M2 LMFI – Quantification du second-ordre et points fixes en logique

Second-order logic and arithmetics

Introduction to system F

1 Definition of second-order logic

Définition 1.1 (***Formulas of second-order logic***)

Let us assume given as countable set of first-order variables ($\mathcal{V}^1$)*, a first-order signature*($\mathcal{L}$) *and the associated set of terms* T *defined as usual:*

$$t, u ::= x \mid f(t_1, \ldots, t_n)$$

where f *is a function symbol of arity* n*. One also assumes that function symboles of arity* n *are in bijection with primitive recursive functions of* $\mathbb{N}^n \longrightarrow \mathbb{N}$ *(in particular, symbols* $\mathsf{0}$ *and* S *are available).*

One considers a countable set of second-order variables $(X, Y, Z, \cdots \in \mathcal{V}^2)$ *structured by arity* ($\mathcal{V}^2 = \cup_{i\in\omega}\mathcal{V}^2_i$) *and disjoint from* $\mathcal{L}$*. One defines the set of second-order formula by induction as follows:*

$$A, B, C ::= t = u \mid R(t_1, \ldots, t_n) \mid X(t_1, \ldots, t_n) \mid A \Rightarrow B \mid \forall x.A \mid \forall X.A.$$

with t, u *and the* t_i *being first-order terms,* R *is a n-ary relational symbol from* $\mathcal{L}$*and* $X \in \mathcal{V}^2_n$*. One shall also write* $(t_1, \ldots, t_n) \in X$ *in place of* $X(t_1, \ldots, t_n)$*.*

Quantifiers bind respectively first- and second-order variables.

Définition 1.2 (***Second-order substitution***)

One defines a substitution operation for second-order as follows:

If A *and* B *are second-order formulas,* X *a* n*-ary second-order variable and* $x_1, \ldots x_n$ *first-order variables, one writes* $A\{B/X(x_1, \ldots, x_n)\}$ *for the formula obtained by replacing, in* A*, every free occurrence of* $X(t_1, \ldots, t_n)$ *with* $B\{t_1/x_1, \ldots, t_n/x_n\}$*.*

Exemple 1.3

For instance, $\mathsf{0} \in X\{(\mathsf{S0} = x)/X(x)\} \triangleq (\mathsf{S0} = \mathsf{0})$.

$$A\{B/X(x_1 \dots x_n)\}$$

$$B$$

$$X(t_1, t_2) \Rightarrow X(t_2, t_1). \{B/X(x_1, x_2)\}$$

$$= B(t_1/x_1, t_2/x_2) \Rightarrow B(t_2/x_1, t_1/x_2).$$

Définition 1.4 (*Second-order natural deduction*)

Second-order natural deduction, NK^2*, is obtained by considering the usual classical natural deduction system for first-order logic,* NK*, over formulas of second-order logique, extended with the two following inference rules:*

