Première partie

L'induction

Chapitre 1

Concepts mathématiques de base

1.1 Ensembles

Nous introduisons ici les notions et notations de base portant sur les ensembles.

Dans le tableau suivant, A, B désignent des sous-ensembles d'un ensemble E, e un élément de E et n un entier strictement positif.

Notation	signification
$e \in A$	e appartient à A
$A \subseteq B$	A est inclus dans B : tout élément de A est un élément de B
$\varnothing$	ensemble vide : il est inclus dans tous les ensembles
$A \cup B$	union de A et B : l'ensemble des éléments qui appartiennent à A ou a B
$A \cap B$	intersection de A et B : l'ensemble des éléments qui appartiennent à A et a B
$A \times B$	produit de A et B : $\{(a, b) \mid a \in A \text{ et } b \in B\}$
A^n	produit itéré de A : $\{(a_1, \ldots, a_n) \mid a_1, \ldots a_n \in A\}$
A^0	produit nul de A : $\{()\}$ ce n'est pas l'ensemble vide !
$A - B$	ensemble des éléments qui sont A mais pas dans B
$\mathcal{P}(A)$	ensemble des parties de A : $\{X \mid X \subseteq A\}$

Exemple 1.1 (Les mots)**.** Etant donné un ensemble fini A, un mot sur A est soit le mot vide noté ε, soit une suite $a_1 \ldots a_n$ d'éléments de A. L'ensemble A^* est l'ensemble des mots sur A. Un *langage* sur A est un ensemble de mots. Ainsi, l'ensemble des langages sur A est égal à $\mathcal{P}(A^*)$.

Important : L'équivalence suivante est fréquemment utilisée pour montrer que deux ensembles sont égaux :

$$A = B \text{ ssi } A \subseteq B \text{ et } B \subseteq A.$$

L'inclusion se prouvera en utilisant l'équivalence suivante :

$$A \subseteq B \text{ ssi pour tout élément } e, \text{ si } e \in A \text{ alors } e \in B.$$

Proposition 1.2. *Soient A, B et C trois parties d'un ensemble E :*

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
3. $E - (A \cap B) = (E - A) \cup (E - B)$,
4. $E - (A \cup B) = (E - A) \cap (E - B)$.

Exemple 1.3. Soient $A = \{1, 2, 3\}$ et $B = \{0, 1\}$. On a :
$A \cap B = \{1\}$,
$A \cup B = \{0, 1, 2, 3\}$,
$A \times B = \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}$,
$A - B = \{2, 3\}$, $B - A = \{0\}$.

Proposition 1.4. *Soient A un ensemble de cardinal n (c'est-à-dire que A contient exactement n éléments), B un ensemble de cardinal m et k un entier naturel.*
$\#(A \times B) = n \times m$, $\#(A^k) = n^k$ *et* $\#(\mathcal{P}(A)) = 2^n$.

1.2 Fonctions

Etant donné un ensemble E, et n un entier positif, une fonction n-aire (ou d'arité n) sur E est une fonction de E^n dans E. Une fonction n'est pas une forcément une application : elle peut être non définie pour certains éléments de E^n, dans ce cas on dira que c'est une fonction partielle.

Exemple 1.5.

1. $E = \{1, 2, 3\}$ et f est la fonction binaire (d'arité 2) définie pour tout couple $(a, b) \in E^2$ par :
   — $f(a, b) = 1$ si $a = 1$ et $b = 2$,
   — $f(a, b) = 2$ si $a = 2$ et $b = 3$,
   — $f(a, b) = 3$ si $a = 3$ et $b = 1$,
   — $f(a, b)$ est indéfinie sinon (i.e., pour les couples $(1, 1), (2, 2), (3, 3)(3, 2), (2, 1), (1, 3)$).
2. $E = \mathbb{N}$ et f est la fonction d'arité 1 définie pour tout $n \in \mathbb{N}$ par $f(n) = n + 1$.

Remarque 1.6. En particulier, observez que les fonctions d'arité 0, $f : D^0 \to D$ sont en bijection avec les éléments $d \in D$ (via l'évaluation $f() = d \in D$). Nous allons donc identifier une fonction d'arité 0 à une constante, c'est-à-dire à un élément $d \in D$.

1.3 Relations

Etant donné un ensemble E, et $n \geq 0$ un entier. Une relation n-aire (ou d'arité n) sur E est un sous-ensemble de E^n.

Exemple 1.7.

