

Preuves en logique équationnelle

David Delahaye

David.Delahaye@lirmm.fr

Université de Montpellier
Faculté des Sciences

Licence Informatique L3 2022-2023



Égalité

Syntaxe

- C'est un prédicat binaire, noté de manière infixe ;
- $s \doteq t$, où s et t sont des termes.

Sémantique

- $\llbracket s \doteq t \rrbracket'_\rho = (\llbracket s \rrbracket'_\rho = \llbracket t \rrbracket'_\rho)$;
- Où « $=$ » est l'égalité sur D_I ;
- Ne pas confondre la syntaxe et la sémantique :
 - « \doteq » \equiv égalité syntaxique ;
 - « $=$ » \equiv égalité sémantique.

Égalité

Syntaxe

- C'est un prédicat binaire, noté de manière infixé ;
- $s \doteq t$, où s et t sont des termes.

Sémantique

- $\llbracket s \doteq t \rrbracket'_\rho = (\llbracket s \rrbracket'_\rho = \llbracket t \rrbracket'_\rho)$;
- Où « $=$ » est l'égalité sur D_I ;
- Ne pas confondre la syntaxe et la sémantique :
 - ▶ « \doteq » \equiv égalité syntaxique ;
 - ▶ « $=$ » \equiv égalité sémantique.

Équations : syntaxe

- Équation \equiv paire de termes notée $s \doteq t$;
- Les termes s et t ne sont pas forcément clos ;
- Mais la quantification sur les variables libres est implicite ;
- $s \doteq t \equiv \forall \vec{x}. s \doteq t$, où $\vec{x} = FV(s) \cup FV(t)$;
- Exemple : $x + 0 \doteq x \equiv \forall x. x + 0 \doteq x$.

Équations : sémantique

- Soit $s \doteq t$ une équation et I une interprétation ;
- I est un modèle de $s \doteq t$ ou I satisfait $s \doteq t$, noté $I \models s \doteq t$, ssi pour toute affectation ρ , $\llbracket s \rrbracket_\rho^I = \llbracket t \rrbracket_\rho^I$;
- Un ensemble \mathcal{E} d'équations entraîne $s \doteq t$, noté $\mathcal{E} \models s \doteq t$, ssi toutes les interprétations satisfaisant toutes les équations de \mathcal{E} en même temps (les modèles de \mathcal{E}) sont aussi des modèles de $s \doteq t$, c'est-à-dire quand $I \models s' \doteq t'$ pour tout $s' \doteq t' \in \mathcal{E}$ implique $I \models s \doteq t$.

Exemple

Conséquence logique

- Démontrer que : $x + 0 \doteq x, x + y \doteq y + x \models 0 + x \doteq x$, où 0 est une constante et « $+$ » est un symbole de fonction binaire noté de manière infixé ;
- Démonstration :
 - Soit I une interprétation telle que $I \models x + 0 \doteq x$ et $I \models x + y \doteq y + x$, c'est-à-dire pour toute affectation ρ :
 - ★ $\llbracket x + 0 \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), I(0)) = \rho(x)$ (1) ;
 - ★ $\llbracket x + y \rrbracket_{\rho}^I = \llbracket y + x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), \rho(y)) = I(+)(\rho(y), \rho(x))$ (2).
 - On doit démontrer que $I \models 0 + x \doteq x$, c'est-à-dire pour toute affectation ρ , $\llbracket 0 + x \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(I(0), \rho(x)) = \rho(x)$:
 - ★ $I(+)(I(0), \rho(x)) = I(+)(\rho(x), I(0))$, selon (2) ;
 - ★ Puis, $I(+)(\rho(x), I(0)) = \rho(x)$, selon (1).

Exemple

Conséquence logique

- Démontrer que : $x + 0 \doteq x, x + y \doteq y + x \models 0 + x \doteq x$, où 0 est une constante et « $+$ » est un symbole de fonction binaire noté de manière infixe ;
- Démonstration :
 - ▶ Soit I une interprétation telle que $I \models x + 0 \doteq x$ et $I \models x + y \doteq y + x$, c'est-à-dire pour toute affectation ρ :
 - ★ $\llbracket x + 0 \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), I(0)) = \rho(x)$ (1) ;
 - ★ $\llbracket x + y \rrbracket_{\rho}^I = \llbracket y + x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), \rho(y)) = I(+)(\rho(y), \rho(x))$ (2).
 - ▶ On doit démontrer que $I \models 0 + x \doteq x$, c'est-à-dire pour toute affectation ρ , $\llbracket 0 + x \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(I(0), \rho(x)) = \rho(x)$:
 - ★ $I(+)(I(0), \rho(x)) = I(+)(\rho(x), I(0))$, selon (2) ;
 - ★ Puis, $I(+)(\rho(x), I(0)) = \rho(x)$, selon (1).

