Dowodzenie twierdzeń i programowanie z typami zależnymi w Coqu

Równość

26 kwietnia 2016

Typowanie jako relacja indukcyjna

```
Inductive exp : Set :=
| Nat : nat → exp
| Plus : exp → exp → exp
| Bool : bool → exp
| And : exp → exp → exp.
```

Typowanie jako relacja indukcyjna

```
Inductive type : Set := TNat | TBool.

Inductive hasType : exp → type → Prop :=
| HtNat : ∀ n,
  hasType (Nat n) TNat
| HtPlus : ∀ e1 e2,
  hasType e1 TNat
  → hasType e2 TNat
  → hasType (Plus e1 e2) TNat
| HtBool : ∀ b,
  hasType (Bool b) TBool
| HtAnd : ∀ e1 e2,
  hasType e1 TBool
  → hasType e2 TBool
  → hasType (And e1 e2) TBool.
```

Rozstrzygalność porównywania typów

```
Definition eq_type_dec : ∀ t1 t2 : type, {t1 = t2} + {t1 ≠ t2}.
  decide equality.
Defined.
```

Dowód przez indukcję po dowodzie

```
Lemma hasType_det : ∀ e t1,
  hasType e t1
  → ∀ t2, hasType e t2
    → t1 = t2.
  induction 1; inversion 1; auto.
Qed.
```

Patrz plik: hastype.v

Konwersja — równość definicyjna, obliczeniowa

ang. *d*efinitional equality

reguła konwersji

$$\frac{\Gamma \vdash M : A \qquad \Gamma \vdash A =_{\beta\eta\delta\zeta\iota} B \qquad \Gamma \vdash B : s}{\Gamma \vdash M : B}$$

$$\Gamma \vdash A =_{\beta\eta\delta\zeta\iota} B$$

jeśli

- $\Gamma \vdash A \rhd^* A'$
- $\Gamma \vdash B \rhd^* B'$
- $A' = B'$ lub
  $(A' = \lambda x : T.A''$ i $\Gamma, x : T \vdash B'x =_{\beta\eta\delta\zeta\iota} A'')$ lub
  $(B' = \lambda x : T.B''$ i $\Gamma, x : T \vdash A'x =_{\beta\eta\delta\zeta\iota} B'')$

$$\Gamma \vdash A \rhd B$$

domknięcie przechodnie redukcji beta, iota, delta i zeta.

Konwersja — równość definicyjna, obliczeniowa

ang. *d*efinitional equality

reguła konwersji

$$\frac{\Gamma \vdash M : A \qquad \Gamma \vdash A =_{\beta\eta\delta\zeta\iota} B \qquad \Gamma \vdash B : s}{\Gamma \vdash M : B}$$

$$\Gamma \vdash A =_{\beta\eta\delta\zeta\iota} B$$

jeśli

- $\Gamma \vdash A \triangleright^* A'$
- $\Gamma \vdash B \triangleright^* B'$
- $A' = B'$ lub
  $(A' = \lambda x : T.A''$ i $\Gamma, x : T \vdash B'x =_{\beta\eta\delta\zeta\iota} A'')$ lub
  $(B' = \lambda x : T.B''$ i $\Gamma, x : T \vdash A'x =_{\beta\eta\delta\zeta\iota} B'')$

$$\Gamma \vdash A \triangleright B$$

domknięcie przechodnie redukcji beta, iota, delta i zeta.

Reguły redukcji na przykładzie

```
Definition pred' (x : nat) :=
  match x with
    | O ⇒ O
    | S n' ⇒ let y := n' in y
  end.

Theorem reduce_me : pred' 1 = 0.


  cbv delta.
```

Reguły redukcji w taktyce cbv

```
============================
 (fun x : nat ⇒ match x with
                | 0 ⇒ 0
                | S n' ⇒ let y := n' in y
                end) 1 = 0
```

```
cbv beta.
```

Reguły redukcji w taktyce cbv

```
============================
 match 1 with
 | 0 ⇒ 0
 | S n' ⇒ let y := n' in y
 end = 0
```

```
cbv iota.
```

Reguły redukcji w taktyce cbv

```
============================
 (fun n' : nat ⇒ let y := n' in y) 0 = 0

cbv beta.

============================
 (let y := 0 in y) = 0

cbv zeta.

============================
 0 = 0
```

eq — równość definiowalna

ang. *p*ropositional equality
definiowana jako relacja indukcyjna

$$\texttt{Inductive}\ \mathbf{eq}\ (A : \texttt{Type})\ (x : A) : A \to \texttt{Prop} := \texttt{eq\_refl} : x = x$$

```
eq_ind: forall (A : Type) (x : A) (P : A -> Prop),
                        P x -> forall y : A, x = y -> P y
```

eq — równość definiowalna

ang. *p*ropositional equality
definiowana jako relacja indukcyjna

$$\texttt{Inductive } \mathbf{eq}\ (A : \texttt{Type})\ (x : A) : A \to \texttt{Prop} := \texttt{eq\_refl} : x = x$$

```
eq_ind: forall (A : Type) (x : A) (P : A -> Prop),
                        P x -> forall y : A, x = y -> P y
```