$$\frac{A}{\forall X.A}\ (\forall^2 i)\quad (\star)$$

$$\frac{\forall X.A}{A\{B/X(x_1,\ldots,x_n)\}}\ (\forall^2 e(B))$$

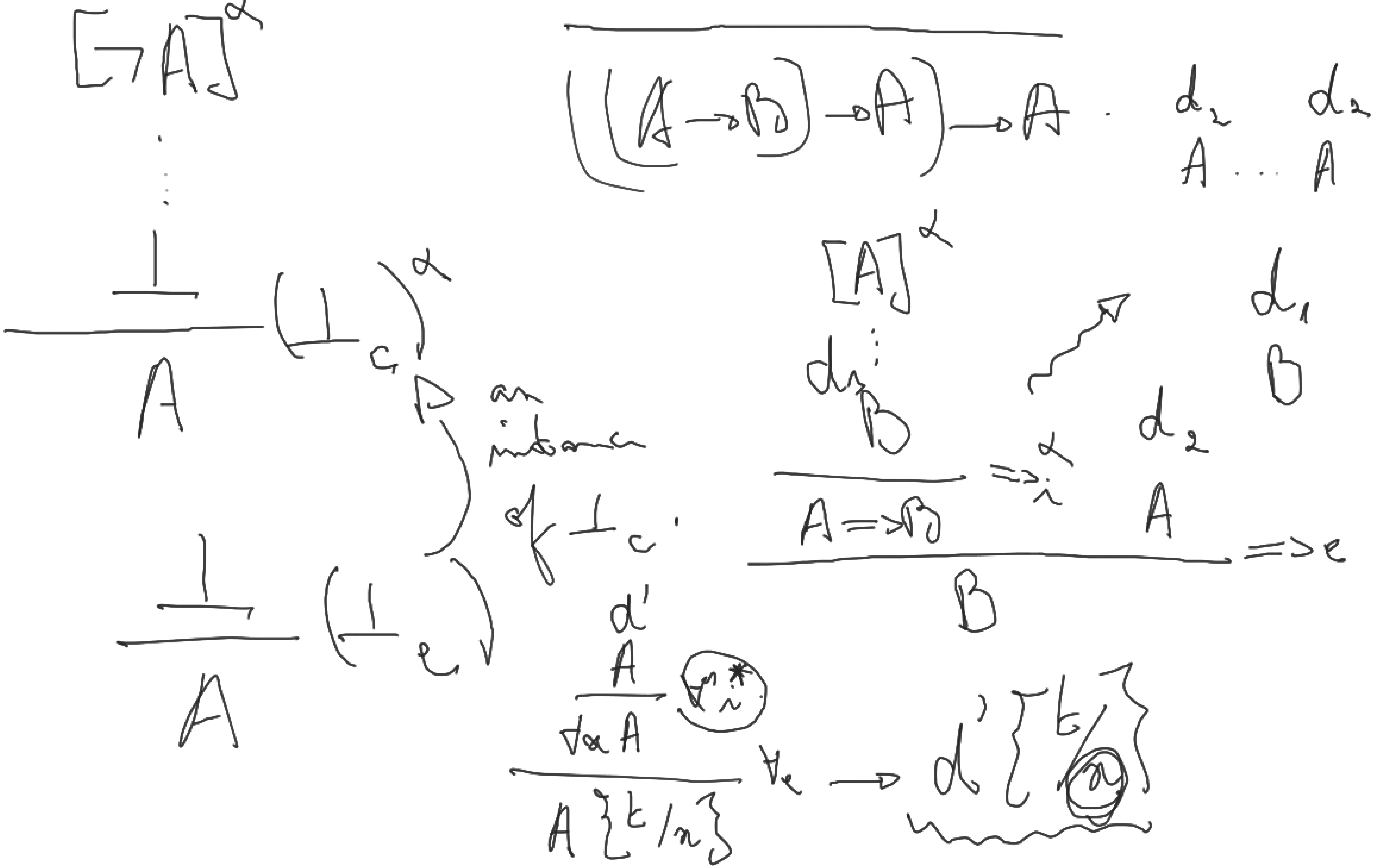
($\star$) *The inference rule $\forall^2 i$ can only be applied if X does not occur free in the non-discharged hypotheses of the deduction of conclusion A.*

Remarque 1.5

Note then it is significant to write explicitely **in the rule lable** *the formula B by which one instanciates the variable in the second-order quantifier elimination rule. We shall come back to this point later.*

Exemple 1.6

$$\cfrac{\cfrac{[X]^\alpha}{X \Rightarrow X}\ (\Rightarrow i)^\alpha}{\forall X.X \Rightarrow X}\ (\forall\ i)$$



[¬A]^α
⊥
A
(⊥_c)^α
⊥
A
(⊥_e)
an instance of ⊥_c
((A → B) → A) → A
d_2 d_2
A A
[A]^α
d_1
B
A ⇒ B
⇒_i^α
d_2
A
⇒e
B
d_1
B
d_2
d'
A
∀x A
∀_i
A{t/x}
∀_e
d'{t/x}

$$\frac{A}{\forall X.A}\ (\forall^2 i)\quad (\star)$$

$$\frac{\forall X.A}{A\{B/X(x_1,\ldots,x_n)\}}\ (\forall^2 e(B))$$

($\star$) *The inference rule* $\forall^2 i$ *can only be applied if* X *does not occur free in the non-discharged hypotheses of the deduction of conclusion* A.

Let d be a universal cut, that is a deduction of formula $A\{B/X\}$ of the form:

$$d : \dfrac{\dfrac{d' : A}{\forall X.A}\ (\forall^2 i)}{A\{B/X\}}\ (\forall^2 e)(B)$$

The reduct/contractum of this cut is the deduction:

~~$d'\{B/X\} : A\{B/X\}$~~

where $d'\{B/X\}$ represents deduction d' in which every occurrence of variable X has been replaced by formula B. The deduction so obtained is a valid deduction precisely because X does not occur free in the undischarged hypothese of d' and this also explains the need to make explicit the name of formula B in the deduction.)

