L3I COMBINATOIRE — 3 : NATURELS ET ENSEMBLES FINIS

Christian RONSE, ICube, Département d'Informatique de l'Université de Strasbourg

Les *entiers naturels* (on dit aussi tout simplement : les *naturels*) sont les entiers non-négatifs $0, 1, 2, \ldots$, tandis que les *entiers relatifs* sont tous les entiers positifs ou négatifs : $0, 1, -1, 2, -2, \ldots$ On écrit $\mathbb{N}$ pour l'ensemble des entiers naturels et $\mathbb{Z}$ pour celui des entiers relatifs ; on pose $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, l'ensemble des entiers > 0.

Les entiers naturels sont caractérisés par les *axiomes de Peano.* Etant donnés une propriété (en fait, un prédicat) notée P et un entier naturel n, nous écrirons $P(n)$ pour dire que n satisfait la propriété P. Les axiomes sont :

1. 0 est un naturel.
2. Tout naturel n a un successeur, noté $s(n)$ (en fait, $s(n) = n + 1$).
3. Aucun naturel n'a 0 comme successeur : $\forall n \in \mathbb{N},\ s(n) \neq 0$.
4. Deux naturels distincts ont des successeurs distincts : $\forall m, n \in \mathbb{N},\ m = n \ \Leftrightarrow\ s(m) = s(n)$.
5. Toute propriété satisfaite par 0, et satisfaite par le successeur de tout naturel qui la satisfait, doit alors être satisfaite par tous les naturels : pour un prédicat P,

$$\Big(P(0) \text{ et } \big[\forall n \in \mathbb{N},\ P(n) \ \Rightarrow\ P(s(n))\big]\Big) \implies \big[\forall n \in \mathbb{N},\ P(n)\big] \ .$$

Le 5ème axiome est en fait le *principe de récurrence*, aussi appelé *principe d'induction.* Ces axiomes permettent de définir l'ordre numérique $<$ et les opérations arithmétiques (addition, soustraction, multiplication, division, factorielle, etc.), et de prouver leur propriétés. Le principe de récurrence est souvent utilisé pour prouver des théorèmes en arithmétique, mais aussi pour définir une propriété ou construire une fonction de domaine $\mathbb{N}$, par exemple la factorielle :

$$0! = 1, \qquad \forall n \in \mathbb{N}, \quad (n+1)! = (n+1) \cdot n!$$

Les naturels peuvent aussi être définis comme des ensembles, selon la *construction des ordinaux de von Neumann* :

$$\begin{aligned} 0 &= \emptyset \ , \\ 1 &= \{0\} \ , \\ 2 &= 1 \cup \{1\} = \{0, 1\} \ , \\ 3 &= 2 \cup \{2\} = \{0, 1, 2\} \ , \\ &\vdots \quad \vdots \\ s(n) &= n \cup \{n\} = \{0, \ldots, n\} \ , \\ &\vdots \quad \vdots \end{aligned}$$

Ainsi par exemple $3 = \big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\big\}$. Tout naturel n vérifie alors

$$n = \{m \in \mathbb{N} \mid m < n\} \ ,$$

et pour deux naturels m, n, on a

$$m < n \ \Leftrightarrow\ m \in n \ \Leftrightarrow\ m \subset n \ .$$

Cette définition permet d'identifier E^n, le produit cartésien de E par lui-même n fois, avec l'ensemble des fonctions $n \to E$. En effet, $n = \{0, \ldots, n-1\}$, et on peut identifier un n-uple $(x_0, \ldots, x_{n-1})$ avec la fonction $n \to E : i \mapsto x_i$.

