On supposera connue la syntaxe de la logique du premier ordre.

I) Systèmes formels - Définitions.

def 1 : Soit $\mathcal{L}$ un langage. Les **formules atomiques** de $\mathcal{L}$ sont les formules de la forme $R(t_1, \dots, t_n)$ où R est un symbole de relation n-aire et $t_1, \dots t_n$ des termes de $\mathcal{L}$. L'ensemble $\mathcal{F}$ des **formules** du 1er ordre de $\mathcal{L}$ est défini par la grammaire $\mathcal{F} = \text{Atom} \mid \mathcal{F} \vee \mathcal{F} \mid \mathcal{F} \wedge \mathcal{F} \mid \mathcal{F} \to \mathcal{F} \mid \neg \mathcal{F} \mid \exists x \mathcal{F} \mid \forall x \mathcal{F}$

def 2 : Une **sous-formule** de F est l'un de ses composants, ie une formule à partir de laquelle F est construite.

def 3 : Une formule F de $\mathcal{L}$ n'utilise qu'un nombre fini de symboles de F. Ce sous-ensemble est appelé **langage de la formule** et noté $\mathcal{L}(F)$.

def 4 : Soit F une formule. L'ensemble $VL(F)$ des **variables libres** de F est défini par :
- si $F = R(t_1, \dots, t_n)$ est atomique : $VL(F)$ est l'ensemble des variables apparaissant dans les t_i
- si $F = F_1 \oplus F_2$ où $\oplus \in \{\wedge, \vee, \to\}$, $VL(F) = VL(F_1) \cup VL(F_2)$
- si $F = \neg F_1$, $VL(F) = VL(F_1)$
- si $F = Qx F_1$ avec $Q \in \{\exists, \forall\}$, $VL(F) = VL(F_1) - \{x\}$

exemple 5 : $VL(\forall x, (x.y = y.x)) = \{y\}$
$VL((\forall x \exists y (x = z = z \cdot y)) \cap (x = z \cdot z)) = \{x, z\}$.

def 6 : Un **séquent** est un couple noté $\Gamma \vdash A$ où Γ est un ensemble fini de formules et A une formule. Sous les hypothèses Γ, on montre A.

def 7 : Une **règle de démonstration** notée $\frac{\text{prémisses}}{\text{conclusion}}$ nommé est un couple où les prémisses sont un nombre fini de séquents et la conclusion un séquent.

def 8 : Un **système formel de preuve** est un couple formé d'un ensemble d'axiomes et d'un ensemble de règles d'inférence.

def 9 : Un séquent est **prouvable** ou **dérivable** s'il peut être obtenu par une application finie de règles d'inférence. Une formule est prouvable si le séquent $\vdash F$ est prouvable.

II) Systèmes formels classiques.

21 - La déduction naturelle

def 10 : règles de la déduction naturelle en annexe.

exemple 11 : $\vdash (A \wedge B \to C) \to (A \to B \to C)$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A \wedge B \to C}\,ax \quad \dfrac{\dfrac{}{\Gamma \vdash A}\,ax \quad \dfrac{}{\Gamma \vdash B}\,ax}{\Gamma \vdash A \wedge B}\,\wedge i}{\Gamma = A \wedge B \to C, A, B \vdash C}\,\to e}{\vdash (A \wedge B \to C) \to (A \to B \to C)}\,\to i \times 3$$

Remarque 12 : On préfèrera par la suite une notation linéaire.

Def 13 : Une **règle dérivée** est une règle démontrée à l'aide des règles de base.

Exemple 14 : Les règles suivantes sont dérivables :

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \text{coupure} ; \qquad \frac{\Gamma, A \vdash B \quad \Gamma, \neg A \vdash B}{\Gamma \vdash B}\ \text{tiers exclu}$$

$$\frac{\Gamma, u = v \vdash A[x := u]}{\Gamma, u = v \vdash A[x := v]}\ =g \qquad \frac{}{\Gamma, u = v \vdash t[x := u] = t[x := v]}\ =c$$

Exple 15 : Exemple de démonstration : "les involutions sont des bijections".

