4 . Induction

Les entiers naturels

* L'ensemble IN peut être défini à l'aide des axiomes de Péano
  * l'élément appelé zéro et noté 0 est un entier naturel.
  * Tout entier naturel n a un unique successeur, succ(n).
  * Aucun entier naturel n'a 0 pour successeur.
  * Deux entiers naturels ayant même successeur sont égaux.
  * Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à IN.

Les entiers naturels

* On note $n=succ^n(0)$
  * Le successeur d'un entier n est aussi noté n+1
  * On peut alors définir n+p par $succ^p(n)$ et on peut ensuite définir $n*p$, n^p, $n<p$
* Propriétés
  * Toute partie A non vide possède un plus petit élément (borne inférieure)
  * Toute partie A non vide et majorée admet un plus grand élément (borne supérieure)
  * L'ensemble N tout entier n'a pas de majorant

Récurrence (simple)

Soit P une propriété définie sur les entiers

* SI
  * P(0) est vraie
  * Pour tout n, (P(n) $\Rightarrow$P(n+1))
* ALORS la propiété P est vraie pour tout entier n

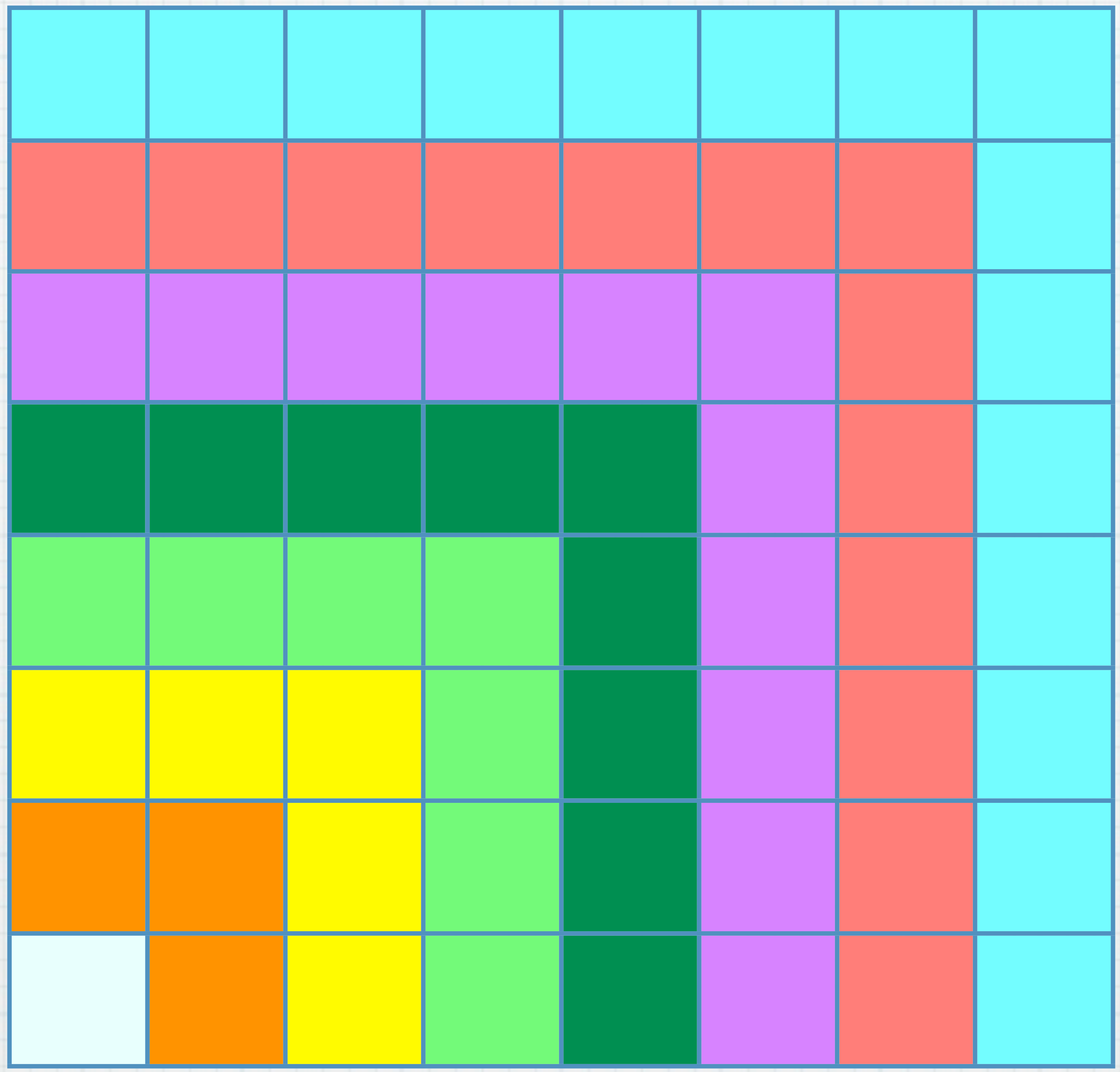
Preuve par récurrence

Soit à démontrer la propriété P(n) : « $(n+1)^2 = \sum_{0 \leq i \leq n} (2i + 1)$ ».

* **Initialisation** : pour n = 0, P(0) est vraie.
* **Hypothèse de récurrence**

  Supposons que P(n) soit vraie pour un certain n, à savoir $(n+1)^2 = \sum_{0 \leq i \leq n} (2i + 1)$
* **Hérédité**
  * On a $((n+1)+1)^2 = (n+1)^2 + 2n + 3$. et donc, d'après l'hypothèse de récurrence,
  * $(n+2)^2 = \left(\sum_{0 \leq i \leq n} (2i + 1)\right) + 2n + 3 = \sum_{0 \leq i \leq n+1} (2i + 1)$
* **Conclusions**
  * P(0) est vraie