1. $E = \{1, 2, 3\}$ et R est la relation binaire (d'arité 2) définie par $R = \{(1, 1), (2, 2), (3, 3)\}$.
2. $E = \mathbb{N}$ et S est la relation d'arité 2 définie par $S = \{(n, n + 1) \mid n \in \mathbb{N}\}$.
3. $E = \{1, 2, 3\}$ et R est la relation unaire (d'arité 1) définie par $R = \{1, 2\}$.

Attention aux relations définies sur des tuples ! Par exemple, la relation $R = \{(1, 1), (2, 2), (3, 3)\}$ est d'arité 2 sur $\mathbb{N}$, mais d'arité 1 sur $\mathbb{N}^2$.

Notation Si R est une relation d'arité n, on note $R(a_1, \ldots, a_n)$ ssi $(a_1, \ldots, a_n) \in R$.

1.3.1 Propriétés des relation binaires

Une relation binaire R sur un ensemble E est dite :
— *reflexive* ssi
$$\text{pour tout } x \in E,\ R(x, x)\,;$$
— *symétrique* ssi
$$\text{pour tout } x, y \in E, \text{ si } R(x, y) \text{ alors } R(y, x)\,;$$
— *antisymétrique* ssi
$$\text{pour tout } x, y \in E, \text{ si } R(x, y) \text{ et } R(y, x) \text{ alors } x = y\,;$$
— *transitive* ssi
$$\text{pour tout } x, y, z \in E, \text{ si } R(x, y) \text{ et } R(y, z) \text{ alors } R(x, z).$$

Ces propriétés permettent de caractériser les deux plus importants types de relations.
Une relation binaire R est une
— *relation d'équivalence* ssi elle est reflexive, symétrique et transitive.
— *relation d'ordre* ssi elle est réflexive, antisymétrique et transitive.
On peut facilement vérifier que la relation d'égalité ($=$) sur les entiers est une relation d'équivalence, et que la relation $\leq$ sur les entiers est une relation d'ordre.

Exemple 1.8. Voici des exemples de relation sur l'ensemble A^* des mots un alphabet A :
La relation $\equiv$ définie par $u \equiv v$ ssi u et v sont de même longueur est une relation d'équivalence.
La relation $u \leq_{pref} v$ ssi u prefixe de v est une relation d'ordre.

1.3.2 Relations fonctionnelles

Terminons par remarquer qu'une fonction est une relation particulière : une fonction f d'arité n sur un ensemble E peut se représenter par une relation R_f d'arité $n+1$ sur E définie par $R_f = \{(x_1, \ldots, x_n, f(x_1, \ldots, x_n) \mid (x_1, \ldots, x_n) \in E^n\}$.
Une relation R d'arité $n+1$ sera donc dite *fonctionnelle* si :

$$\text{pour tout } (x_1, \ldots, x_n) \in E^n, \text{ il existe au plus un } y \in E \text{ tel que } (x_1, \ldots, x_n, y) \in R.$$

Elle sera dite fonctionnelle totale (c'est à dire qu'elle représente une fonction totale) si :

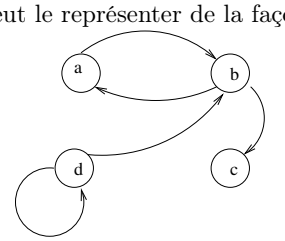
$$\text{pour tout } (x_1, \ldots, x_n) \in E^n, \text{ il existe un et un seul } y \in E \text{ tel que } (x_1, \ldots, x_n, y) \in R.$$

Exemple 1.9. Soit $E = \{0, 1, 2\}$, la relation $R = \{(0, 0), (1, 0), (2, 0)\}$ est une relation fonctionnelle décrivant la fonction constante $0 \mapsto 0, 1 \mapsto 0, 2 \mapsto 0$.

1.4 Graphes

Un graphe est la donnée d'une paire $G = (V, E)$ telle que
— V est un ensemble d'éléments appelés *sommets* ou *noeuds* (vertices en anglais)
— $E \subseteq V \times V$ est l'ensemble des *arcs* (edges en anglais)

Exemple 1.10. La structure $G = (\{a, b, c, d\}, \{(a, b), (b, a), (b, c), (d, b), (d, d)\})$ est un graphe. On peut le représenter de la façon suivante :



Un graphe est donc un ensemble muni d'une relation binaire.

1.4.1 Une sous-classe : les graphes orientés

Par défaut, les graphes sont orienté, cela signifie qu'avoir un arc entre a et b n'implique pas d'avoir un arc entre b et a. Cela s'explicite graphiquement comme dans le schéma ci-dessus, en représentant les arcs par des flèches.

