Automatsko generisanje mašinski proverivih i čitljivih dokaza i dijalekt koherentne logike

Sana Stojanović

Argo seminar, jul 2014

Dokazivanje teorema

- Dokazivanje teorema na papiru — Nemamo garancije!
- Automatsko dokazivanje teorema — Da/Ne!
- Interaktivno dokazivanje teorema — Formalni dokazi!
- Cilj: Napraviti sistem koji će:
  - automatski dokazivati matematičke teoreme
  - generisati mašinski proverive dokaze
  - generisati čitljive dokaze (nalik dokazima u udžbenicima)

Kombinacija dokazivača

- Dokazivač za koherentnu logiku (ArgoCLP)
  - automatsko dokazivanje teorema
  - generiše mašinski proverive i čitljive dokaze
  - ...ali nije efikasan
- Rezolucijski dokazivači (Vampire, E, SPASS)
  - automatsko dokazivanje teorema
  - veoma efikasni
  - ...ali ne generišu čitljive dokaze niti mašinski proverive dokaze
- Interaktivni dokazivači teorema (Isar, Coq)
  - mašinski proverivi dokazi
  - ...ali automatizacija nije dovoljno razvijena

Osnovni algoritam

1. Rezolucijski dokazivači pokušavaju da dokažu teoremu uz pomoć određenog skupa aksioma i teorema (u normalnom i obrnutom redosledu)
2. Ako jedan (ili više) rezolucijskih dokazivača uspe, najmanji skup aksioma koji je pronađen se upotrebljava ponovo (da bi dobili što manji skup)
3. Dobijeni skup aksioma se prosleđuje koherentnom dokazivaču
4. Ako koherentni dokazivač dokaže teoremu dokaz se eksportuje u XML formatu, koji može biti preveden u Isar, Coq ili u prirodni jezik

Opis alata

1. Koherentna logika
   $A_1(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \exists \vec{y}(B_1(\vec{x}, \vec{y}) \vee \ldots \vee B_m(\vec{x}, \vec{y}))$ (ax)
2. Ulazni format aksioma i teorema: TPTP
3. Rezolucijski dokazivači: Vampire, E, SPASS
4. Dokazivač za koherentnu logiku: ArgoCLP
5. Izlazni format dokaza: XML (dijalekt za koherentnu logiku)
6. Interaktivni dokazivači teorema: Isar, Coq

Knjiga Tarskog

- Wolfram Schwabhaüser, Wanda Szmielew, Alfred Tarski: *Metamathematische Methoden in der Geometrie* (1983)
- Jedna vrsta objekata – tačka
- Dva primitivna predikata (između, podudarno)
- Jedanaest aksioma

Aksiome

1. $\forall A\, \forall B\ cong(A, B, B, A)$
2. $\forall A\, \forall B\, \forall P\, \forall Q\, \forall R\, \forall S\ (cong(A, B, P, Q) \wedge cong(A, B, R, S) \Rightarrow cong(P, Q, R, S))$
3. $\forall A\, \forall B\, \forall C\ (cong(A, B, C, C) \Rightarrow A = B)$
4. $\forall A\, \forall B\, \forall C\, \forall Q\, \exists X\ (bet(Q, A, X) \wedge cong(A, X, B, C))$
5. $\forall A\, \forall B\, \forall C\, \forall D\, \forall A1\, \forall B1\, \forall C1\, \forall D1\ (A \neq B \wedge bet(A, B, C) \wedge bet(A1, B1, C1) \wedge cong(A, B, A1, B1) \wedge cong(B, C, B1, C1) \wedge cong(A, D, A1, D1) \wedge cong(B, D, B1, D1) \Rightarrow cong(C, D, C1, D1))$
6. $\forall A\, \forall B\ (bet(A, B, A) \Rightarrow A = B)$
7. $\forall A\, \forall B\, \forall C\, \forall P\, \forall Q\ (bet(A, P, C) \wedge bet(B, Q, C) \Rightarrow \exists X\ (bet(P, X, B) \wedge bet(Q, X, A)))$
8. $\exists A\, \exists B\, \exists C\ (\neg bet(A, B, C) \wedge \neg bet(B, C, A) \wedge \neg bet(C, A, B))$
9. $\forall P\, \forall Q\, \forall A\, \forall B\, \forall C\ (P \neq Q \wedge cong(A, P, A, Q) \wedge cong(B, P, B, Q) \wedge cong(C, P, C, Q) \Rightarrow (bet(A, B, C) \vee bet(B, C, A) \vee bet(C, A, B)))$
10. $\forall A\, \forall B\, \forall C\, \forall D\, \forall T\ (bet(A, D, T) \wedge bet(B, D, C) \wedge A \neq D \Rightarrow \exists X\, \exists Y\ (bet(A, B, X) \wedge bet(A, C, Y) \wedge bet(X, T, Y)))$