Exemple

Conséquence logique

- Démontrer que : $x + 0 \doteq x, x + y \doteq y + x \models 0 + x \doteq x$, où 0 est une constante et « $+$ » est un symbole de fonction binaire noté de manière infixé ;
- Démonstration :
 - ▶ Soit I une interprétation telle que $I \models x + 0 \doteq x$ et $I \models x + y \doteq y + x$, c'est-à-dire pour toute affectation ρ :
 - ★ $\llbracket x + 0 \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), I(0)) = \rho(x)$ (1) ;
 - ★ $\llbracket x + y \rrbracket_{\rho}^I = \llbracket y + x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), \rho(y)) = I(+)(\rho(y), \rho(x))$ (2).
 - ▶ On doit démontrer que $I \models 0 + x \doteq x$, c'est-à-dire pour toute affectation ρ , $\llbracket 0 + x \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(I(0), \rho(x)) = \rho(x)$:
 - ★ $I(+)(I(0), \rho(x)) = I(+)(\rho(x), I(0))$, selon (2) ;
 - ★ Puis, $I(+)(\rho(x), I(0)) = \rho(x)$, selon (1).

Exemple

Conséquence logique

- Démontrer que : $x + 0 \doteq x, x + y \doteq y + x \models 0 + x \doteq x$, où 0 est une constante et « $+$ » est un symbole de fonction binaire noté de manière infixe ;
- Démonstration :
 - ▶ Soit I une interprétation telle que $I \models x + 0 \doteq x$ et $I \models x + y \doteq y + x$, c'est-à-dire pour toute affectation ρ :
 - ★ $\llbracket x + 0 \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), I(0)) = \rho(x)$ (1) ;
 - ★ $\llbracket x + y \rrbracket_{\rho}^I = \llbracket y + x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), \rho(y)) = I(+)(\rho(y), \rho(x))$ (2).
 - ▶ On doit démontrer que $I \models 0 + x \doteq x$, c'est-à-dire pour toute affectation ρ , $\llbracket 0 + x \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(I(0), \rho(x)) = \rho(x)$:
 - ★ $I(+)(I(0), \rho(x)) = I(+)(\rho(x), I(0))$, selon (2) ;
 - ★ Puis, $I(+)(\rho(x), I(0)) = \rho(x)$, selon (1).

Exemple

Conséquence logique

- Démontrer que : $x + 0 \doteq x, x + y \doteq y + x \models 0 + x \doteq x$, où 0 est une constante et « $+$ » est un symbole de fonction binaire noté de manière infixé ;
- Démonstration :
 - ▶ Soit I une interprétation telle que $I \models x + 0 \doteq x$ et $I \models x + y \doteq y + x$, c'est-à-dire pour toute affectation ρ :
 - ★ $\llbracket x + 0 \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), I(0)) = \rho(x)$ (1) ;
 - ★ $\llbracket x + y \rrbracket_{\rho}^I = \llbracket y + x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(\rho(x), \rho(y)) = I(+)(\rho(y), \rho(x))$ (2).
 - ▶ On doit démontrer que $I \models 0 + x \doteq x$, c'est-à-dire pour toute affectation ρ , $\llbracket 0 + x \rrbracket_{\rho}^I = \llbracket x \rrbracket_{\rho}^I$, c.-à-d. $I(+)(I(0), \rho(x)) = \rho(x)$:
 - ★ $I(+)(I(0), \rho(x)) = I(+)(\rho(x), I(0))$, selon (2) ;
 - ★ Puis, $I(+)(\rho(x), I(0)) = \rho(x)$, selon (1).

Substitution

Définition

- Une substitution σ est une application de \mathcal{V} vers \mathcal{T} ;
- Elle se définit par récurrence structurelle comme suit :
 - ▶ Si $x \in \mathcal{V}$ alors $\sigma(x) = \sigma(x)$;
 - ▶ Si $f \in \mathcal{S}_{\mathcal{F}}$ d'arité n et $t_1, \dots, t_n \in \mathcal{T}$ alors
 $\sigma(f(t_1, \dots, t_n)) = f(\sigma(t_1), \dots, \sigma(t_n))$.