22 - Calcul des séquents.

Ici on ne se préoccupe pas des règles sur l'égalité : elles peuvent être remplacées par des axiomes (théorie de l'égalité).

214

Prénom :

NOM :

N° - Date - Titre de la leçon : 58

On souhaite avoir un système de règles plus symétriques, donc les règles d'élimination sont remplacées par des règles d'introduction à gauche.

Def 16 : Un **séquent** est une expression de la forme $\Gamma \vdash \Delta$, où Δ et Γ sont des multi-ensembles finis de formules.

Rmq 17 : . Le sens de $A_1, \dots, A_n \vdash B_1, \dots, B_m$ est celui de $A_1 \wedge \dots \wedge A_n \to B_1 \vee \dots \vee B_m$.
. le séquent $A_1, \dots, A_n \vdash$ est interprété comme $\neg(A_1 \wedge \dots \wedge A_n)$ et le séquent $\vdash B_1, \dots, B_m$ comme $B_1 \vee \dots \vee B_m$.
. le séquent $\vdash$ (vrai implique (aux)) est interprété comme l'absurde.

Def 18 : règles du calcul des séquents en annexe 2.

Exple 19 : . $\vdash A \vee \neg A$ (tiers exclu)

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ax}{\vdash A, \neg A}\,\neg_d}{\vdash A \vee \neg A}\,\vee_d$$

Th 20 : . Soient Γ, A des formules.
. Si $\Gamma \vdash A$ en déduction naturelle, alors $\Gamma \vdash A$ en calcul des séquents.
. Soient Γ, Δ des formules. Si $\Delta = A_1, \dots, A_n$ on notera $\neg\Delta = \neg A_1, \dots, \neg A_n$. Si $\Gamma \vdash \Delta$ en calcul des séquents, alors $\Gamma, \neg\Delta \vdash \bot$ en déduction naturelle.

Def 21 : Une **dérivation normale** est une dérivation qui n'utilise pas la règle de coupure.

Th 22 : **Elimination des coupures.** Soient Γ, Δ des formules. Si $\Gamma \vdash \Delta$, alors il en existe une dérivation normale.

Csq 23 : Soit A une formule atomique.
(i) les séquents $\vdash$ et $\vdash A$ ne sont pas dérivables
(ii) Si $A \neq \bot$, alors $A \vdash$ et $\vdash \neg A$ ne sont pas dérivables.

Csq 24 : **Propriété de la sous-formule** : "Un théorème contient tout ce qu'il faut pour sa démonstration". Soient Γ, Δ des formules. Si $\Gamma \vdash \Delta$ alors il existe une dérivation de ce séquent dont toutes les formules sont de la forme $A(x_1 := t_1, \dots, x_n := t_n)$ où A est une sous-formule de Γ ou Δ et t_i sont des termes.

Th 25 : **Théorème d'interpolation.**
Soient A, B des formules telles que $\vdash A \to B$. Il existe une formule F telle que $\vdash A \to F$, $\vdash F \to B$ et $\mathcal{L}(F) \subset \mathcal{L}(A) \cap \mathcal{L}(B)$.

23 - Systèmes de Hilbert :

Def 26 : Un **système de Hilbert** est la donnée d'un ensemble $\mathcal{A}$ d'axiomes et d'un ensemble $\mathcal{R}$ de règles. Soit Γ un ensemble de formules.
. Une **Γ-dérivation** est une suite finie $A_1 \dots A_n$ de formules telles que, pour tout $i \leq n$
- $A_i \in \mathcal{A}$ ou $A_i \in \Gamma$
ou - A_i est la conclusion d'une règle de $\mathcal{R}$ dont les prémisses appartiennent à $\{A_1, \dots, A_{i-1}\}$
. Une formule est **Γ-dérivable** s'il existe une Γ-dérivation qui se termine par A.