Définition 1.7 (*Axioms of second-order arithmetics,* $\mathsf{HA}_2, \mathsf{PA}_2$)

One considers the formula $Int(x) \triangleq \forall X.0 \in X \Rightarrow (\forall y.y \in X \Rightarrow \mathsf{S}(y) \in X) \Rightarrow x \in X$.

The theory of second-order arithmetics (called HA_2 *or* PA_2 *depending on whether one considers intuitionistic of classical logic) is given by the following axioms:*

- $E_{\mathsf{Refl}} \triangleq \forall x.x = x$
- $E_{\mathsf{Leibniz}} \triangleq \forall x, y.x = y \Rightarrow \forall Z.(x \in Z \Rightarrow y \in Z)$
- $P_4 \triangleq \forall x.\mathsf{S}(x) \neq 0$ $\triangleq \forall x.\neg(S(x) = 0)$ $\triangleq \forall x.(S(x) = 0) \Rightarrow \bot \triangleq \forall x.((S(x) = 0) \Rightarrow \forall X.X)$
- $I \triangleq \forall x.Int(x)$
- *as well as, for every symbol of primitive recursive function, a universally closed formula expressing the definition of this function, this will be noted* E_{PrimRec}*, the primitive recursive axiom schema.*

0 S/1

X(0)

X(S(y))

S(y) ∈ X

Exemple 1.8

The following formulas are two examples of axioms in E_{PrimRec}*:*

- $\forall x.\mathsf{Pred}(\mathsf{S}(x)) = x$;
- $(\forall x.x + 0 = x) \wedge (\forall x.\forall y.x + \mathsf{S}(y) = \mathsf{S}(x + y))$.

$$\frac{\forall X.X}{X\{B/X\}}\ \forall_e(B) \qquad X\{B/X\} = B$$

Proposition 1.9

The following formulas which are axioms of first-order arithmetics, are now provable from the other axioms:

- $P_3 \triangleq \forall x.\forall y.\mathsf{S}(x) = \mathsf{S}(y) \Rightarrow x = y$;
- $E_{\mathsf{Sym}} \triangleq \forall x.\forall y.x = y \Rightarrow y = x$;
- $E_{\mathsf{Trans}} \triangleq \forall x.\forall y.\forall z.x = y \Rightarrow (y = z \Rightarrow x = z)$;
- $E^{u}_{\mathsf{Subst}} \triangleq \forall x.\forall y.x = y \Rightarrow u\{x/z\} = u\{y/z\}$, *for any term u.*

Démonstration : One proves that P_3 is provable in PA_2:

$$\dfrac{\dfrac{E_{\mathsf{Trans}} \quad \dfrac{E_{\mathsf{Sym}} \quad \dfrac{\forall z.\mathsf{Pred}(\mathsf{S}(z)) = z}{\mathsf{Pred}(\mathsf{S}(x)) = x}\,(\forall^1 e)}{x = \mathsf{Pred}(\mathsf{S}(x))}\,(\Rightarrow e) \quad \dfrac{E_{\mathsf{Trans}} \quad \dfrac{\forall z.\mathsf{Pred}(\mathsf{S}(z)) = z}{\mathsf{Pred}(\mathsf{S}(y)) = y}\,(\forall^1 e) \quad \dfrac{\dfrac{E^{\mathsf{Pred}(\mathsf{S}(z))}_{\mathsf{Subst}}}{\mathsf{S}(x) = \mathsf{S}(y) \Rightarrow \mathsf{Pred}(\mathsf{S}(x)) = \mathsf{Pred}(\mathsf{S}(y))}\,(\forall^1 e)^2 \quad [\mathsf{S}(x) = \mathsf{S}(y)]^{\alpha}}{\mathsf{Pred}(\mathsf{S}(x)) = \mathsf{Pred}(\mathsf{S}(y))}\,(\Rightarrow e)}{\mathsf{Pred}(\mathsf{S}(x)) = y}\,(\Rightarrow e)}{\dfrac{x = y}{\mathsf{S}(x) = \mathsf{S}(y) \Rightarrow x = y}\,(\Rightarrow i)^{\alpha}}\,(\Rightarrow e)^2$$

$$\dfrac{\mathsf{S}(x) = \mathsf{S}(y) \Rightarrow x = y}{\forall x.\forall y.\mathsf{S}(x) = \mathsf{S}(y) \Rightarrow x = y}\,(\forall^1 i)^2$$

The other axioms are left as exercises.