Les *graphes non orientés* sont les graphes $G = (V, E)$ pour lesquels la relation E est symétrique, cela signifie que si on peut aller d'un sommet a à un sommet b du graphe, alors on peut aussi aller du sommet b au sommet a. Les arcs sont alors représentés par des traits et non par des flèches.

1.5 Conclusion : tout est relation

Vous pouvez noter en conclusion de ce court chapitre, que tous les objets couramment manipulés en informatique : mots, fonctions, graphes, arbres, ... peuvent toujours être vus comme des relations.

Chapitre 2

Définition inductives - Inductions

La représentation des objets mathématiques est fondamentale, puisque c'est selon leur représentations que les objets sont étudiés. Cela est d'autant plus important en informatique, puisque les objets, même si ils sont potentiellement en nombre infini doivent être représentés de façon finie.

Un type de représentation très utilisé est la définition inductive, qui permet une représentation finie d'objets en exploitant une notion d'ordre (partiel) inhérente à ces objets.

Prenons un exemple simple : si je veux parler des entiers naturels, je peux les énumérer un par un pour les décrire 0,1,2,3,4, ... , mais j'en ai pour un petit moment. Je peux aussi utiliser les faits suivants :

1. cet ensemble peut-être muni d'un ordre ;
2. il possède un élément minimal pour cet ordre ;
3. étant donné un entier n, je sais calculer de façon simple l'élément suivant (toujours pour l'ordre choisi) : il suffit d'ajouter 1 à n.

Je suis donc capable de donner une définition inductive de ce qu'est un entier : c'est soit 0, soit un entier auquel j'ajoute 1. En utilisant cette définition, je suis certaine de les énumérer tous dans l'ordre naturel sur les entiers.

Cette façon de décrire les entiers donne un outils très puissant pour prouver des propriétés sur les entiers : la preuve par récurrence. Pour prouver une propriété portant sur les entiers, il suffit de la prouver pour 0, puis de prouver que si elle est vraie entier n, alors elle l'est aussi pour l'entier $n+1$.

Pour vous faire une image mentale de la preuve par récurrence, imaginez une série de dominos alignés. Vous voulez être sûr que tous les dominos tombent. Pour cela il suffit de vous assurer que :

— (Base) le premier domino tombe ;

— (Induction) si un domino tombe, alors le suivant tombe aussi.

Nous présentons ici ces concepts, puis les plaçons dans le cadre plus général de la définition inductive.

2.1 Raisonnement par récurrence sur $\mathbb{N}$

Le raisonnement par récurrence un cas particulier de l'induction structurelle que nous verrons plus loin. C'est une notion que vous maitrisez normalement tous, mais sur laquelle il est certainement utile de revenir.

Théorème 2.1. *Soit $P(n)$ un prédicat (une propriété) dépendant de l'entier n. Considérons les deux conditions suivantes.*

— *(Base) $P(0)$ est vrai ;*

— *(Induction) pour tout entier n : si $P(n)$ est vrai alors $P(n+1)$ est vrai.*

Si (Base) et (Induction) sont vérifiées, alors $P(n)$ est vrai pour tout entier n.

Démonstration. Le raisonnement se fait par l'absurde. Considérons $X = \{k \in \mathbb{N} \mid P(k) \text{ est faux }\}$. Si X est non vide, il admet au moins un élément minimal n_0. D'après la condition (Base), $n_0 \neq 0$,

et donc $n_0 - 1$ est un entier, et $P(n_0 - 1)$ est vrai par définition de X et n_0. On obtient une contradiction avec la propriété (Induction) appliquée à l'entier $n = n_0 - 1$. □

Notez que la preuve repose uniquement sur le fait que $(\mathbb{N}, \leq)$ est un ordre bien fondé : tout sous-ensemble de $\mathbb{N}$ admet un élément minimal. Le principe de récurrence peut donc être généralisé à tout ensemble muni d'un ordre bien fondé.

Bien entendu, il est possible de modifier un peu le schéma de récurrence, pour prouver qu'une propriété est vraie pour tout $n \geq k$, pour k fixé. Il suffit de prouver les deux conditions suivantes :

— (Base) $P(k)$ est vrai ;

— (Induction) si $P(n)$ est vrai alors $P(n+1)$ est vrai, pour tout entier $n \geq k$.