Prevođenje u koherentnu logiku

- 211 teorema u prvih 12 poglavlja
  - 93 već pripadaju koherentnoj logici (44%)
  - 36 se trivijalno transformišu u koherentnu logiku (17%)
  - 68 se mogu prevesti/preformulisati u koherentnu logiku (32%)
  - 14 se tiču n-torki – nismo ih razmatrali (7%)
- 269 teorema koherentne logike
- Dokazano oko 1/3 teorema

Postojeće formalizacije knjige Tarskog

- Braun, Narboux – interaktivno dokazivanje, Coq
- Beeson, Wos – polu-automatsko dokazivanje, rezolucijski dokazivač Otter
  - Ne koriste skupove, teoreme iz knjige su preformulisane
  - Linije su predstavljene parovima tačaka, ne koriste dodatne predikate za predstavljanje relacija nad skupovima

Uparivanje naše i Coq formalizacije

- Razlika u sintaksi
- Promena imena
- Razbijanje teorema na leme
- Dodatne leme
- Fajl zavisnosti

Načini dokazivanja teorema

- *Potpuno automatski*, bez navođenja – sve aksiome i teoreme iz knjige koje joj prethode
- *Automatski*, sa navođenjem:
  1. Implicitno navođenje – proširujemo skup teorema dodatnim lemama (dobijenim iz Coq formalizacije)
  2. Eksplicitno navođenje – koristimo tačan spisak teorema koje se koriste u dokazu (liste zavisnosti dobijene iz Coq formalizacije)

Rezultati

	RD	ArgoCLP	Kompletan dokaz
Bez navođenja	48%	37%	17%
Implicitno navođenje	55%	42%	17%
Eksplicitno navođenje	63%	40%	22%

Zaključak

- Naš sistem može biti korisan kao pomoćni alat prilikom formalizacije teorema
  - Potpuno automatski, za generisanje određenog dela formalizacije
  - Interaktivno, za dokazivanje jedne po jedne teoreme
- Može se koristiti sa različitim količinama informacija
- Dobijene informacije u nekim slučajevima mogu pojednostaviti interaktivne dokaze

Dijalekt i matematički dijalekt

- Dijalekt, dijalekat ili narečje je varijetet jezika koji koriste ljudi određene geografske oblasti
- Matematički dijalekt, Freek Wiedijk (2000):
  It turns out that in a significant number of systems (proof assistants) one encounters languages that look almost the same. Apparently there is a canonical style of presenting mathematics that people discover independently: something like a natural *mathematical vernacular. Because this language apparently is something that people arrive at independently, we might call it* the *mathematical vernacular.*

Dijalekt za koherentnu logiku

- Ne predstavlja matematički dijalekt
- Ne predstavlja format za prevođenje dokaza između različitih interaktivnih dokazivača teorema
- Predstavlja format dokaza u koherentnoj logici
- Lako može biti automatski generisan
- Lako prevodiv u prirodni jezik i formalni jezik (Isar, Coq)

Pravila – prirodna dedukcija

$$\frac{A_1(\vec{a}) \quad \ldots \quad A_n(\vec{a}) \quad A_1(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \exists \vec{y}(B_1(\vec{x},\vec{y}) \vee \ldots \vee B_m(\vec{x},\vec{y}))}{B_1(\vec{a},\vec{b}) \vee \ldots \vee B_m(\vec{a},\vec{b})}\ ax$$

$$\frac{B_1(\vec{c}) \vee \ldots \vee B_n(\vec{c}) \qquad \begin{matrix}[B_1(\vec{c})] \\ \vdots \\ P\end{matrix} \qquad \ldots \qquad \begin{matrix}[B_m(\vec{c})] \\ \vdots \\ P\end{matrix}}{P}\ \vee E$$

$$\frac{B_i(\vec{a},\vec{b})}{\exists \vec{y}(B_1(\vec{a},\vec{y}) \vee \ldots \vee \ B_m(\vec{a},\vec{y}))}\ \exists I, \wedge I$$

$$\frac{\bot}{A}\ efq$$

Pravila – racučun sekvenata

$$\frac{\Gamma, ax, \underline{A_1(\vec{a}) \wedge \ldots \wedge A_n(\vec{a})}, B_1(\vec{a}, \vec{b}) \vee \ldots \vee B_m(\vec{a}, \vec{b}) \vdash P}{\Gamma, ax, \underline{A_1(\vec{a}) \wedge \ldots \wedge A_n(\vec{a})} \vdash P} \; mp \; (modus\ ponens)$$

