Zápočet z předmětu Výroková a predikátová logika

Tomáš Kafka

10. 9. 2007

1 Zadání:

Uvažujte následující formální systém pro výrokovou logiku s jednou binární logickou spojkou d:
schéma axiomu L: $d(d(P,d(Q,R)),d(d(P,d(R,P)),d(d(S,Q),d(d(P,S),d(P,S)))))$
odvozovací pravidlo N: Pokud platí $d(P,d(Q,R))$ a P, pak platí R.

V tomto systému formálně dokažte následující formuli (jako řešení chci kompletní formální důkaz dle definice):
$d(d(d(d(d(A,A),d(A,A)),d(A,A)),d(d(d(A,A),d(A,A)),d(A,A))),d(d(d(d(A,A),d(A,A)),d(A,A)),d(d(d(A,A),d(A,A)),d(A,A))))$

2 Řešení

Úvod:

Zjistil jsem že logický systém popsaný v zadání je logickým systémem se Shefferovou logickou spojkou (Sheffer Stroke alias NAND). Tento systém s jednou spojkou organickým (neobsahuje tautologii jako podformuli) axiomem formy DDpDqrDDpDrpDDsqDDpsDps objevil J. Lukasiewicz, a Branden Fitelson poté ukázal, že tento axiom je se svými 23 symboly nejkratším možným (New Elegant Axiomatizations of Some Sentential Logics `http://fitelson.org/ar.html#SH`).

K důkazu uvedené formule jsem nejdříve začal psát dokazující program, během práce na něm jsem objevil program pro logické dokazování Prover9 a v něm jsem danou formuli dokázal.

Můj dokazující program:

Idea:

Podle odvozovacího pravidla platí $d(x,d(y,z)),x \vdash z$, a tak, chceme-li dokázat A, musíme dokázat $d(1,d(y,A))$ a 1, kde 1 je volná proměnná která v obou formulích zastupuje stejnou formuli. Abychom ale dokázali nové dvě formule, musíme dokázat tentokráte už čtyři nové formule, a pokud takto budeme postupovat iterativně, dostaneme důkazový strom. Příklad důkazového stromu pro formuli $d(a,a)$:

```
d(a,a)
d(1,d(2,d(a,a)))  1
d(3,d(4,d(1,d(2,d(a,a)))))  3  d(5,d(6,1))  5
d(7,d(8,d(3,d(4,d(1,d(2,d(a,a))))))) 7  d(9,d(10,3))  9  d(11,d(12,d(5,d(6,1))))  11  d
    (13,d(14,5))  13
...
```

Následně je potřeba tento strom 'uříznout', tj. najít důkazy takové množiny listů, aby byl strom konečný. Probíráme tedy po řadě všechny množiny listů M a to tak dlouho, dokud nenajdeme *dokazatelnou* množinu M.

Množinu M nazveme *dokazatelnou*, je-li každá z jejích formulí instancí axiomu L, a unifikují-li volné proměnné (vyjádřené čísly) v takové množině vždy se stejnou podformulí (a jejich hodnota je tak jednoznačně dána).

Pokud existuje dokazatelná množina listů M, je formule A dokázána.

Implementace:

Nejříve jsem chtěl použít Prolog, ale poté jsem narazil na obtížnou manipulaci s řetězci, rozhodl jsem se tedy programovat řešení jako konzolovou aplikaci v PHP. To jsem si vybral pro automatickou správu paměti, funkcionální prvky (asociativní array, map, atd...), a výbornou podporou práce s řetězci.

Program ve stávajícím stavu umí generovat dokazovací strom, a unifikovat výsledné formule s axiomem M každou zvlášť (implementován je Robinsonův unifikační algoritmus). Při unifikacích více formulí najednou jsem ale narazil na problémy a nechtěl jsem programovat to, co už je lépe udělané v Prologu, proto jsem chtěl generovat množiny formulí jako prologové programy a k jejich ověřování volat Prolog z příkazové řádky. Tam jsem skončil úplně, jelikož se mi nepodařilo donutit Prolog pracovat jako konzolovou plikaci odpovídající yes nebo no na možnost unifikace vstupu.

