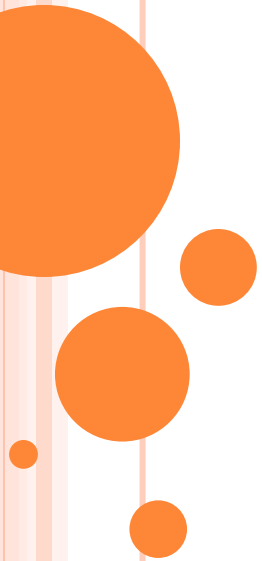
Pravdepodobnostné a nedeterministické formálne metódy pri modelovaní protokolov



Seminár umelej inteligencie
Ing. Peter Marko
21. 3. 2011

Obsah

- Metódy analýzy a verifikácie protokolov
  - Formálne, neformálne, automatické , manuálne
- Príklad pre nedeterministické modely
- Príklad pre pravdepodobnostné modely

Analyzovanie sieťových protokolov

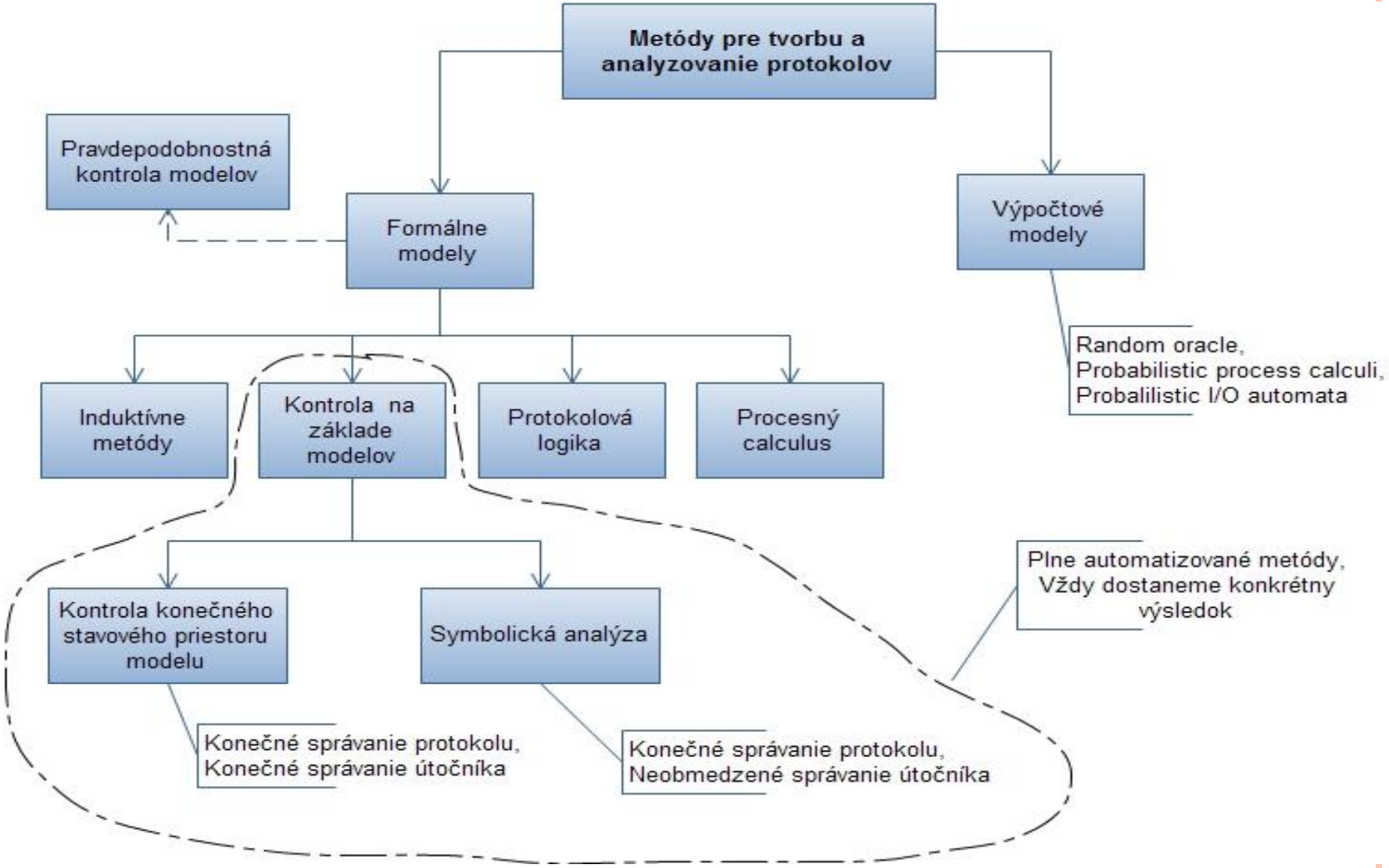
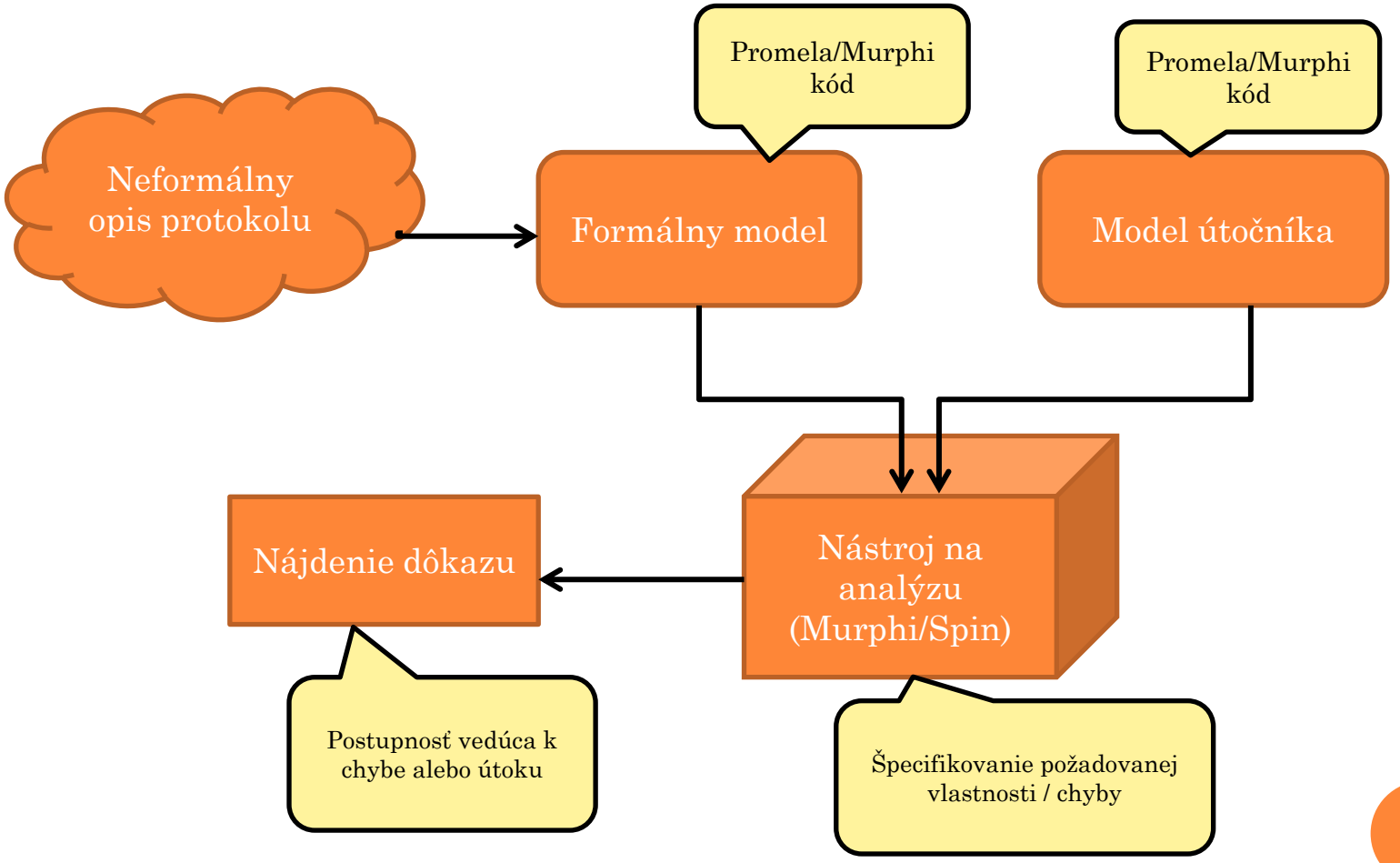


