L1MD – feuille 4 **avril 2017**

*La marque * déclare une question comme délicate*

Définition d'une formule et raisonnement par équivalence

On définit une formule f de type énoncé par équivalence avec un énoncé P bien défini, *i.e.* obéissant à la syntaxe du langage en cours. On écrit la règle

$f \Leftrightarrow P \quad (\text{def } f)$

qui est un axiome. Voir plus loin les exemples $k \leq l$ pour les entiers, $E \subset F$ pour les ensembles.

On définit une formule f de type objet par une égalité avec une formule g bien définie dans le langage en cours. On écrit la règle

$f = g \quad (\text{def } f)$

qui est un axiome. Voir les exemples de la constante 1 et de la formule 121 pour les entiers

On définit une formule f de type objet implicitement par une propriété caractéristique $P(f)$, *i.e.* par la règle (qui s'ajoute aux règles en cours)

$\exists x,\ P(x)$
$Q(f) \Leftrightarrow \big(\forall x,\ P(x) \Rightarrow Q(x)\big) \quad (\text{déf. } f)$

pour tout énoncé $Q(x)$ dépendant d'une variable libre x ne faisant pas apparaître la formule f. Voir l'exemple de la constante $\emptyset$ et de la formule $\{x, P(x)\}$ pour les ensembles.

Plus généralement on définit les formules $f, g, \ldots$ vérifiant dans leur ensemble une propriété caractéristique $P(f, g, \ldots)$ par la règle

$\exists x, y, \ldots,\ P(x, y, , \ldots)$
$Q(f, g, \ldots) \Leftrightarrow \big(\forall x, y, \ldots,\ P(x, y, \ldots) \Rightarrow Q(x, y, \ldots)\big) \quad (\text{déf. } f)$

Voir l'exemple de $(\mathbb{N}, 0, S)$.

Le raisonnement par équivalence consiste à appliquer la macro-règle

$A \Leftrightarrow B$
B
$A \quad (\Leftrightarrow\vdash)$

Typiquement on écrit l'esquisse de preuve

$A \Leftrightarrow A_1$
$\ldots$
$A \Leftrightarrow A_n$
A_n
$A \quad (\Leftrightarrow\vdash)$

où on dispose d'une preuve de $A \Leftrightarrow A_1$, $A_1 \Leftrightarrow A_2$,... (par définition ou par application d'une règle élémentaire de calcul).

Les entiers

On introduit l'objet 0 (de type entier) et la formule Sn pour n un entier (le successeur de n, il correspond à $n + 1$). On ajoute aux règles de la logique du premier ordre les règles et axiomes spécifiques

$\neg(\exists n,\ 0 = Sn) \quad (\text{ax.}S) \qquad \forall m, n,\ Sm = Sn \Rightarrow m = n \quad (\text{ax.}S)$

$\forall n,\ n + 0 = n \quad (\text{ax.}+) \qquad \forall m, n,\ m + Sn = S(m + n) \quad (\text{ax.}+)$

$\forall n,\ n \times 0 = 0 \quad (\text{ax.}\times) \qquad \forall m, n,\ m \times Sn = (m \times n) + m \quad (\text{ax.}\times)$

$\forall n,\ n \uparrow 0 = S0 \quad (\text{ax.}\uparrow) \qquad \forall m, n,\ m \uparrow Sn = (m \uparrow n) \times m \quad (\text{ax.}\uparrow)$

$P(0)$
$\forall n,\ P(n) \Rightarrow P(Sn)$
$\forall n,\ P(n) \quad (\text{réc.})$

On définit la relation $\leq$ entre entiers par $m \leq n \Leftrightarrow (\exists p, n = m + p)$.

1. Calculer $SS0 + SSS0$ et $S0 \times SS0$ sous forme de mot $S \ldots S0$.

2. *Représentation décimale.* On définit les entiers $1, , 9$ par les axiomes $1 = S0, \ldots, 9 = SSSSSSSSS0$. On

définit la formule $a_n \dots a_1$, où les a_i sont des éléments de $\{0, \dots, 9\}$, par l'axiome $a_n \dots a_1 = a_1 + a_2 \times (S0) + \dots + a_n \times ((S0) \uparrow n - 1)$.

Calculer 22 sous forme d'un mot $S \dots S0$.

3. On définit récursivement $m \uparrow\uparrow n$ par $m \uparrow\uparrow 0 = S0$ et $m \uparrow\uparrow Sn = m \uparrow (m \uparrow\uparrow n)$. Calculer la représentation décimale de $2 \uparrow\uparrow 2$.