Exemple

- Soit la substitution σ telle que $\sigma(x) = a$ et $\sigma(y) = f(b)$, où a et b sont des constantes, et f un symbole de fonction unaire ;
- $\sigma(f(x, y)) = f(a, f(b))$.

Position et substitution

Position

- Une position est un élément de $(\mathbb{N} - \{0\})^*$;
- Étant donné un terme t , le terme $t|_p$ désigne le terme à la position p et se définit par récurrence structurelle sur les positions :
 - ▶ Si $p = \epsilon$, $t|_\epsilon = t$;
 - ▶ Si $p = i \cdot p'$ et $t = f(t_1, \dots, t_n)$, où l'on a $i \leq n$ et où p' est une position, alors $t|_{i \cdot p'} = t_i|_{p'}$.
- Exemples : si $t = f(x, g(y, z))$, $t|_\epsilon = f(x, g(y, z))$, $t|_1 = x$, $t|_2 = g(y, z)$, $t|_{21} = y$, $t|_{22} = z$.

Substitution à une position donnée

- La notation $t[u]_p$ désigne la substitution de u au terme $t|_p$ dans t ;
- Exemple : si $t = f(x, g(y, z))$, $t[h(a)]_{21} = f(x, g(h(a), z))$.

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Règles

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ ax}$$

$$\frac{}{s \doteq s} \text{ refl}$$

$$\frac{s \doteq t}{t \doteq s} \text{ sym}$$

$$\frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ trans}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ subst}$$

$$\frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ cont}$$

Système de preuve pour la logique équationnelle (EQ)

Arbre de preuve (arbre de dérivation)

- On part de l'équation initiale à démontrer ;
- On applique les règles en raisonnement abductif (raisonnement arrière), c'est-à-dire que l'on part de ce qu'on veut montrer pour aller vers les hypothèses/axiomes) ;
- On construit ainsi un arbre dont le séquent est la racine et les branches sont créées par les différentes prémisses des règles de déduction ;
- Dans une branche, on s'arrête lorsqu'on atteint une règle axiomatique, qui devient ainsi une feuille de l'arbre ;
- Un arbre de preuve est un arbre dont toutes les branches se terminent par une règle axiomatique (on parle alors de branche close).

Prouvabilité

- $s \doteq t$ est prouvable dans EQ à partir de \mathcal{E} , noté $\mathcal{E} \vdash_{\text{EQ}} s \doteq t$, ssi il existe une dérivation dans EQ se terminant sur $s \doteq t$ à partir de \mathcal{E} .

Théorème d'adéquation (Birkhoff, 1933)

- Correction : Si $\mathcal{E} \vdash_{\text{EQ}} s \doteq t$ alors $\mathcal{E} \models s \doteq t$;
- Complétude : Si $\mathcal{E} \models s \doteq t$ alors $\mathcal{E} \vdash_{\text{EQ}} s \doteq t$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$\frac{\begin{array}{c} x + y \doteq y + x \in \mathcal{E} \\ x + y \doteq y + x \quad x + 0 \doteq x \in \mathcal{E} \\ 0 + x \doteq x + 0 \quad x + 0 \doteq x \end{array}}{0 + x \doteq x}$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$x + y \doteq y + x \in \mathcal{E}$$

$$x + y \doteq y + x$$

$$x + 0 \doteq x \in \mathcal{E}$$

$$0 + x \doteq x + 0$$

$$x + 0 \doteq x$$

$$0 + x \doteq x$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$\frac{\begin{array}{c} x + y \doteq y + x \in \mathcal{E} \\ x + y \doteq y + x \end{array} \quad \begin{array}{c} x + 0 \doteq x \in \mathcal{E} \\ x + 0 \doteq x \end{array}}{0 + x \doteq x + 0 \quad x + 0 \doteq x} \text{trans}$$
$$0 + x \doteq x$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$\frac{\frac{x + y \doteq y + x \in \mathcal{E}}{0 + x \doteq x + 0} \text{ subst} \quad \frac{x + 0 \doteq x \in \mathcal{E}}{x + 0 \doteq x} \text{ trans}}{0 + x \doteq x} \text{ trans}$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$\frac{\frac{\frac{x + y \doteq y + x \in \mathcal{E}}{x + y \doteq y + x} \text{ ax}}{0 + x \doteq x + 0} \text{ subst} \quad \frac{x + 0 \doteq x \in \mathcal{E}}{x + 0 \doteq x} \text{ trans}}{0 + x \doteq x} \text{ trans}$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Exemple de preuve

