35 - Verifikace ukazatelových programů založená na lesních automatech

Martin Hruška
xhrusk16@stud.fit.vutbr.cz

Excel@FIT

Proč?

- Zvýšení kvality software
- Nalezení všech chyb (bugů) v programu
- Formální důkaz korektnosti programu vůči specifikaci
- Nerozhodnutelné problémy, či problémy s vysokou časovou složitostí

Jak?

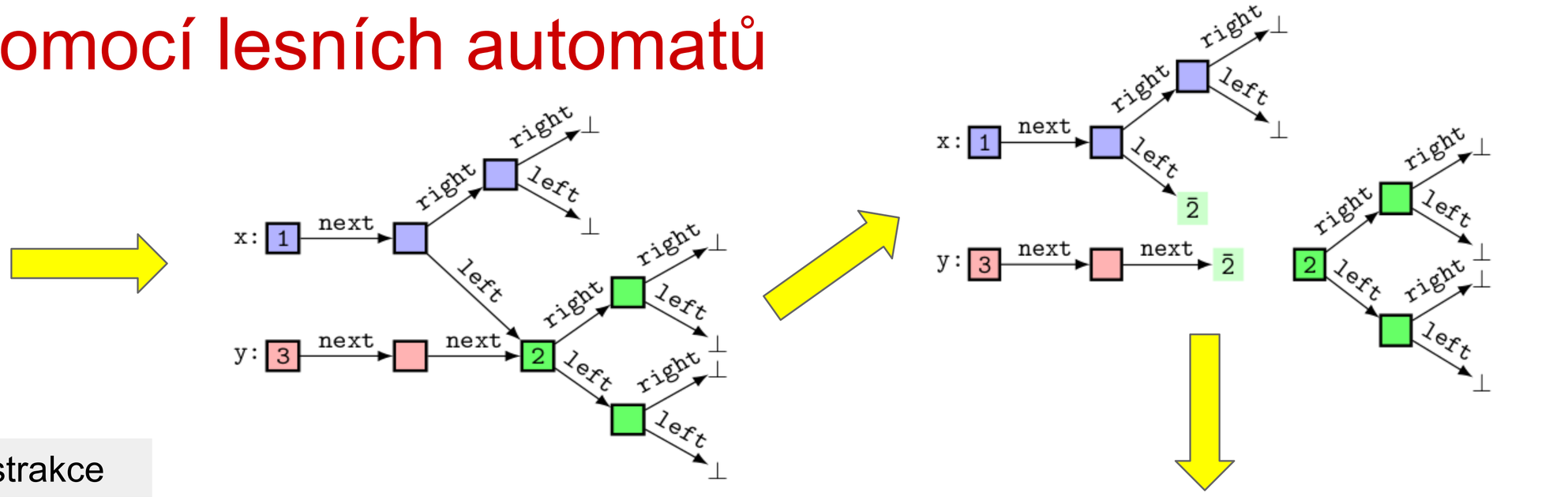
- Formální metody, konkrétně lesní automaty
- Automaty reprezentují dosažitelné stavy programu
- Lokální usuzování (jako v separační logice)
- Implementace v nástroji Forester jako GCC plug-in

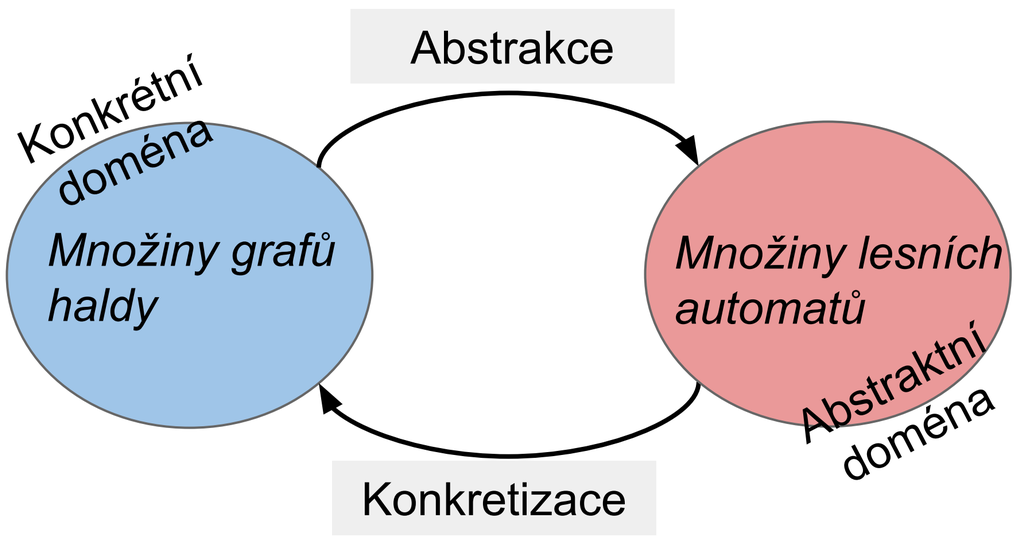
Co?

- Programy v jazyce C
- Komplexní dynamické datové struktury (např. skip list 2. a 3. úrovně)
- Detekce chyb při práci s ukazateli, či dosažitelnost chybového stavu

Verifikace pomocí lesních automatů

```
struct Tree {
  struct Tree* left;
  struct Tree* right;
  int data;
};
```





A (finite, non-deterministic, top-down) *tree automata* (over structured labels) is quadruple $A = (Q, 2^{\Gamma}, \delta, R)$ where

- Q is a finite set of states.
- Γ is a ranked alphabet.
- Δ is a set of transition rules set with rules in the form $(q, \{a_1, \ldots, a_m\}, q_1 \cdots q_n)$ where $q, q_1, \ldots, q_n \in Q$, $\{a_1, \ldots, a_m\} \in \Gamma$. Each rule could be interpreted as a sequence of the *rule-terms* $d\langle 1\rangle = q \mapsto (a_1, q_1 \cdots q_{\#a_1}) \cdots d\langle n\rangle = q \mapsto (a_m, q_{n-\#a_m+1} \cdots q_n)$ and we denote the i-th rule term of sequence again by $d\langle i\rangle$ where $i \in \{1, \ldots, m\}$.
- $R \subseteq Q$ is a finite set of root states.

Přínos této práce

ETAPS EUROPEAN JOINT CONFERENCES ON THEORY & PRACTICE OF SOFTWARE

SV-COMP'15
Soutěž ve verifikaci software

Zpětný běh

- Lesní automaty umožňují reprezentovat i nekonečný stavový prostor
- Abstrakce nad těmito automaty urychluje výpočet a zvyšuje pravděpodobnost terminace
- Abstrakce nadaproximuje množinu dostupných stavů
- Nutnost zpřesňování abstrakce ⇨ zpětný běh
- Přesnější abstrakce - predikátová abstrakce

Forester & VATA

- Lesní automaty jsou n-tice stromových automatů
- VATA je efektivní knihovna pro stromové automaty
- Využití VATA v nástroji Forester
  - Modularita
  - Udržovatelnost
  - Efektivita