Syntax dukaz.php - generování stromu:

```
php dukaz.php <hloubka> <výstupní soubor> <dokazovaná formule>
```

Ukázka generování prologových dotazů pro formuli $d(a,a)$ (zatím se ptá jen na unifikaci jednotlivých úrovní dok. stromu):

```
E:\Dokumenty\Programming\Eclipse workspaces\logika\logika>php dukaz-prolog.php 3 out.
    txt d(a,a)
d(a,a)
d(1,d(2,d(a,a))) 1
d(3,d(4,d(1,d(2,d(a,a))))) 3 d(5,d(6,1)) 5

d(a,a)=d(d(P1,d(Q1,R1)),d(d(P1,d(R1,P1)),d(d(S1,Q1),d(d(P1,S1),d(P1,S1))))).

d(Var1,d(Var2,d(a,a)))=d(d(P2,d(Q2,R2)),d(d(P2,d(R2,P2)),d(d(S2,Q2),d(d(P2,S2),d(P2,
    S2))))) Var1=d(d(P3,d(Q3,R3)),d(d(P3,d(R3,P3)),d(d(S3,Q3),d(d(P3,S3),d(P3,S3))))).

d(Var3,d(Var4,d(Var1,d(Var2,d(a,a)))))=d(d(P4,d(Q4,R4)),d(d(P4,d(R4,P4)),d(d(S4,Q4),d
    (d(P4,S4),d(P4,S4))))),
Var3=d(d(P5,d(Q5,R5)),d(d(P5,d(R5,P5)),d(d(S5,Q5),d(d(P5,S5),d(P5,S5))))),
d(Var5,d(Var6,Var1))=d(d(P6,d(Q6,R6)),d(d(P6,d(R6,P6)),d(d(S6,Q6),d(d(P6,S6),d(P6,S6)
    )))),
Var5=d(d(P7,d(Q7,R7)),d(d(P7,d(R7,P7)),d(d(S7,Q7),d(d(P7,S7),d(P7,S7))))).
```

Prover9

Nakonec jsem při hledání narazil na Prover9, program pro automatické dokazování.

Prover9 umí hledat spor, pokud tedy od něj chceme dokázat nějakou formuli, předložíme mu axiomy a odvozovací pravidla, a znegovanou dokazovanou formuli $\neg A$, Prove9 se pak snaží najít spor - tj. dokázat A.

Vstup: fle.in:

```
formulas(sos).

P(d(d(u,d(v,w)),d(d(u,d(w,u)),d(d(x,v),d(d(u,x),d(u,x)))))).
(P(d(u,d(v,w))) & P(u)) -> P(w).
-P(d(d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))),d(d(d(d(a,a),d(a,a)
    ),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))))).

end_of_list.
```

Zpracování:

```
prover9 -f fle.in > fle.out
prooftrans expand renumber striplabels parents_only -f fle.out > fle.proof4
```

Práce s odvozovacím pravidlem:

Do důkazu přidáme mezikroky $x \vdash z$ pro snadnější pochopení.

1. pokud platí: $\vdash x$

2. a také platí: $\vdash d(x, d(y, z))$

3. tak platí: $\vdash z$

a zároveň z 1,2: $x \vdash z$

Dále jsem z důkazu odstranil duplicity a přečísloval ho.

Jak interpretovat výstupní soubor:

```
1 P(d(x,d(y,z))) & P(x) -> P(z).   [assumption].
2 P(d(d(x,d(y,z)),d(d(x,d(z,x)),d(d(u,y),d(d(x,u),d(x,u)))))).   [assumption].
3 -P(d(x,d(y,z))) | -P(x) | P(z).   [clausify(1)].
4 -P(d(d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))),d(d(d(d(a,a),d(a,a)),
    d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))))).   [assumption].
5 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).   [resolve(3,a,2,a)].
6 P(d(d(x,d(y,d(z,y))),d(d(d(y,d(u,z)),x),d(d(y,d(u,z)),x)))).   [resolve(5,a,2,a)].
```

P je unární predikát platnosti.

1 $P(d(x, d(y, z))) \wedge P(x) \rightarrow P(z)$ [assumption].

2 $P(d(\underbrace{d(x, d(y, z))}_{x}, d(\underbrace{d(x, d(z, x))}_{y}, \underbrace{d(d(u, y), d(d(x, u), d(x, u)))}_{z})))$. [assumption].

- 1 a 2 jsou předpoklady, termy se přepíší tak, že nejdříve se vyskytující term se stane x, z druhého je y, atd...

3 $-P(d(x, d(y, z)))| - P(x)|P(z)$. [clausify(1)].

- 3 si Prover9 převede do formy bez implikace, zjevně používá minimální množinu symbolů

4 $-P(d(d(d(d(d(a, a), d(a, a)), d(a, a)), d(d(d(a, a), d(a, a)), d(a, a))), d(d(d(d(a, a), d(a, a)), d(a, a)), d(d(d(a, a), d(a, a)), d(a, a))))$ [assumption].

