Bachelor-Thesis: Parallel-Implementation eines Statistischen Model Checking Verfahrens

I. PROBLEMBESCHREIBUNG

Moderne Systeme werden aufgrund von voranschreitender Automation immer komplexer und gleichzeitig haben sie eine größere Abhängigkeit von ihrer Umwelt. So müssen z.B. hochautomatisierte Fahrfunktionen in neueren Autos ihre Umwelt genau wahrnehmen - z.B. die Position des vorherfahrenden Fahrzeuges bestimmen und auf diese adäquat reagieren. Aufgrund der Variabilitäten, welche in der Umwelt auftreten können, ist ein Sicherheitsnachweis, also dass das Fahrzeug / das Assistenzsystem seine Funktion sicher ausführt nur schwer zu erbringen.

Eine mögliche Option ist es, auf Simulationen zurückzugreifen, welche mehrere verschiedene Umweltsituationen virtuell simulieren und jeweils die Güte bzw. die Sicherheit innerhalb des Simulationslaufes bewerten. Eine Absicherung des Gesamtsystems ist somit aber nicht mehr formal vollständig möglich, sondern ist von statistischer Natur. Genauer gesagt, wird zur Absicherung ein Hypothesenthest auf Basis der generierten Simulationsläufe / Trajektorien durchgeführt.

Für einen solchen, sequentiellen Hypothesen-test werden typischer Weise zufällge Simulationsläufe $x_i = \phi(x_1^i, x_2^i, \dots x_T^i)$ generiert. Hierbei entspricht $x_i = 1$ einem Simulationslauf, welcher die Anforderungen ϕ genügt und $x_i = 0$ einem, in dem die Anforderungen nicht erfüllt sind. Aus diesen wir nach jedem Simulationslauf folgender Quotient gebildet:

$$f_m = \frac{p_1^{d_m}(1-p_1)^{m-d_m}}{p_0^{d_m}(1-p_0)^{m-d_m}}$$
$$d_m = \sum_i x_i$$

wobei p_1, p_0 gewählte Grenzwerte, die jeweils 'genügend sicher' von 'zu unsicher' bestimmen. Durch vergleichen von f_m gegen Schwellwerte $f_m \geq A$ bzw. $f_m \leq B$ ergibt sich ein sequentieller Test, bei dem nach jedem neu berechneten Simulationslauf ein Test durchgeführt werden kann und falls f_m eine der beiden Bedingungen erfüllt das gesamte Testen abgebrochen werden kann und man entscheidet sich für die jeweilige Hypothese $(B : H_o; A : H_1)$.

Bei einer naiven, praktischen Umsetzung eines solchen Verfahrens kann es vorkommen, dass durch die Parallelisierung des Simulationsverfahrens die Ergebnisse verfälscht werden. So ist es möglich, dass durch die Wahl der Abbruchkrietrien der Simulationen (z.B. Timeout) bestimmte Simulationsausgänge häufiger als dem zugrunde liegenden Modell gemäß vorkommen. Dies kann im schlimmsten Fall dazu führen, dass ein System fälschlicher Weise mit einer zu hohen Erfüllwahrscheinlichkeit bewertet wird. Der Grund hierfür besteht darin, dass Simulationsläufe, welche zu Verletzungen der Anforderungen führen meistens schneller zu simulieren sind also solche, welche den Anforderungen genügt.

Um diesen Effekt zu kontern ist in dieser Arbeit zu untersuchen, ob in einem ersten Schritt die Abhängigkeit der einzelnen Samples aufgrund derer Kopplung über die Zeit hinweg geschätzt werden kann. In einem zweiten Schritt soll diese Schätzung dazu genutzt werden um die verfälschte Gewichtung mittels der Schätzung des 1. Schrittes durch eine entsprechende Gewichtung rückgängig gemacht werden kann.

