Nowe metody weryfikacji systemów wielo-agentowych i protokołów elektronicznego głosowania

Wojciech Penczek
Institute of Computer Science, PAS, Warsaw
penczek@ipipan.waw.pl

1. Opis Projektu

Systemy wielo-agentowe opisują interakcje wielu podmiotów zwanych agentami, często uważanymi za inteligentne i autonomiczne. Logika temporalna czasu alternującego **ATL*** i jej fragment **ATL** [1] są logikami, które pozwalają na wnioskowanie o strategicznych interakcjach w takich systemach, rozszerzając formalizm logiki temporalnej przez pojęcie *strategicznych umiejętności* z teorii gier. W związku z tym **ATL*** umożliwia wyrażanie własności na temat tego, co agenci (lub grupy agentów) mogą osiągnąć. Takie własności mogą być przydatne do specyfikacji, weryfikacji i wnioskowania o interakcjach agentów w systemach agentowych oraz bezpieczeństwie i użyteczności w protokołach elektronicznego głosowania. Stały się one szczególnie istotne ze względu na aktywny rozwój algorytmów i narzędzi do weryfikacji, gdzie własność "poprawności" jest zadawana przy użyciu strategicznych umiejętności [4]. Istnieje jednak kilka przeszkód. Po pierwsze, większość narzędzi i rozwiązań algorytmicznych koncentruje się na agentach dysponujących pełną informacją, tzn. agentów, którzy w dowolnym momencie gry dokładnie znają globalny stan gry, co jest oczywiście nierealistyczne za wyjątkiem najprostszych wielo-agentowych scenariuszy. Semantyka **ATL** z niepełną informacją nie posiada stało-punktowej charakteryzacji [3], co sprawia, że przyrostowa synteza strategii jest niemożliwa, a przynajmniej trudna do osiągnięcia. Po drugie, semantyka logik strategicznych jest niemal wyłącznie oparta na synchronicznych modelach gier współbieżnych. Oznacza to, że zakłada się wprost istnienie globalnego zegara, który taktuje kolejne globalne zdarzenia w systemie. Jednak wiele rzeczywistych systemów jest z natury asynchronicznych i nie działa zgodnie z globalnym zegarem, który synchronizuje kroki atomowe wszystkich komponentów.
Celem projektu jest opracowanie nowych metod weryfikacji systemów wielo-agentowych z niepełną informacją, przy użyciu logiki strategicznej interpretowanej w modelach asynchronicznych [2]. Jeśli chodzi o praktyczne zastosowania, to główny nacisk zostanie położony na procedury i protokoły głosowania, a w szczególności na ich zasadnicze cechy, takie jak poufność, nie uleganie przymusowi i weryfikowalność wyborców.

W szczególności, metody weryfikacji będą wykorzystywać następujące podejścia :

- Symboliczna weryfikacja modelowa za pomocą BDD, SAT-solverów lub SMT-solverów,
- Algorytmy inspirowane naturą, takie jak algorytm genetyczny, symulowane wyżarzanie, lub ogólny algorytm optymalizacji,
- Algorytmy hybrydowe łączące metody symboliczne i inspirowane naturą,
- Abstrakcja modeli wykorzystująca abstrakcję danych i stanów,
- Redukcje modeli, takie jak redukcje częściowo-porządkowe i wykorzystujące symetrię.

2. Profil Kandydata

Kandydat musi mieć dobre przygotowanie w zakresie logiki matematycznej, w tym logiki modalnej, a także umiejętności programowania (C, Java). Oczekuje się znajomości podstaw metod formalnych i technik weryfikacji. Kandydat powinien posiadać również dobre umiejętności komunikowania się oraz dobrą znajomość języka angielskiego w mowie i piśmie

Referencje

1. R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time Temporal Logic. Journal of the ACM, 49:672–713, 2002.

2. P. Dembiński, W. Jamroga, A. Mazurkiewicz, and W. Penczek. Towards partial order reductions for fragments of alternating-time temporal logic. Technical report, ICS PAS Report 1036, 2016.

3. C. Dima, B. Maubert, and S. Pinchinat. Relating paths in transition systems: The fall of the modal mu-calculus. In Proceedings of MFCS, volume 9234 of Lecture Notes in Computer Science, pages 179–191. Springer, 2015.

4. A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: An open-source model checker for the verification of multi-agent systems. International Journal on Software Tools for Technology Transfer, 2015. Availabe online.