Schéma využitia formálnych deterministických metód



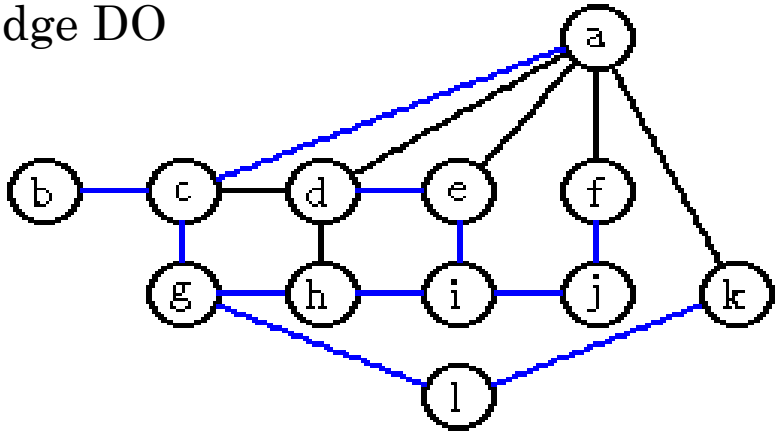
Vlastnosti daného prístupu

- Uzavretý model (protokol aj prípadný útočník)
- Problém „false positive“ výsledku
- Problém zložitých modelov
- Vhodné pre vlastnosti:
  - Čo sa musí vždy udiať.
  - Čo sa nesmie nikdy udiať
  - Ak niečo, tak potom určite aj ...

Príklad nedeterministického modelovanie a analýzy

- Uzavretý priestor všetkých možností ako sa môže daný protokol správať.
  - Predmodelovaná komunikácia
- Depth-first & breadth-first search alg.

```
algorithm  dft(x)
  visit(x)
  FOR each y such that (x,y) is an edge DO
    IF y was not visited yet THEN
      dft(y)
```



Rozmiestnenie 8 dám na šachovnici

```
active proctype Queens() {
        byte col = 1;
        byte row;
        do
        ::      Choose();           //nondeter choice row=[1...8]
                !a[row-1];          //je dama v tomto riadku?
                !b[row+col-2];      //je dama na diagonale zlava-doprava?
                !c[row-col+7];      //je dama na diagonale zprava-dolava?
                a[row-1]= true;
                    b[row+col-2]= true;
                    c[row-col+7] = true;
                    result[col-1] = row;//posad damu na tento riadok
                if
                :: col == 8 -> break
                :: else ->    col++      //chod obsadit dalsi stlpec
                fi
        od;
        Print();
        assert(false);                   //ak sme tu, nasli sme riesenie
}
```

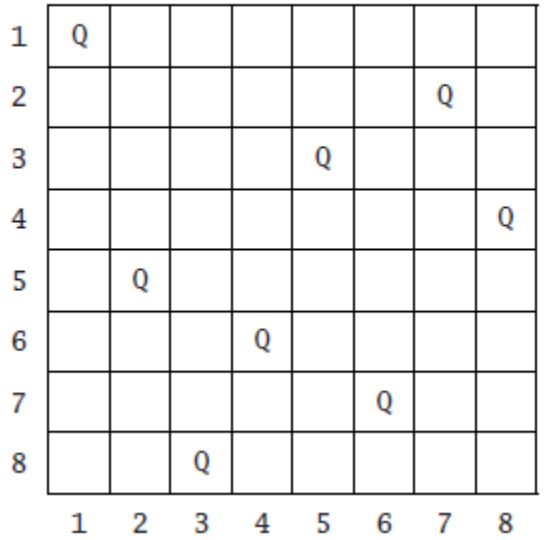
```
byte result[8];
bool a[8];
bool b[15];
bool c[15];

inline Choose(){
            if
            ::row=1
            ::row=2
            ::row=3
            ::row=4
            ::row=5
            ::row=6
            ::row=7
            ::row=8
            fi;
}
```