Exple 27 : utilisant 2 axiomes et une règle :

$H_1 : A \to B \to A$
$H_2 : (A \to B \to C) \to (A \to B) \to (A \to C)$

$(R_\to)$ $\dfrac{A \quad A \to B}{B}$

$\vdash A \to A$. :

1. $A \to ((A \to A) \to A) \to ((A \to (A \to A)) \to (A \to A))$ H_2
2. $A \to ((A \to A) \to A)$ H_1
3. $(A \to (A \to A)) \to (A \to A)$ $(R_\to\ 1, 2)$
4. $A \to (A \to A)$ H_1
5. $A \to A$ $(R_\to\ 3, 4)$

Th 28 : Un système de Hilbert usuel est équivalent à la déduction naturelle.

III | Automatisation de preuve.

31 - Unification.

Def 29 : Une **substitution** σ est une fonction qui associe un terme à une variable. On note $u[\sigma]$ le terme obtenu en remplaçant dans u chaque variable x par $\sigma[x]$.

Def 30 : Deux termes u et v sont **unifiables** s'il existe une substitution σ telle que $u[\sigma] = v[\sigma]$. Dans ce cas, il existe un unificateur σ appelé **unificateur le plus général** tel que pour obtenir un unificateur quelconque, il suffit de composer σ avec une autre substitution.

Notations 31 : - résoudre $u \sim v$ c'est chercher σ / $u[\sigma] = v[\sigma]$. Les équations sont orientées.
- $E = E_1 \oplus E_2$ signifie $E = E_1 \cup E_2$ et E_1 et E_2 disjoints

Algo 32 : Soit E un ensemble d'équations, on définit par récurrence une suite (E_n, σ_n) : $E_0 = E$, $\sigma_0 = Id$

1 - Si $E_n = E' \oplus \{f(u_1 \dots u_p) \sim g(v_1, \dots, v_q)\}$:
- si $f = g$ on pose $E_{n+1} = E' \cup \{u_1 \sim v_1, \dots, u_p \sim v_p\}$, $\sigma_{n+1} = \sigma_n$
- sinon échec par CLASH

2 - Si $E_n = E' \oplus \{x = x\}$ on pose $E_{n+1} = E'$ et $\sigma_{n+1} = \sigma_n$

3 - Si $E_n = E' \oplus \{x \sim u\}$ ou $E' \oplus \{u \sim x\}$ avec $u \neq x$
- si la variable x n'est pas dans u, on pose $\sigma_{n+1} = [x := u] \circ \sigma_n$ et $E_{n+1} = E'[x := u]$
- sinon échec par occur_check.

4 - Si $E_n = \emptyset$ le programme s'arrête.

Exple 33 : • $u = f(z, x, y)$ et $v = f(f(y, y, 3), f(y, y, 3), a)$ sont unifiables.
• $u = f(x, x, y)$ et $v = f(f(y, y, 3), f(y, x, 3), a)$
• $u = f(x, x, y)$ et $v = f(g(y, y, 3), f(y, y, 3), a)$
ne le sont pas.

Prop 34 : L'algorithme termine toujours, soit par un échec soit avec $E_n = \emptyset$

Prop 35 : Si l'algo termine avec $E_n = \emptyset$, alors $\sigma_n = \text{mgu}(E)$. Sinon le système n'a pas d'unificateur.

Rmq 36 : Algo non déterministe et de complexité exponentielle.

32 - Méthode des tableaux.

Dans le calcul des séquents sans la coupure, on cherche à limiter les règles qui nécessitent de deviner quelque chose.

Règles : On enlève la coupure et les contractions. On remplace les règles $\exists x$ et $\forall l$ par $\dfrac{}{\Gamma, A \vdash A, \Delta}\, ax_0$ (A atomique)
• On contrôle le nombre de fois où on utilise les règles $\forall g$ et $\exists d$.