4. Ecrire une preuve formelle de $\forall n,\ (\neg n = 0) \Rightarrow \big(\exists m,\ n = Sm\big)$

5. Prouver $\forall n,\ 0 + n = n$. Prouver que l'opération $+$ est commutative et associative.

6. Prouver $\forall n,\ 0 \times n = 0, \quad \forall n,\ 1 \times n = n, \quad \times$ est commutative et associative.

Les ensembles

On introduit la relation $\in$ avec l'axiome

$\forall x, y,\ x = y \Leftrightarrow \big(\forall z,\ z \in x \Leftrightarrow z \in y\big)$

On introduit la formule (de type ensemble) $\{x, P(x)\}$, où $P(x)$ est un énoncé dont x est une variable libre, caractérisée par

$\forall y,\ y \in \{x, P(x)\} \Leftrightarrow P(y)$. La variable x est liée par la formule $\{x, P(x)\}$.

On ajoute les axiomes d'existence d'objets de la forme $\{x, P(x)\}$ de Zermelo-Fraenkel qui garantissent l'existence des formules $\emptyset$, $\{x, y\}$, $\mathcal{P}(x)$, $\cup x$, $\{x,\ x \in y \text{ et } P(x)\}$.

On limite la portée d'un quantificateur aux éléments d'un ensemble E en écrivant l'énoncé $\forall x \in E,\ P(x)$ (respectivement $\exists x \in E,\ P(x)$) défini comme étant équivalent à $\forall x,\ x \in E \Rightarrow P(x)$ (respectivement $\exists x,\ x \in E$ et $P(x)$).

7. Donner une preuve formelle que l'existence de $\{x, \neg(x \in x)\}$ (c'est à dire d'un objet y qui vérifie la propriété caractéristique de $\{x, \neg x \in x\}$) aboutit à une contradiction.

8. Rappeler la définition (vue en cours) des formules $x \subset y$, $\emptyset$, $\{a, b\}$, $\{a_1, \dots, a_n\}$, $\mathcal{P}(x)$, $\cup x$, $x \cup y$, $x \cap y$, $x \setminus y$.

9. Montrer formellement qu'on a $\forall x,\ \emptyset \subset x$.

10. Donner la liste des éléments de $\mathcal{P}(\emptyset))$, $\mathcal{P}(\mathcal{P}(\emptyset))$, $\mathcal{P}(\{1, 2, 3\})$, $\cup\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\emptyset))\big)$

11. On définit la formule (x, y) par $(x, y) = \{\{x, x\}, \{x, y\}\}$. Prouver informellement qu'on a

$$\forall a, b, c, d,\ (a, b) = (c, d) \Leftrightarrow (a = c \text{ et } b = d)$$

12. *Relation entre éléments* — Soit f une relation entre les éléments d'un ensemble E et ceux d'un ensemble F, *i.e.* un énoncé $P_f(x, y)$ dépendant des variables libres x et y données dans cet ordre tel que $P_f(x, y)$ est faux si x n'est pas un élément de E ou y n'est pas un élément de F.

Donner la définition du graphe de f en terme de couples (x, y).

Donner la définition de "f est une relation fonctionnelle", de la formule $f(x)$ lorsque f est fonctionnelle, de "f est une application injective", de "f est une application surjective", "f est bijective".

Donner la définition de "f est une relation d'ordre", de "f est une relation d'ordre totale", de "f est une relation d'équivalence".

13. *(Partiel mars 2016)* Soient E, F deux ensembles, $f : E \to F$ une application et A un sous-ensemble de E. Donner une preuve informelle de l'énoncé $A \subset f^{-1}(f(A))$ en raisonnant par équivalence et en utilisant les définitions :

$\forall x,\ x \in f^{-1}(B) \Leftrightarrow x \in E \,\text{et}\, f(x) \in B \quad$ (pour B une partie de F),

$\forall y,\ y \in f(A) \Leftrightarrow \exists x, x \in A \,\text{et}\, f(x) = y \quad$ (pour A une partie de E).

Pouvez vous prouver l'égalité $A = f^{-1}(f(A))$?

Transformer la preuve informelle en preuve formelle.

14. Soit E un ensemble. A une partie A de E on associe l'application $\chi_A : E \to \{0,1\}$, $x \mapsto 1$ si $x \in A$, $x \mapsto 0$ si $x \notin A$. (χ_A est souvent notée 1_A en probabilités). Montrer que l'application $\mathcal{P}(E) \to \{0,1\}^E$, $A \mapsto \chi_A$ est une bijection en exhibant l'application réciproque.