□

Proposition 1.10

In the same way, the following rule is derivable in PA_2*:*

$$\frac{t = u \quad A\{t/x\}}{A\{u/x\}}\ (=e)$$

Démonstration : Equality elimination is actually derivable in PA_2 (as well as its symmetric rule):

$$\dfrac{\dfrac{\dfrac{\dfrac{E_{\mathsf{Leibniz}}}{t = u \Rightarrow (\forall Z.Z(t) \Rightarrow Z(u))}\ (\forall^1 e)^2 \quad t = u}{\forall Z.Z(t) \Rightarrow Z(u)}\ (\Rightarrow e)}{A\{t/x\} \Rightarrow A\{u/x\}}\ (\forall^2 e) \qquad A\{t/x\}}{A\{u/x\}}\ (\Rightarrow e)$$

□

2 Definability of other logical connectives

Définition 2.1 (*Second-order encoding of logical connectives*)

One defines the following formulas:

- $\bot \triangleq \forall X.X$;
- $A \wedge B \triangleq \forall X.(A \Rightarrow (B \Rightarrow X)) \Rightarrow X$;
- $A \vee B \triangleq \forall X.(A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X$;
- $\exists X.A \triangleq \forall Y.(\forall X.A \Rightarrow Y) \Rightarrow Y$.
- $\exists x A \triangleq \forall Y (\forall x A \rightarrow Y) \Rightarrow Y$.

Démonstration :

- The elimination rule for the absurdity is definable:

$$\frac{\bot}{A}\ (\forall^2 e(A))$$

One thus has intuitionistic logic for free from minimal logic.

- $A \wedge B \triangleq \forall X.(A \Rightarrow (B \Rightarrow X)) \Rightarrow X;$
- $\ldots (B \Rightarrow X) \Rightarrow X;$

- Introduction and elimination rules for conjunctions are derivable:

$$\dfrac{\dfrac{d : A \wedge B}{(A \Rightarrow (B \Rightarrow A)) \Rightarrow A}\ (\forall^2 e(A) \qquad \dfrac{\dfrac{[A]^{\alpha}}{B \Rightarrow A}\ (\Rightarrow i)^{\beta}}{A \Rightarrow (B \Rightarrow A)}\ (\Rightarrow i)^{\alpha}}{A}\ (\Rightarrow e)$$

$$\dfrac{\dfrac{d : A \wedge B}{(A \Rightarrow (B \Rightarrow B)) \Rightarrow B}\ (\forall^2 e(B) \qquad \dfrac{\dfrac{[B]^{\beta}}{B \Rightarrow B}\ (\Rightarrow i)^{\beta}}{A \Rightarrow (B \Rightarrow B)}\ (\Rightarrow i)^{\alpha}}{B}\ (\Rightarrow e)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[A \Rightarrow (B \Rightarrow X)]^{\alpha} \quad d_A : A}{B \Rightarrow X}\ (\Rightarrow e) \qquad d_B : B}{X}\ (\Rightarrow e)}{(A \Rightarrow (B \Rightarrow X)) \Rightarrow X}\ (\Rightarrow i)^{\alpha}}{A \wedge B}\ (\forall^2 i)$$

- Introduction and elimination rules for disjunction are derivable:

$$
\dfrac{\dfrac{\dfrac{\dfrac{[A \Rightarrow X]^{\alpha} \quad d_A : A}{X}\;(\Rightarrow e)}{(B \Rightarrow X) \Rightarrow X}\;(\Rightarrow i)^{\beta}}{(A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X}\;(\Rightarrow i)^{\alpha}}{A \vee B}\;(\forall^2 i)
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{[B \Rightarrow X]^{\beta} \quad d_B : B}{X}\;(\Rightarrow e)}{(B \Rightarrow X) \Rightarrow X}\;(\Rightarrow i)^{\beta}}{(A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X}\;(\Rightarrow i)^{\alpha}}{A \vee B}\;(\forall^2 i)
$$

$$
\dfrac{\dfrac{\dfrac{d : A \vee B}{(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow C}\;(\forall^2 e(C)) \qquad \dfrac{\begin{matrix}[A]^{\alpha} \ldots [A]^{\alpha} \\ \vdots\; d_A \\ C\end{matrix}}{A \Rightarrow C}\;(\Rightarrow i)^{\alpha}}{(B \Rightarrow C) \Rightarrow C}\;(\Rightarrow e) \qquad \dfrac{\begin{matrix}[A]^{\beta} \ldots [A]^{\beta} \\ \vdots\; d_B \\ C\end{matrix}}{B \Rightarrow C}\;(\Rightarrow i)^{\beta}}{C}\;(\Rightarrow e)
$$