Exemple 2.2. Soit $S_n = \sum_{i=0}^{n} i$, on prouve par récurrence que pour tout $n \geq 0$, $S_n = \frac{n(n+1)}{2}$. On prouve donc pour tout $n \geq 0$, la propriété $P(n)$ suivante :

$$P(n) := S_n = \frac{n(n+1)}{2}.$$

— (Base) $S_0 = 0 = \frac{0 \times 1}{2}$, donc $P(0)$ est vrai ;

— (Induction) Supposons que $P(n)$ est vrai. On a alors

$$S_{n+1} = \sum_{i=1}^{n+1} i = S_n + (n+1)$$

Puisque $P(n)$ est vrai, on a donc

$$S_{n+1} = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

$P(n+1)$ est donc vrai.

Dans certains cas, une simple récurrence n'est pas suffisante et on a alors recours au second principe de récurrence :

Théorème 2.3. *Soit $P(n)$ un prédicat (une propriété) dépendant de l'entier n. Considérons les deux conditions suivantes.*

— *(Base) $P(0)$ est vrai ;*

— *(Induction) pour tout entier n : si $P(i)$ est vrai pour tout $0 \leq i \leq n$, alors $P(n+1)$ est vrai.*

Si (Base) et (Induction) sont vérifiées, alors $P(n)$ est vrai pour tout entier n.

2.2 Définitions inductives

Les définitions inductives servent à décrire des ensembles. Supposons par exemple que nous cherchions à définir l'ensemble des nombres pairs. Il y a deux approches courantes.

La première consiste à décrire P par une propriété caractérisant les nombres pairs

$$P = \{n \mid \exists k \in \mathbb{N}, n = 2 \times k\}$$

(définition non inductive : on utilise en fait ici une formule de logique).

La seconde consiste à donner une façon de construire cet ensemble, en le faisant grossir itérativement :

P est le **plus petit ensemble** qui contient 0 et tel que si n est dans P alors $n + 2$ est dans P.

Notez la condition *le plus petit ensemble*. Sans cette précision la définition n'est plus valable car P peut alors être n'importe quel ensemble d'entier contenant tous les entiers pairs.

La définition inductive de P est donc la donnée de 2 objets :

— l'élément de base 0, à partir duquel on va pouvoir construire tous les autres

— la fonction de construction d'un entier pair à partir d'un entier pair plus petit : $r : n \mapsto n+2$.
Cette fonction est appelée une règle d'induction.

De manière générale, une définition inductive est toujours de cette forme : c'est la donnée d'un ensemble de base et de règles d'induction, comme formalisé ci-dessous :

Définition 2.4 (Définition inductive)**.** Soit E un ensemble. Une définition inductive d'une partie de E est une paire (B, R) telle que :
— $B \subseteq E$ est un ensemble non vide , appelé *ensemble de base* (ou d'*axiomes*) ;
— R est un ensemble de fonctions de E appelées *règles d'induction*. Une règle peut être partielle et d'arité quelconque.

Exemple 2.5. Continuons l'exemple de la définition des nombres pairs. La définition inductive est (B, R) où :
— $B = \{0\}$,
— $R = \{n \mapsto n + 2\}$.

Une définition inductive (B, R) sert à définir un ensemble X : c'est le plus petit ensemble qui contient les éléments de base et qui est *clos* par l'application des règles de R : si on prend des éléments de X et qu'on leur applique une règle de r, on obtient un élément de X.

Le théorème suivant montre que ce plus petit ensemble existe bien, et permet donc de définir clairement ce qu'est un ensemble défini inductivement.

Théorème 2.6 (Théorème du point fixe)**.** *Etant donnée une définition inductive (B, R) sur un ensemble E. Il existe un plus petit ensemble $X \subseteq E$ qui vérifie les propriétés suivantes :*
— *(Base) $B \subseteq X$;*
— *(Induction) si $x_1, \ldots, x_n \in X$ alors $r(x_1, \ldots, x_n) \in X$,*
pour toute règle $r \in R$ d'arité n, et tous éléments $x_1, \ldots, x_n$.

Démonstration. Clairement, l'ensemble de départ E vérifie (Base) et (Induction). Donc, soit $\mathcal{F}$ l'ensemble des parties de E vérifiant (Base) et (Induction), cet ensemble non vide puisqu'il contient E.

