Formální metody v umělé inteligenci
(Tomáš Brázdil)

Formální metody studují techniky pro modelování počítačových systémů, specifikaci jejich vlastností, a automatické ověřování těchto vlastností. S jejich pomocí je možné garantovat správnou funkcionalitu a bezpečnost systémů, jejichž selhání by potenciálně vedlo ke ztrátám na lidských životech nebo značným ekonomickým škodám. Revoluční postupy využívané v AI (včetně strojového učení a hlubokých neuronových sítí) typicky neposkytují žádné garance stran správné funkcionality výsledných produktů. Výzkum na rozhraní formálních metod a AI, který se velmi dynamicky rozvíjí v celosvětovém měřítku, se snaží tento zásadní nedostatek překlenout. Navíc se ukazuje, že výsledky formálních metod, např. z oblasti algoritmické syntézy programů, temporálních logik, stochastických tahových her, apod. nacházejí přímé uplatnění při řešení problémů, které se dlouhodobě studují v rámci AI, např. v oblasti plánování nebo multiagentních systémů. Přenos poznatků probíhá ale i opačným směrem, intenzivně se zkoumá např. využití strojového učení při optimalizaci programů, kdy se současně požaduje zachování základních bezpečnostních požadavků na jejich chování.

Výzkumu na rozhraní formálních metod a AI se v ČR dlouhodobě věnuje několik výzkumných skupin:

Pracoviště (usp. je nevýznamné)	**Témata**
FIT VUT Brno, výzkumná skupina automatizované analýzy a verifikace (VeriFIT), vedoucí prof. Tomáš Vojnar, celkem 7 kmenových zaměstnanců.	Statická formální analýza a verifikace, dynamická analýza a testování, rozhodovací procedury různých logik, efektivní techniky práce s různými typy automatů, analýza pravděpodobnostních systémů, automatizovaná syntéza, aplikace formálních metod při vývoji systémů pro přibližné počítání.
FI MU Brno, Laboratoř paralelních a distribuovaných systémů (Paradise), vedoucí prof. Jiří Barnat, celkem 5 kmenových zaměstnanců)	Návrh, analýza a formální verifikace paralelních programů včetně analýzy chování vůči relaxovaným paměťovým modelům. Enumerativní a symbolické přístupy k analýze stavových prostorů počítačových systémů, aplikace metod formální analýzy na problematiku tvorby požadavků, syntéza strategií pro distribuované systémy s aplikací do multiagentních systémů a robotiky.
FI MU Brno, Laboratoř formálních metod, logiky a algoritmů (Formela), vedoucí prof. Antonín Kučera, celkem 8 kmenových zaměstnanců.	Metody pro řešení patrolovacích her s obecnou i speciální topologií, syntéza řídících strategií pro agentní systémy s omezenými zdroji (např. drony), efektivní analýza stochastických her s nekonečně mnoha stavy, metody strojového učení pro syntézu bezpečných kontrolerů softwarové systémů, metody pro automatickou analýzu a verifikaci imperativních programů, SMT solving se zaměřením na teorii bitvektorů, algoritmy pro vytváření, úpravu a zpracování automatů nad nekonečnými slovy

MFF UK Praha, vedoucí prof. František Plášil, celkem 5 kmenových zaměstnanců	Metody pro automatickou verifikaci paralelních programů a hledání chyb v interakci vláken. Detekce podezřelého/neobvyklého chování software nebo podezřelých fragmentů zdrojového kódu na základě technik strojového učení, které se aplikují na výsledky statické a dynamické analýzy různých verzí programu/software. Modelování dynamických architektur samovolně se vyvíjejících systémů (cyber-physical systems of systems) a použití stochastických metod pro detekci situací a popis koordinace systémů.
PřF UP Olomouc, skupina prof. Petra Jančara, celkem 3 kmenoví zaměstnanci.	Ověřování behaviorálních ekvivalencí a temporálních vlastností systémů, řízení a plánování výrobních procesů.

Výsledky a aplikace

- **Publikační výstupy.** Získané vědecké výsledku jsou systematicky publikovány ve sbornících flag-ship (CORE Rank A*) konferencí v oblasti formálních metod a umělé inteligence, které definují celosvětové výzkumné trendy. Zejména se jedná o konference CAV, LICS, POPL, PLDI, IJCAI, AAMAS, AAAI. Celkový počet článků publikovaných ve sbornících těchto konferencí za posledních pět let členy výše uvedených výzkumných skupin je zhruba 20.

