Iteration einer probabilistischen Schleife erzeugt werden, aus ihren Momenten abzuleiten. Diese Methode ist direkt anwendbar auf die probabilistische Analyse von Systemen, die als probabilistische Schleifen dargestellt werden können, also auf Algorithmen, die nichtdeterministische Prozesse aus Bereichen wie Robotik, Makroökonomie, Biologie sowie Software- und cyber-physikalische Systeme ausdrücken und implementieren. Die K-Serien-Methode approximiert statisch die gemeinsamen und marginalen Verteilungen eines Vektors kontinuierlicher Zufallsvariablen, die in einer probabilistischen, nicht-verschachtelten Schleife mit nichtlinearen Zuweisungen aktualisiert werden, unter der Annahme einer endlichen Anzahl von Momenten der unbekannten Dichte. Darüber hinaus leitet K-Serien die Verteilung der Zufallsvariablen eines Systems symbolisch als Funktion der Schleifeniteration her. Die Dichteschätzungen mittels K-Serien sind präzise, effizient und schnell berechenbar. Wir demonstrieren die Anwendbarkeit und Leistungsfähigkeit unseres Ansatzes anhand mehrerer Benchmark-Beispiele aus der Fachliteratur.

Das Problem der Schätzung der Verteilung der Ausgabe eines neuronalen Netzwerks (NN), wenn der Input zufällig gestört wird, wird in Kapitel 4 behandelt. Dort leiten wir exakte obere und untere Schranken für die kumulative Verteilungsfunktion (CDF) der Ausgabe eines NN über dessen gesamten Definitionsbereich ab, wobei stochastische (rauschende) Eingaben berücksichtigt werden. Die oberen und unteren Schranken konvergieren mit zunehmender Auflösung zur tatsächlichen cdf

über ihrem Definitionsbereich.

Unsere Methode gilt für jedes Feedforward-NN, das kontinuierliche, monoton wachsende, stückweise zweimal stetig differenzierbare Aktivierungsfunktionen verwendet (z. B. ReLU, tanh und softmax), sowie für konvolutionale NNs, die über den Geltungsbereich konkurrierender Ansätze hinausgehen. Die Neuheit und das zentrale Werkzeug unserer Methode besteht darin, allgemeine NNs mit ReLU-NNs zu beschränken. Die auf ReLU-NNs basierenden Schranken werden dann verwendet, um die oberen und unteren Schranken der CDF der NN-Ausgabe abzuleiten.

Experimente zeigen, dass unsere Methode garantierte Schranken für die Vorhersage der Ausgabeverteilung über deren Definitionsbereich liefert und somit exakte Fehlergrenzen bietet, im Gegensatz zu konkurrierenden Ansätzen.

Abstract

This is a cumulative thesis on distribution recovery in probabilistic loops (Ch. 2 & 3) and the computation of upper and lower bounds of the cumulative distribution function for the output of neural networks with random inputs (Ch. 4).

Many stochastic continuous-state dynamical systems can be modeled as probabilistic programs with nonlinear non-polynomial updates in non-nested loops. We present two methods, one approximate and one exact, to automatically compute, without sampling, moment-based invariants for such probabilistic programs as closed-form solutions parameterized by the loop iteration. The exact method applies to probabilistic programs with trigonometric and exponential updates and is embedded in the POLAR tool. The approximate method for moment computation applies to any nonlinear random function as it exploits the theory of polynomial chaos expansion to approximate non-polynomial updates as the sum of orthogonal polynomials. This translates the dynamical system to a non-nested loop with polynomial updates, and thus renders it conformable with the POLAR tool that computes the moments of any order of the state variables. We evaluate our methods on many examples ranging from modeling monetary policy to several physical motion systems in uncertain environments. The experimental results demonstrate the advantages of our approach as compared with the current state-of-the-art.

In Chapter 3 we propose the K-series method to derive the distribution of all random variables generated at each iteration in a probabilistic loop from their moments. It is directly applicable to the probabilistic analysis of systems that can be represented as probabilistic loops; i.e., algorithms that express and implement non-deterministic processes ranging from robotics to macroeconomics and biology to software and cyber-physical systems. K-series statically approximates the joint and marginal distributions of a vector of continuous random variables updated in a probabilistic non-nested loop with nonlinear assignments given a finite number of moments of the unknown density. Moreover, K-series automatically derives the distribution of the systems' random variables symbolically as a function of the loop iteration. K-series density estimates are accurate, easy and fast to compute. We demonstrate the feasibility and performance of our approach on multiple benchmark examples from the literature.

The problem of estimating the distribution of the output of a neural network (NN) when the input is randomly perturbed is considered in Chapter 4. There we derive exact upper and lower bounds for the cumulative distribution function (cdf) of the output of a NN over its entire support subject to noisy (stochastic) inputs. The upper and lower bounds converge to the true cdf over its domain as the resolution increases. Our method applies to any feedforward NN using continuous monotonic piecewise twice continuously differentiable activation functions (e.g., ReLU, tanh and softmax) and convolutional NNs, which were beyond the scope of competing approaches. The novelty and instrumental tool of our approach is to bound general NNs with ReLU NNs. The ReLU NN-based bounds are then used to derive the upper and lower bounds of the cdf of the NN output. Experiments demonstrate that our method delivers guaranteed bounds of the predictive output distribution over its support, thus providing exact error guarantees, in contrast to competing approaches.