- 4 je negace dokazované formule

5 $-P(d(x, d(y, z)))|P(d(d(u, y), d(d(x, u), d(x, u))))$. [resolve(3,a,2,a)].

- 5 vznikne z axiomu L a odvozovacího pravidla N unifikací zvýrazněných částí.
lze ji přepsat jako $P(d(x, d(y, z))) \rightarrow P(d(d(u, y), d(d(x, u), d(x, u))))$

6 $P(d(d(\underbrace{x}_{u}, \underbrace{d(y, d(z, y))}_{y}), d(d(\underbrace{d(y, d(u, z))}_{x}, \underbrace{x}_{u}), d(\underbrace{d(y, d(u, z))}_{x}, \underbrace{x}_{u})))$. [resolve(5,a,2,a)].

- 6 vznikne jako instance pravé strany 5, zároveň ale víme že pravá strana 5 platí, neboť kdyby $P(d(x, d(y, z)))$ neplatilo, neplatil by ani axiom L který je jen dosazením podformulí za x, y a z.

$\vdots$

Důkaz:

1 - N: $d(x,d(y,z)),x \vdash z$ [odvozovací pravidlo N]

2 - L: $d(d(x,d(y,z)),d(d(x,d(z,x)),d(d(u,y),d(d(x,u),d(x,u)))))$ [axiom L]

3: $d(x,d(y,z)) \vdash d(d(u,y),d(d(x,u),d(x,u)))$ [N,L]
(použijeme L jako jednu formuli pravidla)

4: $d(d(x,d(y,d(z,y))),d(d(d(y,d(u,z)),x),d(d(y,d(u,z)),x)))$[3,L]
(instance pravé strany [3])

5: $d(d(x,d(d(y,d(z,u)),w)),d(d(d(w,d(y,d(u,y))),x),d(d(w,d(y,d(u,y))),x)))$ [3,4]

6: $d(x,d(d(y,d(z,u)),w)) \vdash d(d(w,d(y,d(u,y))),x)$ [N,5]

7: $d(d(d(d(x,y),d(d(z,x),d(z,x))),d(z,d(z,z))),d(z,d(y,u)))$ [6,L]

8: $d(x,d(y,d(z,y))) \vdash d(d(y,d(u,z)),x)$ [N,4]

9: $d(d(x,d(y,z)),d(d(d(u,z),d(d(x,u),d(x,u))),d(x,d(x,x))))$ [7,8]

10: $d(d(x,y),d(d(d(d(d(z,u),d(d(y,z),d(y,z))),d(y,d(y,y))),x),d(d(d(d(z,u),d(d(y,z),d(y,z))),d(y,d(y,y))),x)))$ [3,7]

11: $d(x,d(y,z)) \vdash d(x,d(x,x))$ [N,9]

12: $d(d(x,d(y,z)),d(d(x,d(y,z)),d(x,d(y,z))))$ [11,9]

13: $d(d(d(x,d(y,z)),d(x,d(z,x))),d(x,d(y,z)))$ [6,12]

14: $d(d(x,d(y,d(z,u))),d(d(d(y,d(z,u)),x),d(d(y,d(z,u)),x)))$ [3,12]

15: $d(d(x,d(y,z)),d(d(x,d(z,x)),d(x,d(x,x))))$ [8,13]

16: $d(d(d(x,d(x,x)),d(x,d(x,x))),d(x,d(y,z)))$ [6,15]

17: $d(d(x,d(y,z)),d(d(x,d(x,x)),d(x,d(x,x))))$ [8,16]

18: $d(x,d(y,d(z,u))) \vdash d(d(y,d(z,u)),x)$ [N,14]

19: $d(d(x,d(y,z)),d(d(x,d(y,z)),d(x,d(z,x))))$ [18,13]

20: $d(x,d(y,z)) \vdash d(x,d(z,x))$ [N,19]

21: $d(d(x,d(y,z)),d(d(x,d(z,x)),d(x,d(y,z))))$ [20,19]

22: $d(d(d(x,d(y,x)),d(x,d(z,y))),d(x,d(z,y)))$ [18,21]

23: $d(d(x,d(y,z)),d(d(x,d(x,x)),d(x,d(z,x))))$ [8,22]

24: $d(x,d(y,z)) \vdash d(x,d(x,x))$ [N,17]