Soit X l'intersection de tous les éléments de $\mathcal{F}$:

$$X = \bigcap_{Y \in \mathcal{F}} Y.$$

Vérifions que X satisfait bien lui aussi les propriétés (Base) et (Induction).
— Puisque pour tout $Y \in \mathcal{F}$, $B \subseteq Y$, on a bien $B \subseteq X$ (Base).
— Considérons une règle $r \in R$ d'arité n, et $x_1, \ldots, x_n \in X$. Par définition de X, on a aussi $x_1, \ldots, x_n \in Y$ pour tout $Y \in \mathcal{F}$ et donc par définition de $\mathcal{F}$, $r(x_1, \ldots, x_n) \in Y$ pour tout $Y \in \mathcal{F}$. Mais alors, on a aussi $r(x_1, \ldots, x_n) \in X$ (Induction)

Nous avons donc prouvé que $X \in \mathcal{F}$ et par construction, c'est le plus petit élément de $\mathcal{F}$. □

2.2.1 Notations des définitions inductives

Les définitions inductives apparaissent très souvent en informatique, et il existe différentes manières de les représenter de façon concise. Nous en présentons ici quelques unes.

2.2.1.1 Notation standard

On note souvent une définition inductive (B, R) sous la forme
— (Base) $b \in X$, pour tout $b \in B$
— (Induction) si $x_1, \ldots x_n \in X$ alors $r(x_1, \ldots, x_n) \in X$
avec une telle ligne pour chaque règle $r \in R$.

Exemple 2.7. La définition inductive de l'ensemble P des entiers pairs se note :
— (Base) $0 \in P$

— (Induction) si $x \in P$ alors $x + 2 \in P$

Exemple 2.8. Soit $\Sigma = \{(,)\}$ l'alphabet constitué de la parenthèse ouvrante et de la parenthèse fermante. L'ensemble $D \subseteq \Sigma^*$ des mots bien parenthésés (appelé langage de Dyck) est défini inductivement par :
— (Base) $\varepsilon \in D$;
— (Induction) si $u \in D$ alors $(u) \in D$;
— (Induction) si $u, v \in D$ alors $uv \in D$.

2.2.1.2 Notation sous forme de règles

Certains préfèrent noter une définition inductive (B, R) sous forme de règles d'inférence : pour chaque $b \in B$ et chaque $r \in R$ d'arité n :

$$\frac{}{b \in X} \qquad \frac{x_1 \in X \qquad \dots \qquad x_n \in X}{r(x_1, \dots, x_n) \in X}$$

On pourra aussi écrire plus simplement pour chaque $b \in B$ et chaque $r \in R$ d'arité n :

$$\frac{}{b} \qquad \frac{x_1 \qquad \dots \qquad x_n}{r(x_1, \dots, x_n)}$$

Exemple 2.9. Avec cette notation, l'ensemble des entiers pairs est l'ensemble défini inductivement par

$$\frac{}{0} \qquad \frac{n}{n+2}$$

Exemple 2.10. Avec cette notation, le langage de Dyck est l'ensemble défini inductivement par

$$\frac{}{\varepsilon} \qquad \frac{u}{(u)} \qquad \frac{u \qquad v}{uv}$$

2.3 Quelques définitions inductives

2.3.1 Expression arithmétiques

On peut définir de façon inductive les expressions arithmétiques bien formées (mais pas forcément parenthésées) sur l'alphabet

$$\Sigma_{exp} = \{0, 1, \dots, 9, +, -, \times, /, (,)\}.$$

Commençons par définir ce qu'est un nombre écrit en base 10. A priori on écrit un entier en base 10 sans débuter par un 0 (sauf pour 0). Par exemple 000192 n'est pas autorisé. Par contre 192 est bien une écriture valide. On obtient la définition inductive suivante de l'ensemble B_{10} des nombres écrits en base 10 :
— (Base) $\{0, 1, \dots, 9\} \subseteq B_{10}$;
— (Induction) pour tout $a \in \{, 1, \dots, 9\}$, si $u \in B_{10}$ ne commence pas par 0, alors $ua \in B_{10}$;
On peut alors définir l'ensemble *Arith* des expressions arithmétiques de la façon suivante :

$$\frac{}{u}\ u \in B_{10} \qquad \frac{u \qquad v}{u+v} \qquad \frac{u \qquad v}{u-v} \qquad \frac{u \qquad v}{u \times v} \qquad \frac{u \qquad v}{u/v} \qquad \frac{u}{(u)}$$

Ainsi, on a $(1 + 2 \times 4 + 4 \times (3 + 2)) \in Arith$ qui correspond bien à une expression valide. Par contre $+1 - /2$ n'est pas dans *Arith*.

Vous devez trouvez cette définition peu satisfaisante à cause de l'ambiguité des expressions ; nous reviendrons plus tard sur les problèmes soulevés par cet exemple.