Výsledok

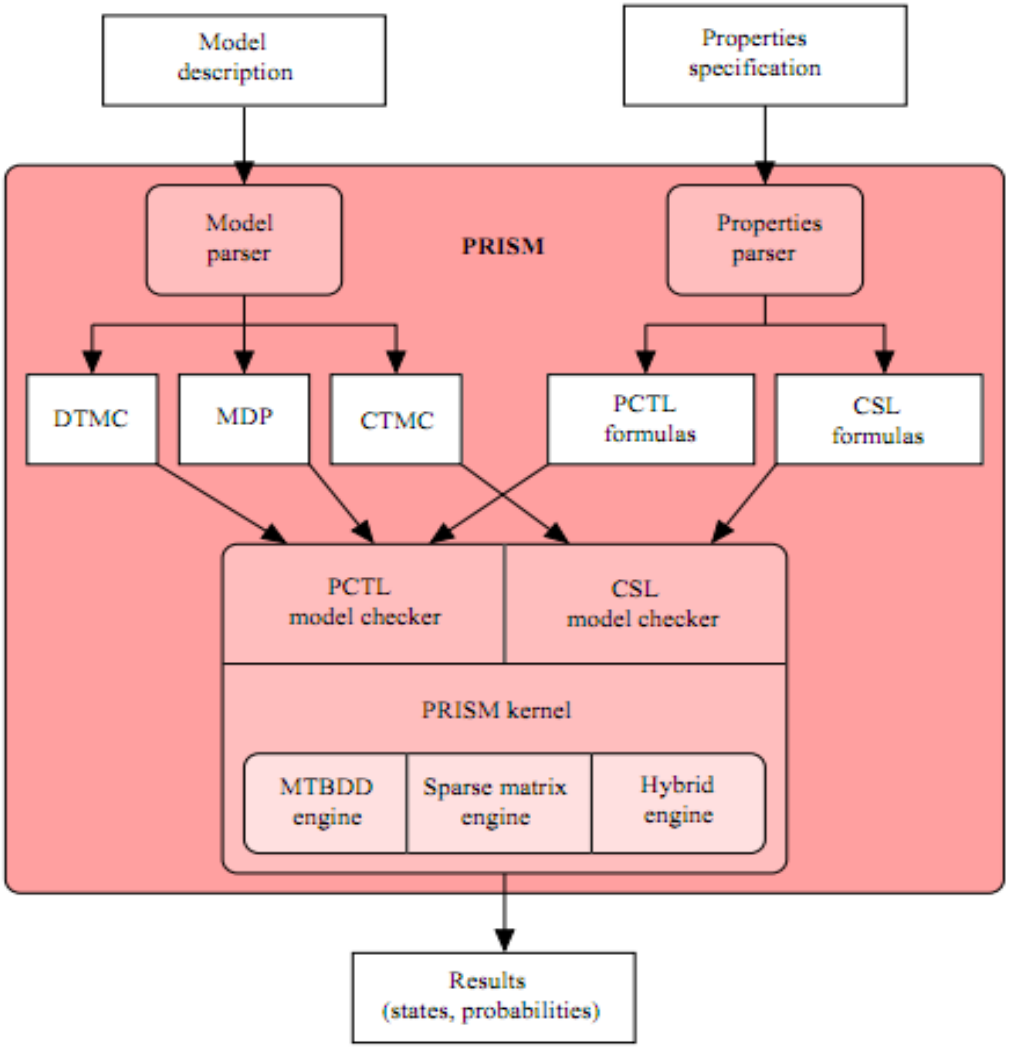
- Nástroj SPIN, verifikácia modelu v PROMELA jazyku

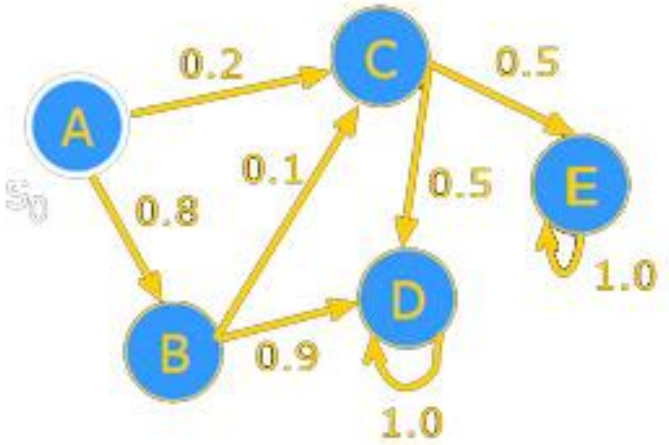
State-vector 56 byte, depth reached 82,
errors: 92
39225 states, stored
0 states, matched
39225 transitions (= stored+matched)
0 atomic steps
hash conflicts: 20 (resolved)