15. On veut montrer qu'un ensemble n'est jamais en bijection avec l'ensemble de ses parties. Transformer le scénario de preuve ci-dessous en preuve formelle :

"Supposons l'existence d'une bijection φ entre un ensemble E et l'ensemble de ses parties. Les éléments de E n'appartenant pas à leur image par φ forment une partie de E, image par φ d'un élement e de E. On observe que l'énoncé $e \in \varphi(e)$ est équivalent à sa négation ce qui conduit à une contradiction."

Les entiers dans la théorie des ensembles

On propose un modèle ensembliste $\mathbb{N}$ des entiers en posant $0 = \emptyset$ (déf.), $\forall x$, $Sx = x \cup \{x\}$ (déf.) et en posant comme axiome l'existence d'un plus petit ensemble $\mathbb{N}$ contenant 0 et stable par S.

16. Formaliser $\mathbb{N}$ est le plus petit ensemble contenant 0 et stable par S.

*****Montrer que l'axiome (ax.S) et la règle (réc.) sont satisfaits lorsqu'on restreint la portée des quantificateurs aux éléments de $\mathbb{N}$.

****** *Définition par récurrence* — Soient E un ensemble, $e \in E$ et $\varphi : \mathbb{N} \times E \to E$ une aplpication. Montrer qu'il existe une application $f : \mathbb{N} \to E$ et une seule vérifiant

$$f(0) = e \quad \text{et} \quad \forall n \in \mathbb{N},\ f(Sn) = \varphi(n, f(n))$$

En déduire que les axiomes pour $+, \times, \uparrow$ sont satisfaits par les éléments de $\mathbb{N}$.

17. On veut prouver (informellement) l'énoncé suivant sur les sous-ensembles de $\mathbb{N}$:

$$(E) \quad \forall A : \mathcal{P}(\mathbb{N}),\ A \neq \emptyset \Rightarrow A \text{ admet un plus petit élement}$$

a. Formaliser "A admet un plus petit élement"

b. Comme pour beaucoup d'énoncés en rapport avec $\mathbb{N}$ on cherche à prouver (E) par récurrence. On cherche donc un énoncé $P(n)$ tel qu'on sache prouver les trois énoncés

$\big(\forall n : \mathbb{N},\ P(n)\big) \Rightarrow (E)$
$P(0)$
$\forall n : \mathbb{N}$, P(n)$\Rightarrow P(n+1)$

Essayer les candidats suivants pour $P(n)$ ($\#A$ désigne le cardinal de A) :

1. $\forall A : \mathcal{P}(\mathbb{N}),\ \big(\exists k : \mathbb{N},\ k \leq n \text{ et } k \in A\big) \Rightarrow A$ admet un plus petit élement
2. $\forall A : \mathcal{P}(\mathbb{N}),\ \#A = n \Rightarrow A$ admet un plus petit élement
3. $\forall A : \mathcal{P}(\mathbb{N}),\ n \in A \Rightarrow A$ admet un plus petit élement

18. *(Session 2, juin 2016)* Soient $n \geq p > 0$ deux entiers et $a_1, \ldots, a_p$ p-élements distincts de l'ensemble $\{1, \ldots, n\}$. On note $(a_1\ a_2\ \ldots\ a_p)$ la bijection de $\{1, \ldots, n\}$ dans lui même définie par $a_1 \mapsto a_2$, $a_2 \mapsto a_3, \ldots$, $a_p \mapsto a_1$ et $k \mapsto k$ si $k \notin \{a_1, \ldots, a_p\}$. On dit qu'une telle bijection est un cycle de longueur p.

a. On fixe $n = p = 4$. Quelle est l'image de 3 par le cycle (3 4 1 2) ?

Quelle est l'image de 3 par le cycle (4 1 2 3) ?

Conbien y a t-il de cycles de longueur 4 parmi les bijections de $\{1, 2, 3, 4\}$?

b. On fixe $n = 7$. On considère la bijection σ obtenue en composant deux cycles de $\{1, \ldots, 7\}$:

$$\sigma = (2\ 5\ 1\ 4) \circ (7\ 2\ 4\ 3)$$

Quelle est l'image de 4 par σ ? Quelle est l'orbite de 4 sous l'action de σ ? La bijection σ est elle un cycle ?