Certified Termination (Overview)

Johannes Waldmann, HTWK Leipzig

Goal

Methods for proving Termination:

- find
- implement
- apply

increase confidence . . .

- in methods (formalized proofs for methods)
- in implementations (instantiate these proofs)

Current State

- Libraries:
  - for Coq:
    - Color (Blanqui et al),
    - Coccinelle (Contejean et al)
  - for Isabelle: (Sternagel, in progress)
- Termination provers with certifiable output:
  - (2007) Cime, TPA, TTTcert
  - (to come) Aprove, Matchbox, . . .

Venues for Certified Termination

- Workshop on Certified Termination
  (2007 Nancy; 2008 Leipzig; 2009 with WST Leipzig)
  details, minutes at
  `http://termination-portal.org/`
- Certified category of the Termination Competition (2007, . . .)
- papers at RTA and other conferences

Contents (Overview) of libraries

Color, Coccinelle:

- path ordering(s)
- interpretations (weak/strict, remove strict rules)
  - polynomial, matrix (natural, arctic)
- DP transformation
  - Color: simple graph approximation (top symbols)
  - Coccinelle: EDG

Example: A Color Theorem

```
Lemma polyInterpretationTermination :
forall R,
lforall (fun r => coef_pos (rulePoly_gt r)) R
     -> WF (red R).

Proof.
intros R H. apply manna_ness with (succ := su
apply pi_red_ord. apply pi_compat. exact H.
Qed.
```

Color: 150 modules, 50 kLOC

Ex.: A Coq Termination Proof

```
Definition R :=  @ATrs.mkRule sig_0 (S__dot__1 (S__dot__1 (A
 (S__dot__1 (AVar 3) (S__dot__1 (AVar 2) (AVar 1))) :: @nil (

  Definition trsInt f :=
    match f as f return AMatrixInt.matrixInt dim (@ASignature
      | M._dot__1 => mkMatrixInt (vec_of_list (1::nil))
        (vec_of_list ((Vcons (vec_of_list( 2::nil)) Vnil)::(V
        (vec_of_list( 1::nil)) Vnil):: nil))
    end.

Lemma termination : WF rel.
Proof.
unfold rel. try (ATrs.no_relative_rules || Srs.no_relative_ru
MI_1.prove_termination. termination_trivial.
```

Results

(from 2007 competition): for 975 selected problems:

- TPA: 354 (simple DP, poly, matrix)
- Cime: 317 (better DP, poly)
- TTTcert: 289 (simple DP, matrix)

(upcoming, inofficial): for 1370 problems in TPDB,

- Aprove: 420 (simple DP, poly) (will add matrices)
- Matchbox: 550 (simple DP, matrices $\mathbb{N} + \mathbb{A}$)

Most Wanted

- (Color) better DP graph approximation (more efficient, more detailed)
    - certificate is a topologically sorted list of sets of rules, and for each “back edge” a proof that we don’t need it.
- simple projections, subterm criterion (Endrullis, Sternagel)
- (RFC) match bounds (Koprowski, Waldmann)

environmental:

- interoperation between Color and Coccinelle

What’s the Difference

…in the Coq formalization of rewriting?

- Color: deep embedding (TRS as data)
- Coccinelle: shallow (TRS is a relation)

```
Inductive R_rules : term -> term -> Prop :=
 | R_rule_0 : forall  V_0 : term, (TERMS.Term signature_i
 signature_idfdi ( V_0::nil))::nil)) -[R_rules]> (TERMS.T
 (TERMS.Term signature_idfdi ( V_0::nil))::nil)).

Definition R  : term -> term -> Prop :=
EQTH.one_step R_rules.
```

Termination certificates

- independent of the producer (TPA, TTT,. . .)
- independent of the verifier (Coq/Color, . . .)

workflow:

- termination problem (z001.srs) $\xrightarrow{\text{Termination prover, e.g. TPA}}$ termination certificate (z001.cert)
- (problem, certificate) $\xrightarrow{\text{Transformer, e.g. Rainbow}}$ formal proof (e.g. z001.v)
- proof $\xrightarrow{\text{Proof checker, e.g. Coq}}$ OK.

Ex.: A Termination Certificate

```
<?xml version='1.0' encoding='ISO-8859-1' ?>
<proof xmlns=''urn:rainbow.proof.format''
       xmlns:xsi=''http://www.w3.org/2001/XMLSchema-instance'
       xsi:schemaLocation=''urn:rainbow.proof.format
       http://color.loria.fr/proof.xsd''
  ><manna_ness><order><matrix_int><dimension >1</dimension
        ><mi_map ><mapping ><fun >.</fun
            ><mi_fun ><const ><velem >1</velem></const
              ><arg ><row ><velem >2</velem></row></arg
              ><arg ><row ><velem
>1</velem></row></arg></mi_fun></mapping></mi_map>
...
```

Certificate formats

what’s the differences between the certificate formats?

- TPG (rainbow)
- for Coccinelle
- Aprove

success story (Thiemann, during Workshop on Certified Termination 2008): XSLT transformers from Aprove format to TPG and to Coccinelle

Technical points

(for Color)

- put less work on the verifier
- make certificate nodes (sub-proofs) self-contained
  (i.e. they should state the sub-statement that they want to prove)

Impact (outside certification)

- modularizaion of certificates . . .
- . . . related to modularization of provers

we want this anyway: makes it easier to

- combine provers
- modify provers
- write new provers

What’s the Proof Node Type?

each node N contains

- a claim C, a proof P,
- and some child nodes $N_1, \ldots, N_k$.

Then, P proves $C_1 \wedge \ldots \wedge C_k \implies C$.
The “claim” type is: the relation given by some (relative) (top) rules (with minimality) is terminating.

…and not: the following DP problem is finite.

DP transform is one source of such problems, but (e.g.) SN∞ is another.