Méthode : 1 - On décore chaque quantificateur avec un entier
2 - On applique les règles jusqu'à obtenir un ensemble S de séquents n'ayant que des formules atomiques.
3 - On utilise un algo d'unification pour trouver une substitution σ tq pour tout séquent $\Gamma \vdash \Delta$ de S, $\Gamma[\sigma] \vdash \Delta[\sigma]$ soit une instance de la règle ax_0.

Th 37 : Si un séquent est prouvable la méthode des tableaux appliquée à ce séquent réussit.

Th 38 : Si la méthode appliquée à un séquent réussit et s'il ne contient que des formules closes, alors le séquent est prouvable.

33 - Résolution.

Def 39 : Un **littéral** est une formule atomique ou sa négation. Une **clause** est un ensemble fini de littéraux.

Méthode : Pour prouver $\Gamma \vdash F$, on met $\{\Gamma, \neg F\}$ en forme normale de Skolem, on enlève tous les quantificateurs puis on réduit sous forme FCN. On résout l'ensemble de clauses obtenu.

Th 40 : Pour $\Gamma \vdash F$ un séquent, $\Gamma \vdash F$ est prouvable ssi la résolution sur $\Gamma \vdash F$ renvoit la clause vide.

NOM :

Prénom :

N° - Date - Titre de la leçon : 918

Annexe 1 - Règles de la déduction naturelle.

axiome : $\dfrac{}{\Gamma, A \vdash A}\ ax$

affaiblissement : $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}\ aff.$

introduction de l'implication : $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i$ et

élimination de l'implication $\dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$

Conjonction : $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_i$

et $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_e^g$; $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e^d$

Disjonction : $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i^g$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_i^d$

et $\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_e$

Négation : $\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i$ | Absurdité classique $\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_c$

et $\dfrac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg_e$

Quantificateur universel $\dfrac{\Gamma \vdash A \quad x \notin VL(\Gamma)}{\Gamma \vdash \forall x A}\ \forall_i$

et $\dfrac{\Gamma \vdash \forall x A}{\Gamma \vdash A(x := t)}\ \forall_e$

Quantificateur existentiel : $\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A}\ \exists_i$

et $\dfrac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C \quad x \notin VL(\Gamma, C)}{\Gamma \vdash C}\ \exists_e$

Égalité : $\dfrac{}{\Gamma \vdash t = t}\ =_i$ et $\dfrac{\Gamma \vdash A(x := t] \quad \Gamma \vdash t = u}{\Gamma \vdash A(x := u]}\ =_e$

Annexe 2 : Règles du calcul des séquents.

Axiomes : $\dfrac{}{\bot \vdash}\ \bot_g$ $\dfrac{}{A \vdash A}\ ax$

Règles structurelles : $\dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ aff_g$ $\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ aff_d$

$\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ contr_g$ $\dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ contr_d$

Règles des connecteurs logiques : $\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_g$ $\dfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge_d$

$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee_g$ $\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee_d$

$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \to_g$ $\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\ \to_d$

$\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ \neg_g$ $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \neg_d$

Règles des quantificateurs : $\dfrac{\Gamma, A(x := t) \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ \forall_g$ $\dfrac{\Gamma \vdash A, \Delta \quad x \notin VL(\Gamma, \Delta)}{\Gamma \vdash \forall x A, \Delta}\ \forall_d$

$\dfrac{\Gamma, A \vdash \Delta \quad x \notin VL(\Gamma, \Delta)}{\Gamma, \exists x A \vdash \Delta}\ \exists_g$ $\dfrac{\Gamma \vdash A(x := t), \Delta}{\Gamma \vdash \exists x A, \Delta}\ \exists_d$

Règle de coupure : $\dfrac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ coupure$