  * $\forall n \in \mathbb{N} \; (P(n) \Rightarrow P(n+1))$ $\Longrightarrow$ $\forall n \in \mathbb{N}$ P(n) est vraie.

Interprétation géométrique



Récurrence (double)

Soit P une propriété définie sur les entiers

* SI
    * $P(0)$ et $P(1)$ sont vraies
    * Pour tout n, $(P(n)$ et $P(n+1) \Rightarrow P(n+2)$
* ALORS

la propiété P est vraie pour tout entier n

Preuve par récurrence

Soit Fn la suite de Fibonnacci 1, 1, 2, 3, 5, 8, 13, ...

Montrer que $F_{p+q} = F_{p-1}F_q + F_pF_{q+1}$ par récurrence d'ordre 2 sur q.

* Initialisation :
  * rang q=0 $F_p = F_{p-1}F_0 + F_pF_1$
  * rang q=1 $F_{p+1} = F_{p-1}F_1 + F_pF_2$
* Hypothèses de récurrence
  * $F_{p+q} = F_{p-1}F_q + F_pF_{q+1}$
  * $F_{p+q+1} = F_{p-1}F_{q+1} + F_pF_{q+2}$
* Hérédité

$$
\begin{aligned}
F_{p+q+2} &= F_{p+q+1} + F_{p+q} \\
&= F_{p-1}F_{q+1} + F_pF_{q+2} + F_{p-1}F_q + F_pF_{q+1} \\
&= F_{p-1}(F_{q+1}+F_q) + F_p(F_{q+2} + F_{q+1}) \\
&= F_{p-1}F_{q+2} + F_pF_{q+3}
\end{aligned}
$$

Récurrence généralisée

Soit P une propriété définie sur les entiers

* SI
  * P(0) est vrai
  * Pour tout n, (Pour tout k< n, P(k) est vrai $\Rightarrow$P(n)
* ALORS la propiété P est vraie pour tout entier n

Propriété. Deux mots commutent si et seulement si ils sont puissances d'un même mot

* Exemples
  * $u=0101$ $v=010101$ et $uv=vu=(01)^5$
  * $u=0101$ $v=01010$ et $uv=0101.01010 \neq 01010.0101=vu$

* Preuve par récurrence généralisée sur la longueur de $|uv| = n$:
  $uv = vu$ et $|uv|=n \Leftrightarrow \exists\, w \in A^* \;\exists\, p,q \in \mathbb{N}$ tels que $u = w^p$ et $v = w^q$