$$\frac{\Gamma, \underline{B_1(\vec{c})} \vdash P \quad \ldots \quad \Gamma, \underline{B_n(\vec{c})} \vdash P}{\Gamma, B_1(\vec{c}) \vee \ldots \vee B_n(\vec{c}) \vdash P} \; cs \; (case\ split)$$

$$\frac{}{\Gamma, \underline{B_i(\vec{a}, \vec{b})} \vdash \exists \vec{y}(B_1(\vec{a}, \vec{y}) \vee \ldots \vee \; B_m(\vec{a}, \vec{y}))} \; as \; (assumption)$$

$$\frac{}{\Gamma, \bot \vdash P} \; efq \; (ex\ falso\ quodlibet)$$

XML

- XML je fleksibilan i stuktuiran
- Format dokaza je opisan `Vernacular.dtd`
- Može sadržati jedno ili više tvrđenja

Vernacular.dtd (1)

```
...
<!--******** Theory ***************-->
<!ELEMENT theory (theory_name, signature, axiom*) >
<!ELEMENT theory_name (#PCDATA)>
<!ELEMENT signature (type*, relation_symbol*, constant*) >
<!ELEMENT relation_symbol (type*)>
<!ATTLIST relation_symbol name CDATA #REQUIRED>
<!ELEMENT type (#PCDATA)>
<!ELEMENT axiom (cl_formula)>
<!ATTLIST axiom name CDATA #REQUIRED>
...
```

Vernacular.dtd (2)

```
...
<!--******** Theorem **************-->
<!ELEMENT theorem (theorem_name, cl_formula, proof+)>
<!ELEMENT theorem_name (#PCDATA)>
<!ELEMENT conjecture (name, cl_formula)>

<!--******** Proof **************-->
<!ELEMENT proof (proof_step*, proof_closing, proof_name?)>
<!ELEMENT proof_name EMPTY>
<!ATTLIST proof_name name CDATA #REQUIRED>

<!--******** Proof steps **************-->
<!ELEMENT proof_step (indentation,modus_ponens)>
<!ELEMENT proof_closing (indentation, (case_split|efq|from),
  (goal_reached_contradiction|goal_reached_thesis))>
...
```

