REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED KHIDER – BISKRA
FACULTE DES SCIENCES ET DES SCIENCES DE L'INGENIEUR
DEPARTEMENT D'INFORMATIQUE

N° D'ORDRE : .....
SERIE : .....

VERIFICATION ET DIAGNOSTIC DES SYSTEMES HARDWARES/SOFTWARES

Thèse présentée pour l'obtention du diplôme de doctorat en informatique

Par

Mr. Mustapha BOURAHLA

Devant le jury composé de :

Dr. BADACHE Nadjib, Prof.	Président	USTHB
Dr. BENMOHAMED Mohamed, Prof.	Rapporteur	Université de Constantine
Dr. BARKAOUI Kamel, Prof.	Examinateur	CNAM, Paris
Dr. DJEDI Noureddine, Prof.	Examinateur	Université de Biskra
Dr. KOUDIL Mouloud, M.C.	Examinateur	INI, Alger
Dr. KIMOUR Mohamed-Tahar, M.C.	Examinateur	Université d'Annaba

Thèse soutenue le .....

خلاصة

التصديق هو مرحلة مهمة في تطوير تصميم الأنظمة المادية أو الحاسبية. فهي طريقة لإثبات أن نظام موصوف بواسطة برنامج ممثلا لتصرفه الممكن، ترضي جملة من المميزات ممثلة لتصرفه المرغوب.

عدد من التقنيات التقليدية، مثل التظاهر و الاختبار قد أثبتوا محدود يتهم، ولا يمكن أن يكونوا شاملين. في العشرية الأخيرة، يوجد توجه نحو استعمال الطرق الشكلية المعتمدة على الشكليات الرياضية من أجل الفحص الكامل للأنظمة.

نستطيع أن نميز ما بين صنفين كبيرين من الطرق الشكلية. الطرق التي تستعمل البرهان الآلي للنظريات. في هذه الطرق، التصرف الممكن لنظام يوصف بجملة من الفرضيات باستعمال نظرية رياضية مؤسسة بدقة. التصرف المرغوب يوصف بجملة من النظريات. طريقة التفحص تثبت رياضيا هذه النظريات على حسب النظرية الرياضية المؤسسة و جملة الفرضيات.

الصنف الثاني، والذي هو أساس أعمالنا المقدمة في هذه الأطروحة، هو تفحص الشكل الممثل لنظام. التصرف الممكن للنظام يوصف بواسطة شكل، على العموم يكون بشكل آلية. هذا الشكل ينتج من برنامج وصفي مقدم. التصرف المرغوب يوصف بواسطة تعبير منطقي رياضي مؤسس بدقة. ينفذ أجراء آلي من أجل اتخاذ قرار إذا كان الشكل يرضي المميزات (التصرف المرغوب).

توجد مشاكل تعترض تطبيق تقنية تفحص الشكل: يمكن أن يكون وصف نظام غير منته. يمكن أن يكون منته و لكنه جد كبير حيث يتجاوز سعة ذاكرة الحاسب. يمكن لنظام أن يكون معقد أين يصعب (أو يستحيل) إنشاء شكله، مثل الأنظمة ذات الوقت الحقيقي و الأنظمة متعددة المؤثرات (الفواعل). الأعمال المقدمة في هذه الأطروحة هي لإعطاء حلول لهذه المشاكل من أجل جعل تقنية تفحص الشكل قابلة للتطبيق لهذه الأنظمة.

من محاسن تقنية تفحص الشكل، استنتاج أمثلة مضادة عندما تكون المميزات غير محققة. هذه الأمثلة المضادة هي أثار لتنفيذات ممكنة تظهر كيف أن الشكل لا يحقق هذه المميزات. المشكل الكبير هو كيف يمكن للمصمم أن يشخص وصف الشكل مستعملا هذه الأمثلة المضادة. في هذه الأطروحة، صممنا طريقة لإدماج تقنية تفحص الشكل مع تقنية التشخيص بواسطة الشكل لمساعدة المصمم على التشخيص.

Résumé

La validation est une étape importante dans le processus de conception des systèmes hardwares ou softwares. C'est une technique pour montrer qu'un système qui est décrit par un programme représentant son comportement possible, satisfait un ensemble de propriétés représentants le comportement désiré.

Plusieurs techniques traditionnelles comme la simulation et le test, ont montrés leurs limites et elles ne peuvent pas être exhaustives. Dans la dernière décennie, il y a une grande tendance à utiliser des méthodes formelles basées sur des formalismes mathématiques pour la vérification exhaustive des systèmes.

Nous pouvons distinguer deux grandes catégories de méthodes formelles. Les méthodes qui sont basées sur la démonstration automatique des théorèmes. Dans ces méthodes le comportement possible d'un système est décrit par un ensemble d'hypothèses en utilisant une théorie mathématiquement bien fondée. Le comportement désiré est spécifié à l'aide des théorèmes. La technique de vérification est de prouver ces théorèmes selon la théorie de base et l'ensemble des hypothèses.

La deuxième catégorie qui est la base de nos travaux présentés dans cette thèse, est la vérification de modèle. Le comportement possible est décrit par un modèle, en général, sous forme d'automate. Ce modèle est généré à partir d'une spécification d'interface sous forme d'un programme. Le comportement désiré est spécifié par une logique mathématique bien fondée. Une procédure de décision automatique sera exécutée pour décider si le modèle satisfait les propriétés (comportement désiré).

L'applicabilité de la vérification de modèle rencontre des problèmes. Une spécification de système peut générer un modèle (automate) infini (un modèle à une infinité d'états). Un modèle fini peut être tout simplement très large qui dépasse la capacité de la mémoire d'un ordinateur. Un système peut être complexe (ou compliqué) où la construction de son modèle est très difficile (ou impossible) comme les systèmes temps réel et les systèmes multi-agents. Les travaux présentés dans cette thèse sont pour donner des solutions à ces problèmes afin de rendre la technique de vérification de modèle applicable pour ces systèmes.

L'un des avantages de la technique de vérification de modèle est la génération des contre exemples une fois la propriété est insatisfaite. Ces contre exemples sont des traces d'exécutions possibles montrant comment le modèle ne satisfait pas cette propriété. Le grand problème qu'un concepteur rencontre est comment diagnostiquer la spécification de modèle en utilisant ces contre exemples. Nous avons développé une approche intégrant la technique de vérification de modèle avec la technique de diagnostic basé modèle pour aider les concepteurs dans leur diagnostic.

Table des matières