Nr rejestracyjny: 2020/39/B/ST6/00521; Kierownik projektu: dr Jakub Dawid Michaliszyn

Wnioskowanie ilościowe odporne na perturbacje
Streszczenie popularnonaukowe

Systemy informatyczne coraz częściej i głębiej wnikają do naszego życia. Czasy pandemii pokazały, że niemal każdy aspekt życia, od zakupów po wizyty lekarskie, daje się realizować z użyciem nowoczesnych technologii. Mimo ciągłego rozwoju inżynierii oprogramowania, wciąż napotyka się na różnego rodzaju błędy, zarówno w sprzęcie, jak i w oprogramowaniu. Sposobem na ich wyeliminowanie ma być formalna weryfikacja, której celem jest stworzenie dowodu poprawności sprzętu lub programu. Z technik tych korzysta wiele firm komercyjnych, takich jak Bosch, Intel, ARM, Microsoft czy Facebook.

Proces weryfikacji można zautomatyzować; *automatyczna weryfikacja* jest aktywnym polem badań, gdzie zweryfikowane właściwości mają charakter jakościowy (poprawność, brak zakleszczeń itp.) lub ilościowy (wydajność, zużycie zasobów itp.). Podczas gdy automatyczna weryfikacja obejmuje szeroki zakres technik, weryfikacja modeli okazała się być techniką najbardziej praktyczną i wszechstronną.

Sprawdzanie modelu polega na zbudowaniu modelu zweryfikowanego systemu (*faza modelowania*), specyfikacji właściwości systemu (*faza specyfikacji*) i sprawdzeniu, czy model jest zgodny ze specyfikacją (*faza sprawdzania*). Odpowiedź zwrócona w fazie sprawdzania może być wartością logiczną dla właściwości jakościowych (np. model spełnia specyfikację) lub liczbą dla właściwości ilościowych (średnia liczba kroków, jakie serwer musi wykonać, aby odpowiedzieć na żądanie klienta). Należy jednak pamiętać, że odpowiedź dotyczy modelu, a nie modelowanego systemu. Jego zastosowanie w systemie i jego właściwościach zależy od dokładności faz modelowania i specyfikacji.

Zakładanie idealnej dokładności modelowania i specyfikacji jest nierealne. Musimy uwzględnić błędy w tych fazach, które mogą skutkować modelem lub specyfikacją inną niż zamierzona. Jest to jednak możliwe do naprawienia, jeśli wymagamy, aby techniki modelowania i specyfikacji były odporna na perturbacje, tzn. aby wyniki fazy sprawdzania zmieniały w kontrolowany sposób w przypadku niewielkich zaburzeń. Wtedy, nawet jeśli model nie odpowiada dokładnie systemowi, to przybliża ilościowe właściwości systemu. Podobnie, specyfikacje odporne na perturbacje dają przybliżone odpowiedzi na zapytania o właściwości ilościowe.

Celem tego projektu jest opracowanie odpornych na perturbacje formalizmów dla faz modelowania i specyfikacji, ze szczególnym naciskiem na specyfikacje ilościowe. Projekt jest podzielony na cztery zadania: pierwsze dwa zadania dotyczą modelowania, trzecie dotyczy fazy specyfikacji, a czwarte podejścia bazodanowego. Efektem projektu powinno być zarówno powstanie podwalin teoretycznych, jak i narzędzi do wnioskowania odpornego na perturbacje.