  * Initialisation $P(0)$ vraie? Oui: $u = v = \varepsilon = \varepsilon^p = \varepsilon^q$ pour n'importe quels entiers p et q
  * Hypothèse de récurrence. Supposons que $P(k)$ est vraie pour tout $k<n$:
  * Hérédité. Supposons $\forall\, u,v \in A^*$ avec $|uv|=k<n$ $\exists\, w \in A^*$ $\exists\, p,q \in \mathbb{N}$ tels que $u = w^p$ et $v = w^q$
    * prenons u et v de A^* avec $|uv|=n$ et tels que $uv = vu$. Sans perte de généralité, on suppose que $|u| \geq |v|$. v est alors préfixe de u donc $u = vx$.
    * $uv = vu$ se réécrit $vx.v = v.vx$ d'où $xv = vx$.
      On applique l'hypothèse de récurrence à $xv=vx$ car $k=|xv|<n$ et $P(k)$ vraie:

      $xv = vx$ et $|xv|=k \Leftrightarrow \exists\, w \in A^* \;\exists\, p,q \in \mathbb{N}$ tels que $x = w^p$ et $v = w^q$ or $u = vx = w^q w^p = w^{p+q}$;

      cqfd.

Récursivité et induction

* En informatique, on définit récursivement des parties d'ensemble.

  C'est le cas de nombreuses structures de données.

  ex: les expressions arithmétiques, les arbres, les programmes syntaxiquement corrects.

* Intuitivement, une définition inductive est la donnée explicite de quelques éléments d'un ensemble infini et la donnée d'un mécanisme pour construire tous les autres éléments à partir de ceux donnés.

* Les éléments de départ constituent la base et on appelle étape inductive le mécanisme.

Ensembles définis inductivement

* Soit E un ensemble. Une définition inductive d'une partie X de E consiste en la donnée :
  * (B) d'un sous-ensemble B de E
  * (I) d'un ensemble K d'opérations Φ: $E_{a(\Phi)} \rightarrow E$ où $a(\Phi) \in \mathbb{N}$ est l'arité de Φ
* X est alors définie comme étant le plus petit ensemble vérifiant les assertions suivantes :
  * (B) $B \subseteq X$
  * (I) $\forall\ \Phi \in K,\ \ \forall\ x_1,\ldots x_{a(\Phi)} \in X,\ \ \Phi(x_1,\ldots,\ x_{a(\Phi)})\ \in X.$
* Une définition inductive d'un ensemble X est dite non ambiguë dès lors qu'il n'existe qu'une seule façon de construire chaque élément de X.

Ensembles définis inductivement

* Entiers naturels IN
  * B={0}
  * Φ: IN $\to$ IN
    n $\to$ succ(n)
* Mots binaires
  * B={ε}
  * Φ_0: u $\to$ 0.u
    Φ_1: u $\to$ 1.u
* Mots de parenthèses
  * B={ε}
  * Φ: (u,v) $\to$ "(".u .")".v

Exemples

- Sur IN :
  - (B) $0 \in P$
  - (I) $n \in P \Rightarrow n+2 \in P$
  - La plus petite partie P qui contient 0 et qui vérifie (I) est l'ensemble des entiers naturels pairs.
- Sur l'alphabet { 0 , 1 } :
  - (B) $\varepsilon \in L$
  - (I) si u et v $\in$ L alors 0.u.1.v $\in$ L et 1.u.0.v $\in$ L
  - La plus petite partie L qui contient ε et qui vérifie (I) est l'ensemble des mots qui contiennent autant de 0 que de 1. .

Fonctions définies inductivement

* Soit X un ensemble défini inductivement par
  * (B) d'un sous-ensemble B de E
  * (I) d'un ensemble K d'opérations Φ: $E_{a(\Phi)} \rightarrow E$ où $a(\Phi) \in \mathbb{N}$ est l'arité de Φ
* Une fonction f définie inductivement sur X est la donnée de
  * (B') f(b) pour tout b de
  * (I') L'expression de $f(\Phi(x_1,\dots, x_{a(\Phi)}))$ en fonction de $f(x_1)$, $f(x_2)\dots f(x_{a(\Phi)})$ pour tout Φservant à définir X.