2.3.2 Les termes

Les termes sont des arbres ordonnés étiquetés particuliers que nous reverrons lorsque nous aborderons la logique du premier ordre. On peut les voir comme l'archétype de la définition inductive, car ils sont définis par une définition inductives dans laquelle les règles ne sont pas "explicités". Chaque règle sera simplement un symbole, muni d'une arité, et n'ayant aucune sémantique (sens). Ils jouent un rôle essentiel dans beaucoup de structures en informatique.

Définition 2.11 (Signature)**.** Une *signature* est un ensemble $\mathcal{S}$ de symboles muni d'une application $\rho : \mathcal{S} \to \mathbb{N}$, appelée *arité*.

On représentera souvent une signature comme un ensemble de couples (symbole, arité). Par exemple, $\{ (f,2), (g,1), (h,0) \}$ est la signature dont les symboles sont f, g, h, d'arité $2, 1$ et 0, respectivement. Formellement, on a ici $\mathcal{S} = \{ f, g, h \}$, $\rho(f) = 2$, $\rho(g) = 1$, $\rho(h) = 0$. Un symbole $f \in \mathcal{S}$ tel que $\rho(f) = 0$ est appelé *constante*.

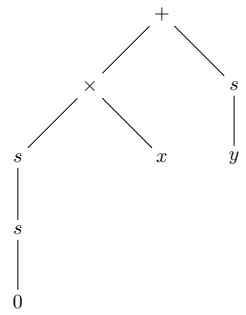
Définition 2.12 (Termes)**.** Étant donné une signature $\mathcal{S}$ et un ensemble X (de variables individuelles), l'ensemble $\mathcal{T}_{\mathcal{S}}(X)$ est défini inductivement par :

$$\frac{}{x \in X} \qquad \frac{x_1 \quad \dots \quad x_n}{f(x_1, \dots, x_n)} \text{ pour tout } f \in \mathcal{S} \text{ d'arité } n.$$

Un terme est donc une expression formée à partir de X en utilisant les symboles de $\mathcal{S}$ de sorte qu'un symbole f soit appliqué à un nombre de termes égal à $\rho(f)$. En particulier, si $f \in \mathcal{S}$ est une constante, alors elle s'applique a une liste vide de termes : $f()$ est un terme ; pour simplifier la notation, on écrit également f.

Exemple 2.13. On considère la signature de l'arithmétique suivante : $\mathcal{S}_{ar} = \{(0,0), (s,1), (+,2), (\times,2)\}$ où s représente la fonction « successeur ».

Pour $x, y \in X$, l'expression $+(\times(s(s(0)), x), s(y))$ (que nous nous autoriserons à écrire $(s(s(0)) \times x) + s(y)$) est un terme de $\mathcal{T}_{\mathcal{S}_{ar}}(X)$, représenté par l'arbre ordonné suivant :



Notez bien la différence avec les expressions arithmétiques présentées dans la section 2.3.1, où il n'était pas possible de dégager une unique interprétation aux expressions.

En fait, tout terme est un arbre ordonné étiqueté : les sommets internes sont étiquetés par les symboles de $\mathcal{S}$, les feuilles par des variables ou des symboles de $\mathcal{S}$ d'arité 0, et un sommet étiqueté par un symbole d'arité k possède exactement k fils.

Leur hauteur (et donc la taille) d'un terme n'est pas bornée car, par exemple,

$$s^n(0) := \underbrace{s(s(\dots s}_{n\text{-fois}}(0)\dots))$$

est un terme, pour tout $n \geq 1$.

Exemple 2.14. Le signature de la théorie des groupes est $\{ (e,0), (inv,1), (*,2) \}$, où $*$ est l'opérateur de composition et inv est l'opérateur « inverse » qui est habituellement noté x^{-1}.

2.3.3 Arbres de dérivation

Etant donné une définition inductive (B, R) d'un ensemble X et $x \in X$. Un arbre de dérivation de x est une trace de la construction inductive de x. C'est en fait une preuve de l'appartenance de x à X. Contrairement aux arbres usuels, les arbres de preuve sont représentés avec la racine en bas. La racine d'une preuve de $x \in X$ est x, les feuilles sont des éléments de B et chaque noeud interne est une instance d'une règle de R (c'est à dire une règle de R appliquée à des valeurs particulières).