25: $d(d(x,y),d(d(x,y),d(x,y)))$ [24,10]

26: $d(d(x,d(y,z)),d(d(d(y,z),x),d(d(y,z),x)))$ [3,25]

27: $d(x,d(y,z)) \vdash d(d(y,z),x)$ [N,26]

28: $d(d(d(d(x,y),z),d(d(x,y),z)),d(z,d(x,y)))$ [27,26]

29: $d(d(x,d(y,z)),d(d(d(z,x),x),d(d(z,x),x)))$ [8,28]

30: $d(d(d(d(x,y),y),d(d(x,y),y)),d(y,d(z,x)))$ [27,29]

31: $d(x,d(y,z)) \vdash d(x,d(z,x))$ [N,23]

32: $d(d(x,d(y,z)),d(d(d(z,x),x),d(x,d(y,z))))$ [31,29]

33: $d(d(x,d(y,z)),d(d(d(x,x),x),d(d(x,x),x)))$ [8,30]

34: $d(d(d(d(x,x),x),d(y,x)),d(x,d(d(x,x),x)))$ [8,32]

35: $d(d(d(d(x,x),x),d(d(x,x),x)),d(x,d(y,z)))$ [27,33]

36: $d(d(x,d(y,d(x,x))),d(d(d(x,x),x),d(z,x)))$ [8,34]

37: $d(x,d(y,d(x,x))) \vdash d(z,x)$ [N,36]

38: $d(x,d(d(d(y,y),y),d(d(y,y),y)))$ [37,35]

39: $d(d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))),d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))))$
[instance 38] QED

