RÉSUMÉ

L'objectif de cette thèse est de développer des méthodes mathématiquement solides et pratiquement efficaces pour améliorer la fiabilité des systèmes logiciels. Ce travail repose sur la théorie de l'Interprétation Abstraite, un cadre formel pour l'approximation des comportements des programmes. En particulier, cette thèse se concentre sur la quantification de l'impact des variables d'entrée sur l'exécution des programmes, un aspect crucial pour garantir la correction, la performance et la sécurité des systèmes logiciels.

Pour ce faire, nous présentons un nouveau cadre quantitatif d'utilisation des entrées permettant de discriminer les variables d'entrée en fonction de leur impact sur le programme. Ce cadre permet d'identifier les variables qui affectent de manière disproportionnée le système et peut être utilisé pour certifier le comportement attendu ou révéler des défauts potentiels. La notion d'impact est paramétrique au cadre, offrant ainsi une flexibilité d'adaptation à différents contextes et exigences.

En particulier, nous explorons l'application de ce cadre quantitatif pour la vérification des propriétés intentionnelles et extensionnelles. Les propriétés extensionnelles concernent le comportement input-output d'un programme, tandis que les propriétés intentionnelles englobent également les états internes.

Les résultats présentés dans cette thèse ont été implémentés dans trois outils : Libra, Impatto et TimeSec. Les résultats expérimentaux montrent la quantification de l'impact dans divers scénarios, y compris l'évaluation de l'équité pour les réseaux de neurones et la détection des vulnérabilités liées aux canaux auxiliaires.

MOTS CLÉS

interprétation abstraite ⋆ analyse statique ⋆ méthodes formelles ⋆ vérification quantitative ⋆ réseaux de neurones ⋆ propriétés de sécurité

ABSTRACT

The aim of this thesis is to develop mathematically sound and practically efficient methods for improving the reliability of software systems. This work is grounded in the theory of Abstract Interpretation, a formal framework for approximating program behaviors. In particular, this thesis focuses on quantifying the impact of input variables on program execution, a critical aspect for ensuring correctness, performance, and security of software systems.

To achieve this, we present a novel quantitative input usage framework to discriminate between input variables based on their impact on the program. This framework allows the identification of variables that disproportionately affect the system, and can be used to certify intended behavior or reveal potential flaws. The notion of impact is parametric to the framework, providing flexibility to adapt to different contexts and requirements.

In particular, we explore the application of this quantitative framework for verifying both intensional and extensional properties. Extensional properties refer to the input-output behavior of a program, while intensional properties also encompass the internal states.

The results presented in this thesis have been implemented into three tools: Libra, Impatto, and TimeSec. Experimental results show the quantification of impact in a variety of scenarios, including the evaluation of fairness for neural networks and the detection of side-channel vulnerabilities.

KEYWORDS

abstract interpretation ⋆ static analysis ⋆ formal methods ⋆ quantitative verification ⋆ neural networks ⋆ security properties