Exemple 2.15. Voici un arbre de dérivation du terme $+(\times(s(s(0)), x), s(y))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{0}}{s(0)}}{s(s(0))} \quad \overline{x}}{\times(s(s(0)), x)} \quad \dfrac{\overline{y}}{s(y)}}{+(\times(s(s(0)), x), s(y))}$$

Notez la ressemblance de votre résultat avec l'arbre représentant le terme : chaque terme est "isomorphe" à son arbre de dérivation.

Exemple 2.16. Le mot $1+2+3$ appartient à *Arithm*. En voici une preuve sous forme d'un arbre de dérivation :

$$\dfrac{\dfrac{\overline{1 \in \mathit{Arithm}} \quad \overline{2 \in \mathit{Arithm}}}{1+2 \in \mathit{Arithm}} \quad \overline{3 \in \mathit{Arithm}}}{1+2+3 \in \mathit{Arithm}}$$

Ce n'est pas la seule preuve possible, en voici une autre :

$$\dfrac{\overline{1 \in \mathit{Arithm}} \quad \dfrac{\overline{2 \in \mathit{Arithm}} \quad \overline{3 \in \mathit{Arithm}}}{2+3 \in \mathit{Arithm}}}{1+2+3 \in \mathit{Arithm}}$$

Définition 2.17. Une définition inductive de X est *non ambiguë* si chaque $x \in X$ admet un unique arbre de dérivation.

L'exemple 2.16 prouve donc que la définition que nous avons donné de l'ensemble *Arithm* est ambiguë. Ce problème est intrinsèque aux expressions arithmétiques, puisque lorsqu'on écrit $1+2+3$, on ne précise pas dans l'écriture si l'on veut parler du résultat de l'addition de 1 à $2+3$ ou de celle de $1+2$ à 3.

Proposition 2.18. *Soit (B, R) une définition inductive d'un ensemble X. Si :*

1. *les axiomes ne peuvent pas être produits par les règles :*
2. *chaque $x \in X$ ne peut être produit que par une seule des règles de R*
3. *les règles sont injectives (chaque x a au plus un antécédent par $r \in R$) ;*

alors la définition est non-ambiguë.

2.4 Preuves par induction

La preuve par induction est une généralisation de la preuve par récurrence aux ensembles définis inductivement.

Théorème 2.19 (Preuve par induction)**.** *Soit $X \subseteq E$ un ensemble défini inductivement par (B, R) et $P(x)$ un prédicat exprimant une propriété d'un élément $x \in E$. Considérons les conditions suivantes :*

- *(Base) $P(x)$ est vrai pour chaque $x \in B$;*
- *(Induction) pour chaque $r \in R$ d'arité n, pour tous $x_1, \ldots, x_n \in E$,*
  si $P(x_1), \ldots, P(x_n)$ sont vrais, alors $P(r(x_1, \ldots, x_n))$ est vrai.

Si (Base) et (Induction) sont vérifiées, alors $P(x)$ est vraie pour chaque $x \in X$.

Démonstration. Supposons que (Base) et (Induction) sont vérifiées, et notons Y l'ensemble des éléments de E qui satisfont la propriété P. Il s'agit donc de prouver que $X \subseteq Y$.

- $B \subseteq Y$ d'après (Base),
- d'après (Induction), si $x_1, \ldots, x_n \in Y$ alors $r(x_1, \ldots, x_n) \in Y$.

Par définition, X est le plus petit ensemble vérifiant les deux points précédents, donc $X \subseteq Y$. □

Exemple 2.20. On prouve par induction que pour tout mot de Dyck w (voir Exemple 2.8) , la propriété suivante est vraie :

$P(w) := w$ possède autant de parenthèses fermantes que de parenthèses ouvrantes.

- (Base) $P(\varepsilon)$ est vraie : ε ne contient aucune parenthèse ;
- (Induction) supposons que $P(w)$ est vrai, et que n est le nombres de parenthèses ouvrantes de w, alors (w) possède $n+1$ parenthèses ouvrantes et $n+1$ parenthèses fermantes. Donc P est vraie pour (w)
- (Induction) supposons que $P(w_1)$ et $P(w_2)$ sont vrais, et que n_1 et n_2 sont les nombres de parenthèses ouvrantes de w_1 et w_2, alors $w_1 w_2$ possède $n_1 + n_2$ parenthèses ouvrantes et $n_1 + n_2$ parenthèses fermantes. Donc P est vraie pour $w_1 w_2$.

2.5 Fonctions définies inductivement

Nous aurons parfois besoin de définir des fonctions sur des ensembles X définis inductivement. Cela peut se faire facilement lorsque X admet une définition non ambigüe. Vous reconnaitrez ici la notion de "fonction récursive" que vous utilisez souvent en programmation.