5.040 memory usage (Mbyte)
pan: elapsed time 0.017 seconds



Modely s pravdepodobnostnými vlastnosťami





Vlastnosti daného prístupu

- Nehľadáme odpoveď typu áno/nie pre danú vlastnosť ale Aká je pravdepodobnosť výskytu danej vlastnosti,...
  - (systémy anonymného smerovania)
- Markovove grafy, nástroj PRISM
- modely obsahujú opis komunikujúcich strán pomocou konečných stavových automatov s vlastnými vnútornými premennými

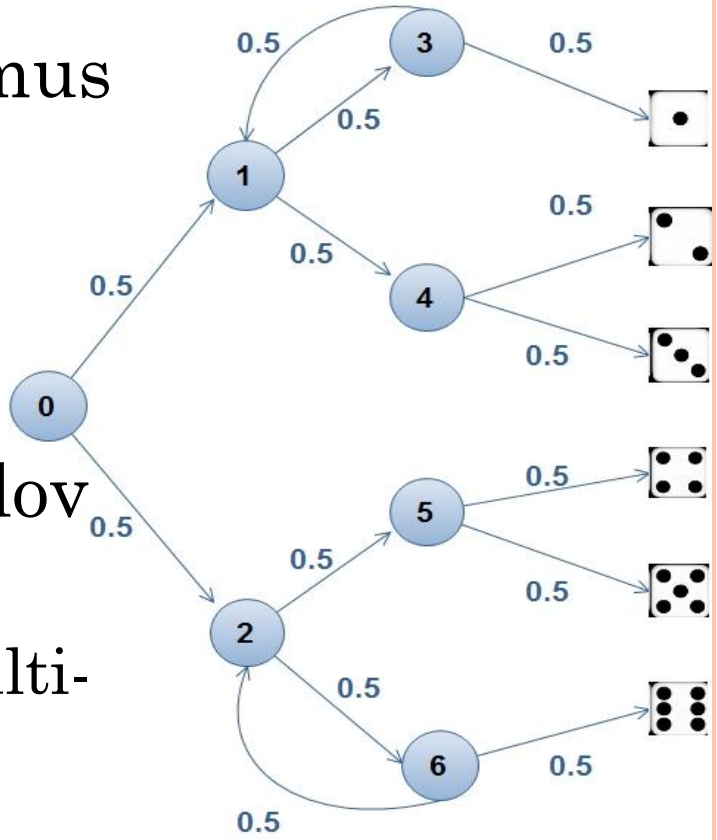
Vlastnosti daného prístupu

- 3 typy modelov (vlastností)
  - MG s diskrétnym časom (DTMC)
  - MG so spojitým časom (CTMC)
  - M rozhodujúci proces (MDP)

- Aká je pravdepodobnosť, že nastane chyba v systéme do 4 hodín od spustenia?
- Za aký najdlhší čas bude vykonaný daný algoritmus?
- Aká je najväčšia pravdepodobnosť, že proces zlyhá?

Príklad pravdepodobnostného modelovanie a analýzy

- pravdepodobnostný algoritmus (Knuth and Yao), ktorý emuluje 6-strannú hraciu kocku na princípe hádzania mince
- PRISM - reaktívnych modulov Alura a Henzingera
- (Binary Dicision Diagrams) (Multi-Terminal Binary Decision Diagrams).
- PCTL, CSL, LTL a PCTL*



PRISM MODEL

```
dtmc

module kocka

        s : [0..7] init 0;      // lokalny stav
        d : [0..6] init 0;      // hodnota na kocke

        [] s=0 -> 0.5 : (s'=1) + 0.5 : (s'=2);
        [] s=1 -> 0.5 : (s'=3) + 0.5 : (s'=4);
        [] s=2 -> 0.5 : (s'=5) + 0.5 : (s'=6);
        [] s=3 -> 0.5 : (s'=1) + 0.5 : (s'=7) & (d'=1);
        [] s=4 -> 0.5 : (s'=7) & (d'=2) + 0.5 : (s'=7) & (d'=3);
        [] s=5 -> 0.5 : (s'=7) & (d'=4) + 0.5 : (s'=7) & (d'=5);
        [] s=6 -> 0.5 : (s'=2) + 0.5 : (s'=7) & (d'=6);
        [] s=7 -> (s'=7);

endmodule
```