Exemple précédent

- $\mathcal{E} = x + 0 \doteq x, x + y \doteq y + x$;
- On veut démontrer que $\mathcal{E} \vdash_{\text{EQ}} 0 + x \doteq x$:

$$\frac{\frac{\frac{x + y \doteq y + x \in \mathcal{E}}{x + y \doteq y + x} \text{ ax}}{0 + x \doteq x + 0} \text{ subst} \quad \frac{x + 0 \doteq x \in \mathcal{E}}{x + 0 \doteq x} \text{ ax}}{0 + x \doteq x} \text{ trans}$$

- Pour la règle subst, σ est telle que $\sigma(x) = 0$ et $\sigma(y) = x$.

Faire le lien entre EQ et LK/LJ

Nouvelle formulation pour EQ

$$\frac{\forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash s \doteq t} \text{ax}_{\text{eq}}$$

$$\frac{}{\Gamma \vdash s \doteq s} \text{refl}$$

$$\frac{\Gamma \vdash s \doteq t}{\Gamma \vdash t \doteq s} \text{sym}$$

$$\frac{\Gamma \vdash s \doteq t \quad \Gamma \vdash t \doteq u}{\Gamma \vdash s \doteq u} \text{trans}$$

$$\frac{\Gamma \vdash s \doteq t}{\Gamma \vdash u[s]_p \doteq u[t]_p} \text{cont}$$

Remarques

- On ajoute un séquent (avec des équations et d'autres formules).
- Les équations sont explicitement (universellement) quantifiées.
- La règle ax_{eq} gère les instanciations.
- La règle subst est capturée par la règle ax_{eq}

Faire le lien entre EQ et LK/LJ

Ajout de règles à LK

$$\frac{\Gamma \vdash \Delta, s \doteq t \quad \Gamma \vdash \Delta, P(s)}{\Gamma \vdash \Delta, P(t)} =_{\text{right}}$$

$$\frac{\Gamma \vdash \Delta, s \doteq t \quad \Gamma, P(s) \vdash \Delta}{\Gamma, P(t) \vdash \Delta} =_{\text{left}}$$

Ajout de règles à LJ

$$\frac{\Gamma \vdash s \doteq t \quad \Gamma \vdash P(s)}{\Gamma \vdash P(t)} =_{\text{right}}$$

$$\frac{\Gamma \vdash s \doteq t \quad \Gamma, P(s) \vdash A}{\Gamma, P(t) \vdash A} =_{\text{left}}$$

Faire le lien entre EQ et LK/LJ

Nouvelle formulation pour EQ

$$\frac{\forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash s \doteq t} \text{ax}_{\text{eq}}$$
$$\frac{}{\Gamma \vdash s \doteq s} \text{refl}$$

Remarques

- Les règles $=_{\text{right}}$ et $=_{\text{left}}$ sont très puissantes.
- Les règles sym, trans et cont deviennent redondantes !
- En effet, il suffit de prendre l'égalité \doteq pour P .

Règles concernant l'égalité

$$\frac{\forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash s \doteq t} \text{ax}_{eq}$$

$$\frac{}{\Gamma \vdash s \doteq s} \text{refl}$$

$$\frac{\Gamma \vdash \Delta, s \doteq t \quad \Gamma \vdash \Delta, P(s)}{\Gamma \vdash \Delta, P(t)} =_{\text{right}}$$

$$\frac{\Gamma \vdash \Delta, s \doteq t \quad \Gamma, P(s) \vdash \Delta}{\Gamma, P(t) \vdash \Delta} =_{\text{left}}$$

Règles concernant l'égalité

$$\frac{\forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash s \doteq t} \text{ax}_{\text{eq}}$$

$$\frac{}{\Gamma \vdash s \doteq s} \text{refl}$$

$$\frac{\Gamma \vdash s \doteq t \quad \Gamma \vdash P(s)}{\Gamma \vdash P(t)} =_{\text{right}}$$

$$\frac{\Gamma \vdash s \doteq t \quad \Gamma, P(s) \vdash A}{\Gamma, P(t) \vdash A} =_{\text{left}}$$