Introduction to system F

1 Definition of System F

Définition 1.1 (*Types of system* **F**)

Let us consider an infinte, countable set of type variables (or second-order type variables), $\mathcal{V}_{\mathsf{F}}$. *System* F *types are given by the grammar:*

$$T, U, V ::= X \mid U \to V \mid \forall X.T$$

$\forall X.T$ *binds* X *in* T, *so that types are considered with the expected notions of free and bound (type) variables, capture-free substitition of an F-type for a variable (written* $T\{U/X\}$*).*

Définition 1.2 (*Church-style System* **F**)

One considers, for each type T *of* F, *an infinite countable set of variables for this type,* $\mathcal{V}^T$.
Church-style System F *terms are the least set such that:*

- *For any variable* x *in* $\mathcal{V}^T$, x^T *is a term of type* T *(with free variables* $\{x\}$*);*
- *For any term* v *of type* V *and any variable* x *in* $\mathcal{V}^U$, $\lambda x^U.v$ *is a term of type* $U \to V$ *(with free variables* $fv(t) \setminus \{x\}$*);*
- *For any terms* t *and* u *of respective types* $U \to T$ *and* U, $(t)u$ *is a term of type* T *(with free variables* $fv(t) \cup fv(u)$*);*
- *For any type variable* X *and any term* t *of type* T, $\Lambda X.t$ *is a term of type* $\forall X.T$ **under the condition that, for any free variable libre** x **of** t, X **does not occur free in the type of** x *(with free variables* $fv(t)$*);*
- *For any term* t *of type* $\forall X.T$ *and any type* U *of* F, $(t)U$ *is a term of type* $T\{U/X\}$ *(with free variables* $fv(t)$*).*

Curry-style System F

As for the simply-typed case, Curry-style system F consists in the pure λ-calculus together with a typing relation given by a type system, inspired by second order natural deduction. That is simply the type system for simply-typed λ-calculus extended with the two following typing rules:

$$\frac{\Gamma \vdash t : T}{\Gamma \vdash t : \forall X.T}\ \forall i\quad (*)$$

$$\frac{\Gamma \vdash t : \forall X.T}{\Gamma \vdash t : T\{U/X\}}\ \forall e(U)$$

$(*)$ The inference rule $\forall i$ can only be applied if X does not occur free in the type of (the variables in) Γ.

The judgement that a λ-term t appear in conclusion of a typing derivation with type T under context Γ will be written $\Gamma \vdash_{\mathsf{F}} t : T$.

Définition 1.2 (*Church-style System* F)

One considers, for each type T of F*, an infinite countable set of variables for this type, $\mathcal{V}^{\mathcal{T}}$.*

Church-style System F *terms are the least set such that:*

- *For any variable x in $\mathcal{V}^{\mathcal{T}}$, x^T is a term of type T (with free variables $\{x\}$);*
- *For any term v of type V and any variable x in $\mathcal{V}^{\mathcal{U}}$, $\lambda x^U.v$ is a term of type $U \to V$ (with free variables $fv(t) \setminus \{x\}$);*
- *For any terms t and u of respective types $U \to T$ and U, $(t)u$ is a term of type T (with free variables $fv(t) \cup fv(u)$);*
- *For any type variable X and any term t of type T, $\Lambda X.t$ is a term of type $\forall X.T$* **under the condition that, for any free variable libre x of t, X does not occur free in the type of** *x (with free variables $fv(t)$);*
- *For any term t of type $\forall X.T$ and any type U of* F*, $(t)U$ is a term of type $T\{U/X\}$ (with free variables $fv(t)$).*

Proposition 1.3

If t is an F*-term of type T, x is a variable of type U and u is an* F*-term of type U, then $t\{u/x\}$ is an* F*-term of type T, having the free variables as $(fv(t) \setminus \{x\}) \cup fv(u)$.*

Proposition 1.4

If t is an F *term of type T and if X is a type variable that does not occur free in the free variables of t, then for any* F*-type U, $t\{U/X\}$ is an* F*-term of type $T\{U/X\}$, having the same free variables as t.*

The previous propositions ensure that the following definition is meaningful:

Définition 1.5 (*Dynamics of* F)

Church-style F*-terms are equipped with two reduction rules:*

$$\begin{array}{lll}(\lambda x.t)u & \longrightarrow_\beta & t\{u/x\} \\ (\Lambda X.t)U & \longrightarrow_\forall & t\{U/X\}\end{array}$$

The first rule is called β-reduction, as usual, while the second is called **universal reduction**.