VÝSLEDOK - VERIFIKÁCIA

- 13 stavov a 20 možných prechodov
- P=? [F s=7 & d=x]
  - Aká je pravdepodobnosť, že na konci simulácie bude hodnota kocky= x ?
- kombinácii multiterminálnych binárnych rozhodovacích diagramov a riedených matíc.
- Cykly - > presnosť výsledku

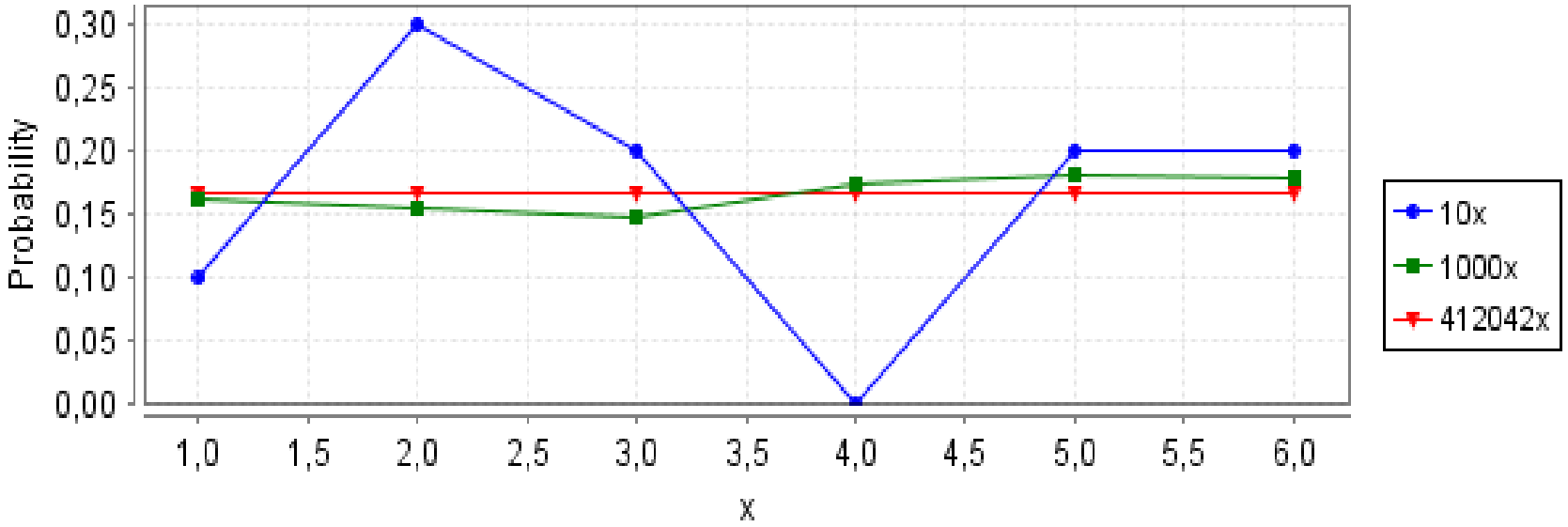
Property:
P=? [F s=7&d=x]

Defined constants:
x=5

Method:
Verification

Result (probability):
0.16666650772094727

Aproximácia vs. verifikácia



Graf presnosti aproximačnej metódy

Zhodnotenie experimentu

- Jednoduchosť jazyka je na druhú stranu často obmedzujúca a núti k vysokej miere abstrakcie
- Pokročilé jadro nástroja PRISM
  - Vhodné pre opakujúce sa úkony
- Nutné poznať dobre základy pravdepodobnostného symbolického modelovania a vedieť formulovať vlastnosti pre overenie pomocou LTL alebo PCTL formúl.

Zhrnutie

- Automatizovaný prístup má zjavné výhody
  - Nutnosť abstrakcie a logiky
- Spomenuté prístupy ako komplementárne metódy
- Ľahká tvorba modelov, ale zložitejšia tvorba pravidiel na overenie (LTL,PCTL)

Čas na otázky

Ďakujem za pozornosť