Přílohy

Výstupní soubor proveru:

```
============================== prooftrans ============================
Prover9 (32) version Aug-2007, Aug 2007.
Process 5744 was started by tk on amidala,
Sat Sep  8 02:59:45 2007
The command was "bin/prover9 -f fle.in".
============================== end of head ===========================

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.09 (+ 0.11) seconds.
% Length of proof is 31.
% Level of proof is 19.
% Maximum clause weight is 48.
% Given clauses 70.

1 P(d(x,d(y,z))) & P(x) -> P(z).  [assumption].
2 P(d(d(x,d(y,z)),d(d(x,d(z,x)),d(d(u,y),d(d(x,u),d(x,u))))).  [assumption].
3 -P(d(x,d(y,z))) | -P(x) | P(z).  [clausify(1)].
4 -P(d(d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a,a)),d(a,a))),d(d(d(d(a,a),d(a,a)),d(a,a)),d(d(d(a,a),d(a
    ,a)),d(a,a))))).  [assumption].
5 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).  [resolve(3,a,2,a)].
6 P(d(d(x,d(y,d(z,y))),d(d(d(y,d(u,z)),x),d(d(y,d(u,z)),x)))).  [resolve(5,a,2,a)].
7 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).  [resolve(3,a,2,a)].
8 P(d(d(x,d(d(y,d(z,u)),w)),d(d(d(w,d(y,d(u,y))),x),d(d(w,d(y,d(u,y))),x)))).  [resolve(7,a,6,a)].
9 -P(d(x,d(d(y,d(z,u)),w))) | P(d(d(w,d(y,d(u,y))),x)).  [resolve(3,a,8,a)].
10 P(d(d(d(d(x,y),d(d(z,x),d(z,x))),d(z,d(z,z))),d(z,d(y,u)))).  [resolve(9,a,2,a)].
11 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
12 P(d(d(x,d(y,z)),d(d(d(u,z),d(d(x,u),d(x,u))),d(x,d(x,x))))).  [resolve(11,a,10,a)].
13 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).  [resolve(3,a,2,a)].
14 P(d(d(x,y),d(d(d(d(d(z,u),d(d(y,z),d(y,z))),d(y,d(y,y))),x),d(d(d(d(z,u),d(d(y,z),d(y,z))),d(y,d(y,y))),
    x)))).  [resolve(13,a,10,a)].
15 -P(d(x,d(y,z))) | P(d(x,d(x,x))).  [resolve(3,a,12,a)].
16 P(d(d(x,d(y,z)),d(d(x,d(y,z)),d(x,d(y,z))))).  [resolve(15,a,12,a)].
17 -P(d(x,d(d(y,d(z,u)),w))) | P(d(d(w,d(y,d(u,y))),x)).  [resolve(3,a,8,a)].
18 P(d(d(d(x,d(y,z)),d(x,d(z,x))),d(x,d(y,z)))).  [resolve(17,a,16,a)].
19 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).  [resolve(3,a,2,a)].
20 P(d(d(x,d(y,d(z,u))),d(d(d(y,d(z,u)),x),d(d(y,d(z,u)),x)))).  [resolve(19,a,16,a)].
21 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
22 P(d(d(x,d(y,z)),d(d(x,d(z,x)),d(x,d(x,x))))).  [resolve(21,a,18,a)].
23 -P(d(x,d(d(y,d(z,u)),w))) | P(d(d(w,d(y,d(u,y))),x)).  [resolve(3,a,8,a)].
24 P(d(d(d(x,d(x,x)),d(x,d(x,x))),d(x,d(y,z)))).  [resolve(23,a,22,a)].
25 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
26 P(d(d(x,d(y,z)),d(d(x,d(x,x)),d(x,d(x,x))))).  [resolve(25,a,24,a)].
27 -P(d(x,d(y,d(z,u)))) | P(d(d(y,d(z,u)),x)).  [resolve(3,a,20,a)].
28 P(d(d(x,d(y,z)),d(d(x,d(y,z)),d(x,d(z,x))))).  [resolve(27,a,18,a)].
29 -P(d(x,d(y,z))) | P(d(x,d(z,x))).  [resolve(3,a,28,a)].
30 P(d(d(x,d(y,z)),d(d(x,d(z,x)),d(x,d(y,z))))).  [resolve(29,a,28,a)].
31 -P(d(x,d(y,d(z,u)))) | P(d(d(y,d(z,u)),x)).  [resolve(3,a,20,a)].
32 P(d(d(d(x,d(y,x)),d(x,d(z,y))),d(x,d(z,y)))).  [resolve(31,a,30,a)].
33 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
34 P(d(d(x,d(y,z)),d(d(x,d(x,x)),d(x,d(z,x))))).  [resolve(33,a,32,a)].
35 -P(d(x,d(y,z))) | P(d(x,d(x,x))).  [resolve(3,a,26,a)].
36 P(d(d(x,y),d(d(x,y),d(x,y)))).  [resolve(35,a,14,a)].
37 -P(d(x,d(y,z))) | P(d(d(u,y),d(d(x,u),d(x,u)))).  [resolve(3,a,2,a)].
38 P(d(d(x,d(y,z)),d(d(d(y,z),x),d(d(y,z),x)))).  [resolve(37,a,36,a)].
39 -P(d(x,d(y,z))) | P(d(d(y,z),x)).  [resolve(3,a,38,a)].
40 P(d(d(d(d(x,y),z),d(d(x,y),z)),d(z,d(x,y)))).  [resolve(39,a,38,a)].
41 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
42 P(d(d(x,d(y,z)),d(d(d(z,x),x),d(d(z,x),x)))).  [resolve(41,a,40,a)].
43 -P(d(x,d(y,z))) | P(d(d(y,z),x)).  [resolve(3,a,38,a)].
44 P(d(d(d(d(x,y),y),d(d(x,y),y)),d(y,d(z,x)))).  [resolve(43,a,42,a)].
45 -P(d(x,d(y,z))) | P(d(x,d(z,x))).  [resolve(3,a,34,a)].
46 P(d(d(x,d(y,z)),d(d(d(z,x),x),d(x,d(y,z))))).  [resolve(45,a,42,a)].
47 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
48 P(d(d(x,d(y,z)),d(d(d(x,x),x),d(d(x,x),x)))).  [resolve(47,a,44,a)].
49 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
50 P(d(d(d(d(x,x),x),d(y,x)),d(x,d(d(x,x),x)))).  [resolve(49,a,46,a)].
51 -P(d(x,d(y,z))) | P(d(d(y,z),x)).  [resolve(3,a,38,a)].
52 P(d(d(d(d(x,x),x),d(d(x,x),x)),d(x,d(y,z)))).  [resolve(51,a,48,a)].
53 -P(d(x,d(y,d(z,y)))) | P(d(d(y,d(u,z)),x)).  [resolve(3,a,6,a)].
54 P(d(d(x,d(y,d(x,x))),d(d(d(x,x),x),d(z,x)))).  [resolve(53,a,50,a)].
55 -P(d(x,d(y,d(x,x)))) | P(d(z,x)).  [resolve(3,a,54,a)].
56 P(d(x,d(d(d(y,y),y),d(d(y,y),y)))).  [resolve(55,a,52,a)].
57 $F.  [resolve(56,a,4,a)].

============================== end of proof ==========================
```

PHP

PHP soubory jsou přiloženy.