Définition 2.21. (Fonction définie inductivement) Soit (B, R) une définition inductive non ambiguë d'un ensemble X, et Y un ensemble quelconque. Une définition par induction structurelle d'une fonction $f : X \to Y$ est la donnée de :

- (Base) la valeur de $f(x)$ pour chacun des éléments $x \in B$;
- (Induction) la valeur de $f(r(x_1, \ldots, x_n))$ en fonction de $x_1, \ldots, x_n$ et $f(x_1), \ldots, f(x_n)$, pour chaque règle $r \in R$ d'arité n.

Exemple 2.22. La fonction factorielle f de $\mathbb{N}$ dans $\mathbb{N}$ se définit inductivement par

- (Base) $f(0) = 1$;
- (Induction) $f(n+1) = (n+1) \times f(n)$.

En utilisant la notation sous forme de règles, la définition de f est :

$$\frac{}{0 : 1} \qquad \frac{\text{n : x}}{n+1 : (n+1) \times x}$$

Exemple 2.23. La hauteur h d'un terme dans $\mathcal{T}_{\mathcal{S}}(X)$ se définit inductivement par

- (Base) $h(x) = 1$ pour tout $x \in X$;
- (Induction) $h(a(t_1, \ldots, t_n)) = 1 + max\{h(t_1), \ldots, h(t_n)\}$, pour tout $a \in \mathcal{S}$ d'arité n.

ou, sous forme de règles :

$$\frac{}{x : 1}\ x \in X \qquad \frac{t_1 : m_1 \quad \cdots \quad t_n : m_n}{a(t_1, \ldots, t_n) : 1 + max\{m_1, \ldots, m_n\}}\ a \text{ d'arité } n$$

Exemple 2.24. La valeur v d'un terme arithmétique (voir Exemple 2.13), à partir d'une valuation val de X (c'est à dire une fonction $val : X \to \mathbb{N}$) se définit inductivement par :
— (Base) $v(x) = val(x)$ pour tout $x \in X$;
— (Induction) $v(0) = 0$;
— (Induction) $v(s(x)) = v(x) + 1$ pour tout $x \in \mathcal{T}_{\mathcal{S}_{ar}}(X)$
— (Induction) $v(+(x, y)) = v(x) + v(y)$ pour tout $x, y \in \mathcal{T}_{\mathcal{S}_{ar}}(X)$
— (Induction) $v(\times(x, y)) = v(x) \times v(y)$ pour tout $x, y \in \mathcal{T}_{\mathcal{S}_{ar}}(X)$

Supposons que $val(x) = 2$ et $val(y) = 3$. Le calcul de la valeur du terme $+(\times(s(s(0)), x), s(y))$ peut se représenter par l'arbre de dérivation suivant :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{0:0}}{s(0):1}}{s(s(0)):2} \quad \dfrac{}{x:2}}{\times(s(s(0)), x):4} \quad \dfrac{\dfrac{}{y:3}}{s(y):4}}{+(\times(s(s(0)), x), s(y)):8}$$

L'exemple suivant prouve que si la définition du domaine de la fonction est ambiguë, alors la fonction peut ne pas être bien définie :

Exemple 2.25. Soit Σ un alphabet, on considère la définition inductive de Σ^* suivante :

$$\dfrac{}{\varepsilon} \qquad \dfrac{}{a}\ a \in \Sigma \qquad \dfrac{u \qquad v}{uv}$$

Cette définition est clairement ambiguë. On définit maintenant la fonction $\varphi : \Sigma^* \to \mathbb{N}$ par :

$$\dfrac{}{\varepsilon\ :\ 1} \qquad \dfrac{}{a\ :\ 1}\ a \in \Sigma \qquad \dfrac{u\ :\ n \qquad v\ :\ m}{uv\ :\ n+m}$$

Puisqu'il y a plusieurs dérivations d'un mot u, il y a donc plusieurs calculs de $\varphi(u)$, chacun pouvant donner un résultat différent :

$$\dfrac{\dfrac{}{a\ :\ 1} \quad \dfrac{}{b\ :\ 1}}{ab\ :\ 2} \qquad \dfrac{\dfrac{}{\varepsilon\ :\ 1} \quad \dfrac{\dfrac{}{a\ :\ 1} \quad \dfrac{}{b\ :\ 1}}{ab\ :\ 2}}{ab\ :\ 3}$$