Genauer können folgende Wahrscheinlichkeiten geschätzt werden:

$$p(t|x_i = 1), p(t|x_i = 0) \tag{1}$$
$$p(x_i|H_i, t) = \frac{p(x_i, t|H_i)}{p(t, H_i)} = \frac{p(t|x_i)p(x_i|H_i)}{\sum_{x_i} p(t|x_i)p(x_i|H_i)} \tag{2}$$

wobei hier x_i die Zufallsvariable ist, welche den Ausgang des unter Umständen parallelisierten Simulationslaufes beschreibt und t den Zeitpunkt beschreibt zu dem jeweils das Ergebnis vorliegt. Basierend auf der in Gleichung Equation 1 geschätzten Verteilung über die Zeitpunkte, welche die Abhängigkeit der positiven $(x_i = 1)$ oder negativen $(x_i = 0)$ Simulationsläufe beschreiben kann dadurch eine korrigierte Schätzung der Likelihood für die Hypothesen H_0 bzw. H_1 ermittelt werden (Gleichung Equation 2). Hierdurch ergibt sich somit ein korrigierter sequentieller Test:

$$f_m = \frac{p(x_i|H_1, t)}{p(x_i|H_0, t)} \tag{3}$$

II. AUFGABENSTELLUNG

Ziel der Arbeit soll es sein, zu analysieren, ob der Bias einer parallelen Implementierung eines statistical model checking Verfahrens durch das oben beschriebene Verfahren behoben werden kann. Hierzu sollen insbesondere folgende Aufgaben durchgeführt werden:

1. Einarbeitung in die Literatur bzgl. des sequentiellen statistischen Tests [5].
2. Parallele Implementierung eines einfachen Münzwurfes, welches stellvertretend für die Simulation eines komplexen Systems mit nachgelagerter Auswertung bzgl. Sicherheitseigenschaften stehen soll.
3. Implementierung einer künstlichen zeitlichen Verzögerung, gemäß einer vorher gewählten Verteilung $p(t|x_i)$.
4. Auswertung des modifizierten Tests (siehe Gleichung 3) bzgl. der zu erreichenden Güte des Tests (Fehler 1. und Fehler 2. Art).

5. Optionen:
    - Ersetzen des Münzwurfmodelles durch ein komplexeres Simulationsmodell (z.B. ACC, siehe [2])
    - Weitere Ausarbeitung der theoretischen Grundlagen des modifizierten Tests)

III. HINTERGRUNDLITERATUR

1. Problembeschreibung der Ergebnisverfälschung durch parallele Check-verfahren aufgrund von unterschiedlichen Simulationslaufzeiten für positiv und negative Beispiele (negativ: Simulationslauf erfüllt nicht die Anforderungen, positiv: Simulationslauf erfüllt Anforderungen): [1]
2. Importance sampling: [4, Chapter 29.2]
3. Statistical model checking, insbesondere sequentieller Test: [5]
4. Simulationsbasierte Verifikation von adaptive cruse control systemen (inklusive modell des Controllers): [2]

[1] Peter Bulychev, Alexandre David, Kim Guldstrand Larsen, Axel Legay, Marius Mikučionis, and Danny Bøgsted Poulsen. Checking and distributing statistical model checking. In *NASA Formal Methods Symposium*, pages 449–463. Springer, 2012.

[2] O Gietelink, B De Schutter, and M Verhaegen. Adaptive importance sampling for probabilistic validation of advanced driver assistance systems. In *Tagungsband: American Control Conference*, pages 4002–4007, 2006.

[3] O Gietelink, Bart De Schutter, and M Verhaegen. Probabilistic approach for validation of advanced driver assistance systems. *Transportation Research Record: Journal of the Transportation Research Board*, (1910):20–28, 2005.

[4] David JC MacKay. *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[5] Håkan LS Younes and Reid G Simmons. Statistical probabilistic model checking with a focus on time-bounded properties. *Information and Computation*, 204(9):1368–1409, 2006.