Problemy z równością

lemmaUIP jest niedowodliwy:

```
Lemma lemmaUIP : ∀ (x : A) (pf : x = x), pf = eq_refl x.
```

dowodliwy jest lemma2:

```
Lemma lemma2 : ∀ (x : A) (pf : x = x), O = match pf with eq_refl ⇒
O end.
```

Dowód lemma2

```
Definition lemma2 :=
  fun (x : A) (pf : x = x) =>
    match pf return (0 = match pf with
                         | eq_refl => 0
                         end) with
      | eq_refl => eq_refl 0
    end.
```

Aksjomat UIP_refl

```
Check UIP_refl.
```

```
UIP_refl
     : ∀ (U : Type) (x : U) (p : x = x), p = eq_refl x
```

UIP_refl równoważny z aksjomatem Streicher_K

```
Check Streicher_K.
```

```
Streicher_K
     : ∀ (U : Type) (x : U) (P : x = x → Prop),
       P eq_refl → ∀ p : x = x, P p
```

Streicher's axiom K jest niesprzeczny z CIC i niedowodliwy w CIC

Dla typów rozstrzygalnych

czyli takich, że

```
Variable eq_dec : forall x y:A, {x = y} + {x <> y}.
```

zachodzą prawa `UIP_dec`, `UIP_refl` i `K_dec`

```
forall (x y:A) (p1 p2:x = y), p1 = p2
```

```
forall (x y:A) (p:x = x), p = eq_refl x
```

```
forall (x:A) (P:x = x -> Prop), P (eq_refl x)
                                  -> forall p:x = x, P p
```

bez dodatkowych aksjomatów (patrz: moduł `Eqdep_dec` z biblioteki standardowej)

Lemat `UIP_refl_nat` jest dowodliwy w Coqu

UIP_refl_nat
: $\forall\ (x : nat)\ (p : x = x),\ p =$ eq_refl x

(patrz: plik `UIP_refl_nat.v`)

Problemy z równością cd.

Poniższego twierdzenia "nie da się zapisać"

```
Theorem vappend_assoc : ∀ a b c
  (va : vector a ) (vb : vector b) (vc : vector c ),
  vappend (vappend va vb) vc = vappend va (vappend vb vc).
```

```
Error:
The term "vappend va (vappend vb vc)"
has type "vector (a + (b + c))"
while it is expected to have type "vector (a + b + c)".
```

Trzeba wstawić "type-cast"

```
Theorem vappend_assoc : ∀ a b c
  (va : vector a ) (vb : vector b) (vc : vector c ),
  vappend (vappend va vb) vc =
    match Plus.plus_assoc a b c in (_ = X)
    return vector X with
      | eq_refl ⇒ vappend va (vappend vb vc)
    end.
```

Równość heterogeniczna

```
Inductive JMeq (A : Type) (x : A) : ∀ B : Type, B → Prop :=
    JMeq_refl : JMeq x x
```

```
Infix "==" := JMeq (at level 70, no associativity).
```

Związki eq i JMeq

```
JMeq_rect
  : forall (A : Type) (x : A) (P : forall B : Type, B -> Type),
  P A x -> forall (B : Type) (b : B), x == b -> P B b

eq_rect
  : forall (A : Type) (x : A) (P : A -> Type),
  P x -> forall y : A, x = y -> P y
```

Związki eq i JMeq

```
Lemma eq_JMeq : ∀ (A : Type) (x y : A), x = y → x == y.
  intros; rewrite H; reflexivity.
Qed.
```

Ale odwrotna implikacja jest niedowodliwa:

```
Check JMeq_eq.
```

```
JMeq_eq
     : ∀ (A : Type) (x y : A), x == y → x = y
```

Związki eq i JMeq

```
Lemma eq_JMeq : ∀ (A : Type) (x y : A), x = y → x == y.
  intros; rewrite H; reflexivity.
Qed.
```

Ale odwrotna implikacja jest niedowodliwa:

```
Check JMeq_eq.
```

```
JMeq_eq
     : ∀ (A : Type) (x y : A), x == y → x = y
```

Aksjomat JMeq_eq

- może być bezpiecznie dodany do CIC
- może byc używany przez rewrite w postaci

```
JMeq_ind_r
  : forall (A : Type) (x : A) (P : A -> Type),
  P x -> forall y : A, x == y -> P y
```

Dowód `pairC'`

Dwa sposoby:

- używający aksjomatu `JMeq_eq`
- używający naturalnej zasady indukcji dla JMeq

Użyte aksjomaty sprawdzamy za pomocą:

```
Print Assumptions pairC'.
```

Patrz plik JMeqRew.v

Dowód `pairC'`

Dwa sposoby:

- używający aksjomatu `JMeq_eq`
- używający naturalnej zasady indukcji dla JMeq

Użyte aksjomaty sprawdzamy za pomocą:

```
Print Assumptions pairC'.
```

Patrz plik JMeqRew.v

Lemat vappend_assoc

Patrz plik vappend_assoc.v