Zastosowanie metod formalnych

Politechnika Warszawska

Karol Kozlowski[1], Katarzyna Mielęcka [2]

Politechnika Warszawska,
Wydzial Elektryczny

Metody formalne

Metody formalne to matematyczne techniki wspomagające projektowanie i analizę systemów informatycznych. Główną zaletą metod formalnych są **matematyczne gwarancje poprawności**, szczególnie istotne w systemach krytycznych (medycznych, transportowych). Pozwalają one identyfikować złożone błędy, takie jak zakleszczenia czy warunki wyścigu, które często wymykają się tradycyjnym metodom testowania.

Kluczowe zalety metod formalnych

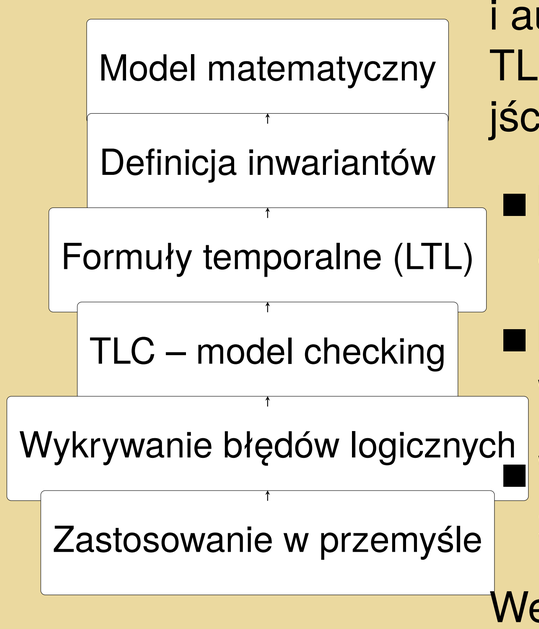
Some introduction of the list.

- Formalne gwarancje poprawności - zapewnienie matematycznie udowodnionej poprawności systemów, szczególnie w przypadku wymagań bezpieczeństwa.
- Precyzyjna specyfikacja wymagań - eliminacja niejednoznaczności dzięki matematycznym modelom i notacjom.
- Wykrywanie złożonych błędów - identyfikacja problemów takich jak zakleszczenia (deadlocks) czy warunki wyścigu (race conditions), które trudno wykryć tradycyjnymi metodami testowania.

System PVS w pigułce

pointer_env $[P : \text{TYPE}, T : \text{TYPE}] : \text{THEORY}$
BEGIN
pointer : TYPE = $P + \{\text{nil}\}$
env : TYPE = $[\text{pointer} \to (T + \{\text{undefined}\})]$
END pointer_env

Zastosowanie metod formalnych – TLA+



Metody formalne pozwalają na matematyczne modelowanie i automatyczną weryfikację systemów. TLA+ wykorzystuje trzy główne podejścia:

- **Modelowanie systemu** – zmienne, akcje, przestrzeń stanów,
- **Inwarianty** – warunki poprawności w każdym stanie,
- **Własności temporalne** – analiza zachowania w czasie.

Weryfikacja odbywa się za pomocą

Metody formalne w systemach wbudowanych

Metody formalne, takie jak RT-EFSM, Sieci Petriego z Czasem i Kolorami (TCPN) oraz metoda B, odgrywają kluczową rolę w projektowaniu, testowaniu i weryfikacji systemów wbudowanych działających w środowiskach krytycznych. Umożliwiają one precyzyjne modelowanie, analizę zachowań czasowych i współbieżnych oraz walidację zgodności z normami bezpieczeństwa, znacząco zwiększając niezawodność systemów.

Thank you for using!

For issues on the template, please visit the Github page:
`https://github.com/zhtluo/purdue-slide-template`

Bibliografia

- Leslie Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley, 2002.
- Chris Newcombe et al., *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, 2015.
- Igor Konnov, Jure Kukovec, Thanh-Hai Tran, *TLA+ Model Checking Made Symbolic*, CAV 2019.
- Hillel Wayne, *Practical TLA+: Planning Driven Development*, Lospinato Books, 2018.
- S. Poreda, *Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych*, Uniwersytet Warszawski, 2023.
- Sławomir Lasota, *Weryfikacja protokołu Needhama-Schroedera przy użyciu narzędzi SPIN i UPPAAL*, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski,
- Igor Wojnicki, *Weryfikacja własności systemów współbieżnych z użyciem metod formalnych*, Praca doktorska, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, 2019,
- Leslie Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley, 2002.
- Chris Newcombe et al., *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, 2015.
- Igor Konnov, Jure Kukovec, Thanh-Hai Tran, *TLA+ Model Checking Made Symbolic*, CAV 2019.
- Hillel Wayne, *Practical TLA+: Planning Driven Development*, Lospinato Books, 2018.
- S. Poreda, *Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych*, Uniwersytet Warszawski, 2023.
- Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, Michael Deardeuff, *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, Vol. 58, No. 4, pp. 66–73, 2015.
- Y. Yin, B. Liu and H. Ni, ”Real-time embedded software testing method based on extended finite state machine,” in Journal of Systems Engineering and Electronics, vol. 23, no. 2, pp. 276-285, April 2012, doi: 10.1109/JSEE.2012.00035.
- F. Moin, F. Azam and M. W. Anwar, ”A Model-driven Approach for Formal Verification of Embedded Systems Using Timed Colored Petri Nets,” 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 2018, pp. 2580-2584, doi: 10.1109/CompComm.2018.8780731.
- J. R. Abrial, *Modeling in Event-B: System and Software Engineering*, Cambridge University Press, 2010.Noguchi, Kenichiro. Application Of Formal Methods For Designing A Separation Kernel For Embedded Systems. Zenodo, 2010.