Curry-style System F

As for the simply-typed case, Curry-style system F consists in the pure λ-calculus together with a typing relation given by a type system, inspired by second-order natural deduction. That is simply the type system for simply-typed λ-calculus exgtended with the two following typing rules:

$$\frac{\Gamma \vdash t : T}{\Gamma \vdash t : \forall X.T}\ \forall i \quad (\star)$$

$$\frac{\Gamma \vdash t : \forall X.T}{\Gamma \vdash t : T\{U/X\}}\ \forall e(U)$$

($\star$) The inference rule $\forall i$ can only be applied if X does not occur free in the type of (the variables in) Γ.

The judgement that a λ-term t appear in conclusion of a typing derivation with type T under context Γ will be written $\Gamma \vdash_{\mathsf{F}} t : T$.

Relations between the two presentations

Définition 1.6 (*forgetful map*)

One defines inductively a type-forgetting map from Church-style F*-terms to pure* λ*-terms:*

- $[x^T]^- = x$;
- $[\lambda x^T.\, t]^- = \lambda x.\, t$;
- $[(t)\, u]^- = ([t]^-)\, [u]^-$;
- $[\Lambda X.\, t]^- = [t]^-$;
- $[(t)\, T]^- = [t]^-$.

Proposition 1.7

Let $t : T$ *be a Church-style* F*-term with free variables libres among* $(x_i^{T_i})_{1 \le i \le n}$*. Then* $x_1 : T_1, \dots x_n : T_n \vdash_{\mathsf{F}} [t]^- : T$ *is derivable in (Curry-style) F.*

Proposition 1.8

A type derivation δ *for a judgment* $\Gamma \vdash_{\mathsf{F}} t : T$ *is isomorphic to a Church-style term* $u : T$ *the free variables of which are among the variables of* Γ *(and typed according to* Γ*. In addition,* $[u]^- = t$*.*

Lemme 1.9

Universal reduction is strongly normalizing in (Church-style) system F.

Reductions in Church-style and Curry-style system F can also be compared:

Proposition 1.10

1. *The type-erasure of a (Church-style) normal form is a normal form.*
2. *If t reduces to u with a universal-step, then $[t]^- = [u]^-$.*
3. *If t reduces to u with a β-step, then $[t]^-$ reduces to $[u]^-$ with a β-step.*
4. *The previous statements show that if $[t]^-$ is normal, reductions from t contain only universal steps.*
5. *If $[t]^-$ reduces in one step to u, then t reduces in at least one step to some v such that $[v]^- = u$.*

Finally, one can state the result we expected:

Théorème 1.11

Weak (resp. strong) normalization of Church-style system F *is equivalent to the weak (resp. strong) normalization of Curry-style system* F.

Finally, one can state the result we expected:

Théorème 1.11

Weak (resp. strong) normalization of Church-style system F *is equivalent to the weak (resp. strong) normalization of Curry-style system* F.

Démonstration : For weak normalization, the reasoning is direct and sumple: Assume F is weakly normalizing and let t be a λ-term which is typable in Curry-style F. We know that there exists u such that $[u]^- = t$ and that by hypothesis, u has a normal form v. The previous propositions ensure that $t \longrightarrow^\star [v]^-$ which is normal. In the other direction, if every λ-term which is typable in Curry-style F normalizes, let us consider some term t of Curry-style F. We know that $[t]^-$ normalizes to u and that there exists v in F such that $t \longrightarrow^\star v$ and $[v]^- = u$. Let us remark that v is not necessarily normal but that, by the previous propositions, all its reductions are universal, which we know to be strongly normalizing.

For strong normalization, the reasoning is slightly less immediate. Assume that there exists a term t typable in Curry-style system F from which an infinite reduction sequence can be drawn. We know that there exists some (Church-style) F-term u such that $[u]^- = t$ and the previous propositions ensure that from this term, an infinite reduction sequence can also be build. By contraposition, strong normalization of F ensures that every pure terme that is typable in (Curry-style) system F strongly normalizes. Assume now that there exists some F-term t having an infinite reduction ρ. By strong normalization of universal reduction, we know that ρ contains infinitely many β-reductions from which one conclude that $[t]^-$ also has an infinite reduction.

□