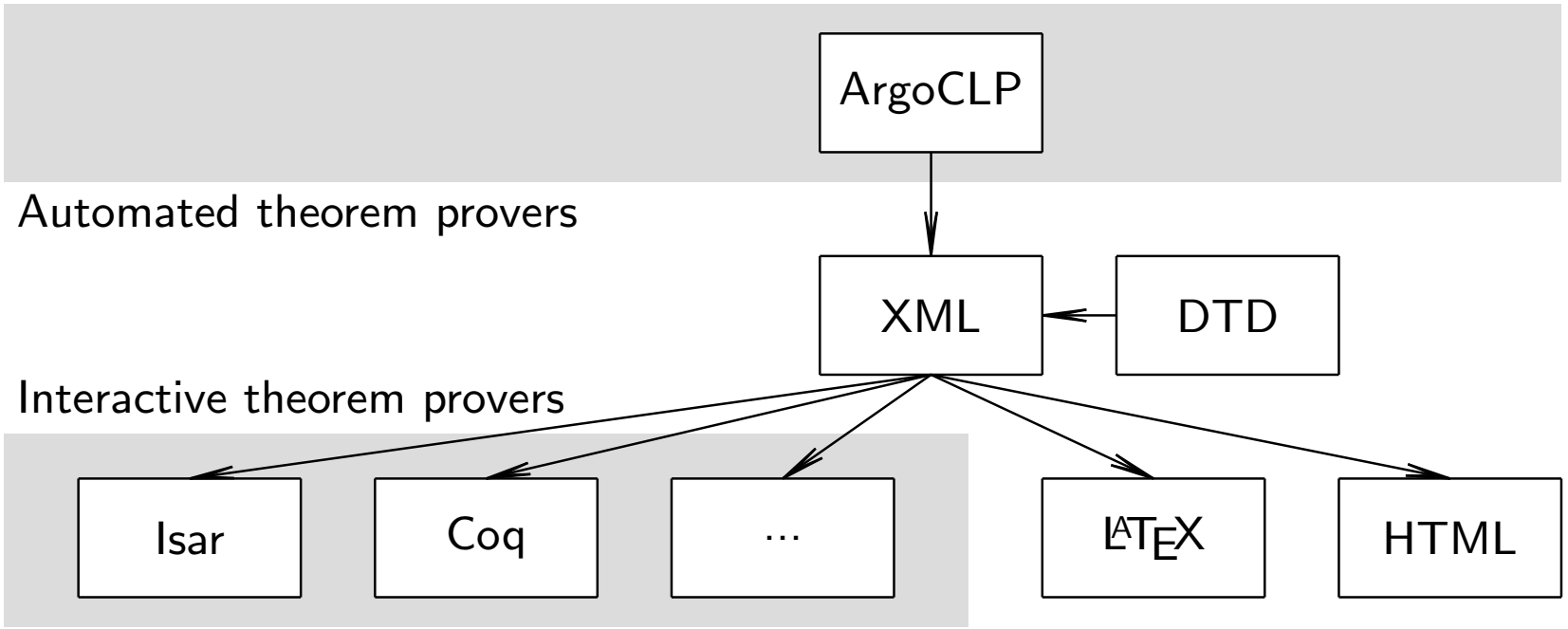
XML transformacije

Omogućene su transformacije XML-a u:

- Isabelle/Isar
- Coq
- prirodni jezik (engleski) – HTML
- prirodni jezik (engleski) – LaTeX

Jednostavne transformacije, svaka ima oko 500 linija

XML kao izlazni format za ArgoCLP



Theorem (th_4_19)

Assuming that $bet(A, B, C)$ and $AB \cong AD$ and $CB \cong CD$ it holds that $B = D$.

Proof:

1. It holds that $bet(B, A, A)$ (using *th_3_1*).
2. From the fact(s) $bet(A, B, C)$ it holds that $col(C, A, B)$ (using *ax_4_10_3*).
3. From the fact(s) $AB \cong AD$ it holds that $AD \cong AB$ (using *th_2_2*).
4. It holds that $A = B$ or $A \neq B$.
   5. Assume that: $A = B$.
      6. From the fact(s) $AD \cong AB$ and $A = B$ it holds that $AD \cong AA$.
      7. From the fact(s) $AD \cong AA$ it holds that $A = D$ (using *ax_3*).
      8. From the fact(s) $A = B$ and $A = D$ it holds that $B = D$.
      9. The conclusion follows from the fact(s) $B = D$.
   10. Assume that: $A \neq B$.
      11. It holds that $A = C$ or $A \neq C$.

...

Teorema 4.19, Isar

```
lemma th_4_19 : assumes "bet A B C" and "cong A B A
D" and "cong C B C D" shows "(B = D)"

proof -

have "bet B A A" by (rule th_3_1)
from ‘bet A B C‘ have "col C A B" by (rule ax_4_10_3)
from ‘cong A B A D‘ have "cong A D A B" by (rule
th_2_2)
have "A = B ∨ A ~= B" by (subst disj_commute, rule
excluded_middle)
   show ?thesis
   proof(cases "A = B")
     case True
      from ‘cong A D A B‘ and ‘A = B‘ have "cong A D A
A" by simp
      from ‘cong A D A A‘ have "A = D" by (rule ax_3)
      from ‘A = B‘ and ‘A = D‘ have "B = D" by simp
      from ‘B = D‘ show ?thesis by assumption
   next
     case False
```

Teorema 4.19, Coq

```
Theorem th_4_19 : ∀ (A:point) (B:point) (C:point) (D:point), (bet A B C ∧ cong
A B A D ∧ cong C B C D) → B = D.
Proof.
 intros.
 assert (bet B A A) by applying (th_3_1 B A ) .
 assert (col C A B) by applying (ax_4_10_3 A B C ) .
 assert (cong A D A B) by applying (th_2_2 A B A D ) .
 assert (A = B ∨ A ≠ B) by applying (ax_g1 A B ) .
 by cases on (A = B ∨ A ≠ B).
 - {
    assert (cong A D A A) by (substitution).
    assert (A = D) by applying (ax_3 A D A ) .
    assert (B = D) by (substitution).
    conclude.
    }
 - {
    assert (A = C ∨ A ≠ C) by applying (ax_g1 A C ) .
    by cases on (A = C ∨ A ≠ C).
    - {
       assert (bet A B A) by (substitution).
       assert (A = B) by applying (th_3_4 A B A ) .
       assert (False) by (substitution).
       contradict.
       }
    - {
       assert (C ≠ A) by (substitution).
```

Zaključak i dalji rad

- Jednostavan format
- Omogućava prevođenje dokaza u LaTeX, HTML, Isar i Coq
- Jednostavan za generisanje i za proširivanje (kako formalnih dokaza tako i dokaza u drugim prirodnim jezicima)
- Dodavanje funkcijskih simbola
- Pojednostavljenje Isar i Coq dokaza