Comme $2 = \{0, 1\}$, on écrira aussi 2^E pour l'ensemble des fonctions $E \to \{0, 1\}$. On a une bijection naturelle entre $\mathcal{P}(E)$ et 2^E : à toute partie P de E on associe sa *fonction caractéristique* χ_P définie par

$$\chi_P : E \to \{0,1\} : p \mapsto \begin{cases} 1 & \text{si } p \in P \ , \\ 0 & \text{si } p \notin P \ . \end{cases}$$

L'application $\mathcal{P}(E) \to 2^E : P \mapsto \chi_P$ est une bijection, et la bijection inverse $2^E \to \mathcal{P}(E)$ associe à toute fonction $f : E \to \{0, 1\}$ la partie

$$f^{-1}(\{1\}) = \{p \in E \mid f(p) = 1\} \ .$$

En effet, on a bien $f = \chi_P \iff P = f^{-1}(\{1\})$.

Le principe de récurrence (ou d'induction) peut prendre plusieurs formes (équivalentes entre elles), nous en donnons trois :

1. Pour un prédicat P, si $P(0)$ et $\forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)$, alors $\forall n \in \mathbb{N},\ P(n)$. C'est la formulation usuelle, cf. l'axiome 5 de Peano.
2. Un prédicat P tel que pour tout naturel n, s'il est satisfait par tous les $m < n$ alors il est satisfait par n, devra être satisfait par tous les naturels :
$$\Big(\forall n \in \mathbb{N},\ \Big[[\forall m < n,\ P(m)] \Rightarrow P(n)\Big]\Big) \implies [\forall n \in \mathbb{N},\ P(n)] \ .$$
Notons que pour $n = 0$, il n'y a aucun $m < n$, donc l'énoncé $\big[\forall m < n,\ P(m)\big]$ est satisfait de façon vide (par le principe logique que les objets qui n'existent pas satisfont n'importe quelle propriété, vu qu'on ne peut pas en montrer un qui ne la satisfait pas). Donc on doit en fait vérifier que
$$\begin{gathered} P(0) \ , \\ \forall n \in \mathbb{N}^*,\ \big[P(0),\ \ldots,\ P(n-1)\big] \implies P(n) \ , \end{gathered}$$
et alors on déduira que $\forall n \in \mathbb{N},\ P(n)$.
3. Pour un prédicat P satisfait par au moins un naturel, parmi ceux qui la satisfont il y en a un qui est le plus petit :
$$[\exists n \in \mathbb{N},\ P(n)] \implies \Big(\exists n \in \mathbb{N},\ P(n) \wedge \big[\forall m \in \mathbb{N},\ P(m) \implies n \le m\big]\Big) \ .$$
Ainsi, si un prédicat n'est pas satisfait par tous les naturels, il y a alors le plus petit naturel qui ne le satisfait pas, ce qu'on appelle le "contre-exemple minimum" ; il est souvent utilisé pour prouver par contradiction qu'un prédicat est satisfait par tous les naturels.

On peut, selon les situations, utiliser d'autres variantes, par exemple prouver que $P(0)$, $P(1)$, et $\forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+2)$, pour obtenir que P est satisfait par tous les naturels.

Chacune de ces formes du principe d'induction admet une variante en termes d'un sous-ensemble F de $\mathbb{N}$ au lieu du prédicat P, où on écrit $n \in F$ au lieu de $P(n)$. Ces variantes sont plus fortes, car il existe des sous-ensembles de $\mathbb{N}$ qui ne sont pas décrits par un prédicat (vu que l'ensemble des prédicats est dénombrable, mais celui des sous-ensembles de $\mathbb{N}$ n'est pas dénombrable).

Nous allons maintenant aborder la question de la taille d'un ensemble, c.-à-d. du nombre de ses éléments. Pour deux ensembles A et B, on dit que A est *équipotent* à B s'il existe une bijection $A \to B$. Cette relation est symétrique, car à toute bijection $A \to B$ correspond la bijection inverse $B \to A$, donc on dira simplement que A et B sont équipotents. Par ailleurs, on voit que A est équipotent à A (par Id_A), et que si A est équipotent à B et B est équipotent à C, alors A est équipotent à C (les bijections $A \to B$ et $B \to C$ se composent en une bijection $A \to C$). La relation d'équipotence est donc une *relation d'équivalence*; elle indique que les deux ensembles ont la même taille.