Preuve dans LK_{EQ}/LJ_{EQ}

Exemple

- $\Gamma = \forall x. x + 0 \doteq x, \forall x, y. x + y \doteq y + x.$
- On veut démontrer que $\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x).$

$$\frac{\frac{\Gamma \vdash x + 0 \doteq 0 + x}{\Gamma \vdash 0 + x \doteq x} \text{ax}_{eq} \quad \frac{\Gamma \vdash x + 0 \doteq x}{\Gamma \vdash 0 + x \doteq x} \text{ax}_{eq}}{\Gamma \vdash 0 + x \doteq x} \text{=right} \quad \frac{\Gamma, P(0 + x) \vdash P(0 + x)}{\Gamma, P(0 + x) \vdash P(x)} \text{ax}$$
$$\frac{\frac{\Gamma \vdash 0 + x \doteq x}{\Gamma \vdash P(0 + x) \Rightarrow P(x)} \Rightarrow_{right} \quad \frac{\Gamma, P(0 + x) \vdash P(x)}{\Gamma \vdash P(0 + x) \Rightarrow P(x)} \Rightarrow_{right}}{\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x)} \forall_{right}$$

Preuve dans LK_{EQ}/LJ_{EQ}

Exemple

- $\Gamma = \forall x. x + 0 \doteq x, \forall x, y. x + y \doteq y + x.$
- On veut démontrer que $\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x).$

$$\frac{\frac{\Gamma \vdash x + 0 \doteq 0 + x}{\Gamma \vdash 0 + x \doteq x} \text{ax}_{eq} \quad \frac{\Gamma \vdash x + 0 \doteq x}{\Gamma \vdash 0 + x \doteq x} \text{ax}_{eq}}{\Gamma \vdash 0 + x \doteq x} =_{right} \quad \frac{\Gamma, P(0 + x) \vdash P(0 + x)}{\Gamma, P(0 + x) \vdash P(x)} \text{ax}$$
$$\frac{\Gamma, P(0 + x) \vdash P(x)}{\Gamma \vdash P(0 + x) \Rightarrow P(x)} \Rightarrow_{right} \quad \frac{\Gamma \vdash P(0 + x) \Rightarrow P(x)}{\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x)} \forall_{right}$$

Optimisations de LK_{EQ}

Remplacement des règles $=_{right}$ et $=_{left}$ dans LK

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{right1}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{right2}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{left1}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{left2}$$

Remarque

- La règle ax_{eq} devient redondante !

Optimisations de LK_{EQ}

Remplacement des règles $=_{right}$ et $=_{left}$ dans LK

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{right1}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{right2}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{left1}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{left2}$$

Remarque

- La règle ax_{eq} devient redondante !

Optimisations de LK_{EQ}

Remplacement des règles $=_{right}$ et $=_{left}$ dans LK

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{right1}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{right2}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{left1}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{left2}$$

Remarque

- La règle ax_{eq} devient redondante !

Optimisations de LK_{EQ}

Remplacement des règles $=_{right}$ et $=_{left}$ dans LK

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{right1}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{right2}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{left1}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{left2}$$

Remarque

- La règle ax_{eq} devient redondante !

Optimisations de LK_{EQ}

Remplacement des règles $=_{right}$ et $=_{left}$ dans LK

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{right1}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{right2}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{left1}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{left2}$$

Remarque

- La règle ax_{eq} devient redondante !

Optimisations de LJ_{EQ}

Remplacement des règles $=_{\text{right}}$ et $=_{\text{left}}$ dans LJ

$$\frac{\Gamma \vdash P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(t)} =_{\text{right1}}$$

$$\frac{\Gamma \vdash P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(s)} =_{\text{right2}}$$

$$\frac{\Gamma, P(s) \vdash A \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash A} =_{\text{left1}}$$

$$\frac{\Gamma, P(t) \vdash A \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash A} =_{\text{left2}}$$

Remarque

- La règle ax_{eq} est toujours redondante.

Système LK_{EQ} (version finale et optimisée)

Règles concernant l'égalité

$$\frac{}{\Gamma \vdash s \doteq s} \text{ refl}$$

$$\frac{\Gamma \vdash \Delta, P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(t)} =_{\text{right1}}$$

$$\frac{\Gamma \vdash \Delta, P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash \Delta, P(s)} =_{\text{right2}}$$

$$\frac{\Gamma, P(s) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash \Delta} =_{\text{left1}}$$

$$\frac{\Gamma, P(t) \vdash \Delta \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash \Delta} =_{\text{left2}}$$

Système LJ_{EQ} (version finale et optimisée)