Adekvátní je rovněž počet a kvalita publikací v impaktovaných časopisech.

Softwarové nástroje.

- DiVinE, explicit state model-checker.
- Knihovna VATA pro efektivní práci se stromovými automaty
- Nástroje Predator a Forester pro statickou analýzu programů s dynamickými datovými strukturami
- Prostředí ANaConDA pro dynamickou analýzu paralelních programů
- Nástroj Sloth pro rozhodování splnitelnosti formulí nad řetězci (spolupráce s Uppsala University a Oxford University)
- Nástroj Gaston pro rozhodování splnitelnosti formulí WS1S
- Podíl na statickém analyzátoru 2LS (spolupráce s firmou DiffBlue Ltd., Velká Británie)
- Nástroj Symbiotic pro analýzu a verifikaci sekvenčních programů v C
- SMT solver Q3B pro kvantifikované bitvektorové formule

- **Významné projekty (výběr)**

    - **Centrum excelence, Institut teoretické informatiky (2012-2018).** Projekt center excelence GAČR, spoluřešitel Antonín Kučera.
    - **European Network in Game Theory, GAMENET, (2017-2020).** Projekt COST (Antonín Kučera, MC member, WP leader).

- **TRUST 4.0 (2018-2019).** Projekt v rámci TAČR DELTA - bilaterální projekt s Německem. Tématem je použití metod pro detekci dynamických situací pro řízení přístupu v Industry 4.0 prostředí
- **AUTODEV - Automata for Decision Procedures and Verification**, GAČR 19-24397S, 2019-2021, řešitel: Lukáš Holík, spoluřešitel: Jan Strejček.
- **AQUAS: Aggregated Quality Assurance for Systems**, ECSEL JU - Horizon 2020, 8A17001, 737475, 2017-2020, koordinátor českého konsorcia Tomáš Vojnar.
- **ROBUST - Verifikace a hledání chyb v pokročilém softwaru**, GAČR 17-12465S, 2017-2019, řešitel: Tomáš Vojnar, spoluřešitel: Jan Kofroň.
- **Přibližná ekvivalence pro aproximativní počítání**, GAČR 16-17538S, 2016-2018, řešitel: Tomáš Vojnar.
- **Automatická inkrementální verifikace a odstraňování chyb pro souběžné systémy**, GAČR 18-17403S, 2018-2020, řešitel: Pavel Parízek
- **Abstrakce a jiné techniky v semi-symbolické verifikaci programů**, GAČR 18-02177S, 2018-2020, řešitel: Jiří Barnat
- **AMASS - Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems**, ECSEL JU - Horizon 2020, 8A16002, 2016-2019, spoluřešitel: Jiří Barnat

- **Spolupráce s průmyslem**
  - **Statická analýza toku dat ve složitých softwarových systémech**
    Projekt s firmou Manta. Tématem je hledání toku dat především mezi databázemi, jednotlivými moduly programů napsaných v objektově-orientovaných jazycích (Java, Scala, C#) a systémy pro zpracování velkých dat.
  - Nově přijatý projekt TAČR **AUFOVER - Automatizace Formální Verifikace** ve spolupráci FI MU, FIT VUT, Honeywell a Red Hat.
  - Dlouhodobá spolupráce skupiny VeriFIT se společností Red Hat v oblasti automatizované analýzy spotřeby zdrojů programy a také v oblasti aplikace formálních pro posuzování změn v různých verzích jádra Linux (projekt DiffKemp).
  - Spolupráce skupiny VeriFIT s firmou CAMEA na aplikaci statické formální analýza i pokročilých metod automatizovaného testování na systémy automatizovaného sledování dopravy v rámci projektu (mj. v rámci projektu **MuSiC - Mnohoúrovňová bezpečnost v kritických aplikacích počítačových systémů**, INTER-EUREKA LTE217, LTE118019, 2018-2020).

Vize rozvoje

Klíčové podmínky dalšího rozvoje špičkového výzkumu v oblasti formálních metod a souvisejícího technologického transferu do průmyslové sféry sjou následující:

- Další prohloubení mezinárodní spolupráce a posílení postavení české komunity formálních metod v celosvětovém kontextu.
- Zlepšení podmínek pro práci malých vědců, zejména v kategorii doktorských studentů a PostDoc pracovníků.

- Další prohloubení orientace na problematiku relevantní pro AI.

Rozšíření spektra řešených projektů, včetně mezinárodních a evropských projektů a společných projektů s průmyslovými partnery.