Un ensemble est dit *fini* s'il n'est pas équipotent à une de ses parties propres. Il est dit *infini* s'il n'est pas fini, c.-à-d. s'il est équipotent à une de ses parties propres. Par exemple $\mathbb{N}$ est infini parce qu'on a la bijection $\mathbb{N} \to \mathbb{N}^* : n \mapsto n+1$, avec $\mathbb{N}^* \subset \mathbb{N}$. On peut démontrer les théorèmes suivants (on suppose les naturels définis comme des ensembles par la construction de von Neumann) :

(i) Tout naturel est fini.

(ii) Tout ensemble fini est équipotent à un naturel, et un seul.

On définit donc le *cardinal* d'un ensemble fini A comme l'unique naturel équipotent à A, et on le note $card(A)$. Notons que $card(n) = n$.

Etant donnés deux ensembles finis A et B et une application $f : A \to B$, on a les propriétés suivantes :

(a) Si f est injective, alors $card(A) \leq card(B)$.

(b) Si f est surjective, alors $card(A) \geq card(B)$.

(c) Si $card(A) = card(B)$, alors f est injective ssi elle est surjective ssi elle est bijective.

Soit E un ensemble et f une application $E \to E$. Pour tout naturel n, on définit $f^n : E \to E$ par récurrence :

$$f^0 = Id_E \quad ,$$
$$\forall n \in \mathbb{N},\ f^{n+1} = f \circ f^n \quad .$$

Supposons E fini, et soit $x \in E$. Alors les $f^n(x)$, $n \in \mathbb{N}$, ne peuvent pas être mutuellement distincts. Plus précisément, il doit exister deux naturels m, n tels que $m < n \leq card(E)$ et $f^m(x) = f^n(x)$, sinon $\{f^n(x) \mid 0 \leq n \leq card(E)\}$ serait une partie de E de cardinal $card(E) + 1$. Soit $h(x)$ le plus petit naturel m tel qu'il existe un naturel $n > m$ pour lequel $f^n(x) = f^m(x)$, et soit $p(x)$ le plus petit naturel $n > 0$ tel que $f^{h(x)+n}(x) = f^{h(x)}(x)$. On a alors les propriétés suivantes :

(i) Pour $0 \leq m < n < h(x) + p(x)$, $f^m(x) \neq f^n(x)$.

(ii) Pour $0 \leq m < n$, on a $f^m(x) = f^n(x)$ ssi $h(x) \leq m$ et $m \equiv n$ modulo $p(x)$.

(iii) $\{f^n(x) \mid n \in \mathbb{N}\} = \{f^n(x) \mid n < h(x) + p(x)\}$.

On appelle $h(x)$ la *hauteur* de x, $p(x)$ la *période* de x, et $\{f^n(x) \mid h(x) \leq n < h(x) + p(x)\}$ le *cycle attracteur* de x. Donc la suite des $f^n(x)$, $n \in \mathbb{N}$, entre dans le cycle attracteur en $n = h(x)$, pour ne plus en sortir, elle va le parcourir circulairement, sans cesse. Nous illustrons ces notions dans le graphique ci-dessous, où $h(x) = 2$ et $p(x) = 4$:

$$\begin{array}{ccccccc} x & \longrightarrow & f(x) & \longrightarrow & f^2(x) & \longrightarrow & f^3(x) \\ & & & & \uparrow & & \downarrow \\ & & & & f^5(x) & \longleftarrow & f^4(x) \end{array}$$

On a donc les $f^n(x)$ mutuellement distincts pour $n < h(x) + p(x) = 6$, et ensuite la suite des $f^n(x)$ va effectuer sans cesse le cycle $\{f^2(x), f^3(x), f^4(x), f^5(x)\}$, car on a

$$f^2(x) = f^6(x) = f^{10}(x) = \dots \quad ,$$
$$f^3(x) = f^7(x) = f^{11}(x) = \dots \quad ,$$
$$f^4(x) = f^8(x) = f^{12}(x) = \dots \quad ,$$
$$f^5(x) = f^9(x) = f^{13}(x) = \dots \quad .$$