Preuves par induction

* Soit X un ensemble défini inductivement par
  * (B) d'un sous-ensemble B de E
  * (I) d'un ensemble K d'opérations Φ: $E_{a(\Phi)} \rightarrow E$ où $a(\Phi) \in \mathbb{N}$ est l'arité de Φ
* Une propriété P sera vérifiée pour tous les éléments de X si et seulement si
  * (B'') P est vérifiée pour pour tout b de B
  * (I') La propriété P est stable par tous les Φservant à définir X.
    Si P est vraie pour $x_1,\ldots x_{a(\Phi)}$ alors P est aussi vraie pour $\Phi(x_1,\ldots, x_{a(\Phi)})$

Principe d'induction

On peut énoncer le principe d'induction (généralisée) sur n'importe quel ensemble inductif.

* **Théorème** Soit $\leq$ un ordre bien fondé sur un ensemble E. On note $<$ l'ordre strict correspondant. Soit P une propriété dépendant d'un élément x de E.
  * **SI** la phrase suivante est vraie :

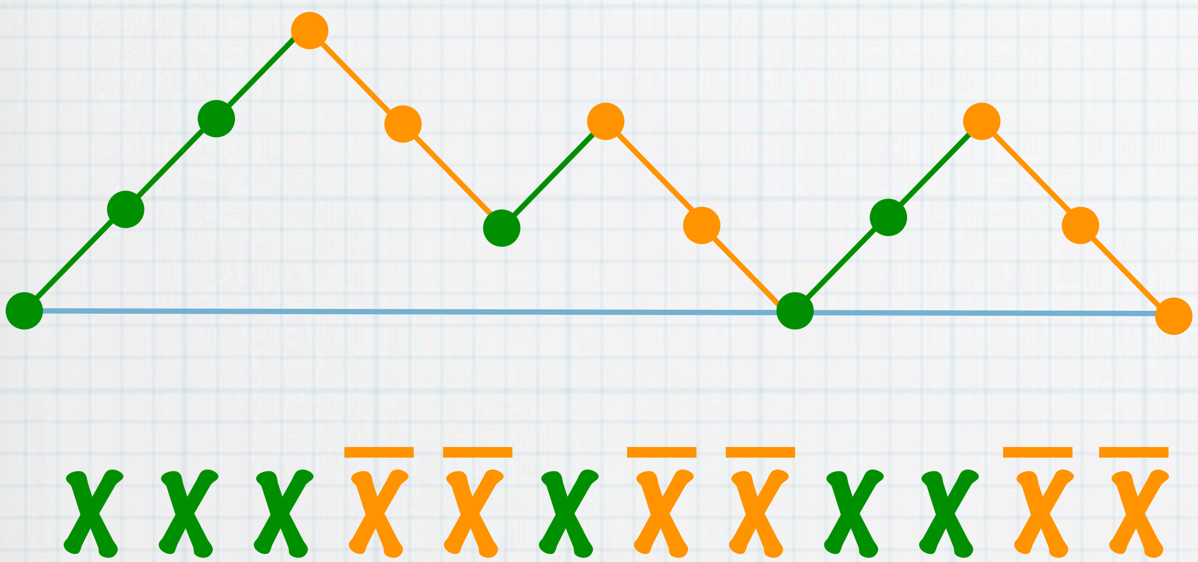
$$\forall x \in E \quad ((\forall y < x \ \ P(y)) \Rightarrow \ \ P(x))$$

  * **ALORS**, pour tout $x \in E$, on a $P(x)$ vraie.

Mots de Dyck

* On peut donner deux définitions d'un mot bien parenthésé
  * Par induction.
    * Δ est l'ensembles des mots sur l'alphabet $\{ x, \overline{x} \}$ défini par
      * $\varepsilon \in \Delta$
      * Si u et v sont dans Δ, il en est de même de $x.u.\overline{x}.v$
  * Par propriétés
    * D est l'ensemble des mots w sur l'alphabet $\{ x, \overline{x} \}$ tels que
      * w a autant de x que de $\overline{x}$
      * Tout préfixe de w a plus de x que de $\overline{x}$
* Théorème. $D = \Delta$

$D=\Delta$



- $B=\{\varepsilon\}$
- $\phi: (u,v) \longrightarrow x.u.\bar{x}.v$