Règles concernant l'égalité

$$\frac{}{\Gamma \vdash s \doteq s} \text{ refl}$$

$$\frac{\Gamma \vdash P(s) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(t)} =_{\text{right1}}$$

$$\frac{\Gamma \vdash P(t) \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(s)} =_{\text{right2}}$$

$$\frac{\Gamma, P(s) \vdash A \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash A} =_{\text{left1}}$$

$$\frac{\Gamma, P(t) \vdash A \quad \forall \vec{x}. s' \doteq t' \in \Gamma \quad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash A} =_{\text{left2}}$$

Exemple

- $\Gamma = \forall x. x + 0 \doteq x, \forall x, y. x + y \doteq y + x$.
- On veut démontrer que $\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x)$.

$$\frac{\frac{\frac{\frac{\overline{\Gamma, P(x) \vdash P(x)}}{ax}}{\Gamma, P(x+0) \vdash P(x)} =_{\text{left2}, \sigma_2}}{\Gamma, P(0+x) \vdash P(x)} =_{\text{left1}, \sigma_1}}{\Gamma \vdash P(0+x) \Rightarrow P(x)} \Rightarrow_{\text{right}} \frac{\Gamma \vdash \forall x. P(0+x) \Rightarrow P(x)}{\forall_{\text{right}}}$$

$$\sigma_1 = [x/x, 0/y], \sigma_2 = [x/x].$$

Exemple

- $\Gamma = \forall x. x + 0 \doteq x, \forall x, y. x + y \doteq y + x$.
- On veut démontrer que $\Gamma \vdash \forall x. P(0 + x) \Rightarrow P(x)$.

$$\frac{\frac{\frac{\overline{\Gamma, P(x) \vdash P(x)}^{ax}}{\Gamma, P(x+0) \vdash P(x)} =_{\text{left2}, \sigma_2}}{\Gamma, P(0+x) \vdash P(x)} =_{\text{left1}, \sigma_1}}{\Gamma \vdash P(0+x) \Rightarrow P(x)} \Rightarrow_{\text{right}} \frac{\Gamma \vdash \forall x. P(0+x) \Rightarrow P(x)}{\Gamma \vdash \forall x. P(0+x) \Rightarrow P(x)} \forall_{\text{right}}$$

$$\sigma_1 = [x/x, 0/y], \sigma_2 = [x/x].$$

Équivalence entre les règles de LJ_{EQ} et les tactiques de Coq

Règle de LJ_{EQ}	Tactique Coq
<code>refl</code>	<code>reflexivity</code>
<code>=right1</code>	<code>rewrite <- id</code>
<code>=right2</code>	<code>rewrite id</code>
<code>=left1</code>	<code>rewrite <- in id</code>
<code>=left2</code>	<code>rewrite in id</code>

- Ne pas oublier que Coq fonctionne en abductif.
- Par défaut, les réécritures sont gauche-droite.
- La réécriture droite-gauche s'indique explicitement avec `rewrite <-`.

Raisonnement équationnel en Coq

Un exemple simple

```
Coq < Parameter E : Set.
```

```
E is assumed
```

```
Coq < Parameters a b : E.
```

```
a is assumed
```

```
b is assumed
```

```
Coq < Parameter P : E -> Prop.
```

```
P is assumed
```

```
Coq < Axiom eq : a = b.
```

```
eq is assumed
```

Raisonnement équationnel en Coq

Un exemple simple

```
Coq < Goal P(b) -> P(a).
```

```
1 subgoal
```

```
=====
```

```
P b -> P a
```

```
Coq < intro.
```

```
1 subgoal
```

```
H : P b
```

```
=====
```

```
P a
```

Raisonnement équationnel en Coq

Un exemple simple

```
Coq < rewrite eq.
```

```
1 subgoal
```

```
  H : P b
```

```
=====
```

```
  P b
```

```
Coq < assumption.
```

```
No more subgoals.
```

Raisonnement équationnel en Coq

Sens de la réécriture

```
Coq < Goal P(a) -> P(b).
```

```
1 subgoal
```

```
=====
```

```
P a -> P b
```

```
Coq < intro.
```

```
1 subgoal
```

```
H : P a
```

```
=====
```

```
P b
```


Raisonnement équationnel en Coq

Sens de la réécriture

```
Coq < rewrite <- eq.
```

```
1 subgoal
```

```
  H : P a
```

```
=====
```

```
  P a
```

```
Coq < assumption.
```

```
No more subgoals.
```