Maths For Fun

1,2,3, soleil ! Dessiner la récurrence

Dominique Duval

Université de Grenoble

5 octobre 2009

II – Induction

Plan

Axiomes de Peano (2nd ordre)

L'ensemble des entiers naturels est un ensemble (noté $\mathbb{N}$)
avec un élément (noté 0)
et une fonction de $\mathbb{N}$ vers $\mathbb{N}$ (notée suc),
qui vérifient :

1. $\forall x \in \mathbb{N}, \mathrm{suc}(x) \neq 0$.
2. $\forall x, y \in \mathbb{N}, \mathrm{suc}(x) = \mathrm{suc}(y) \Rightarrow x = y$.
3. $\forall P \subseteq \mathbb{N}$,
   Initialisation. si $0 \in P$
   Hérédité. et si $\forall x \in \mathbb{N}\ (x \in P \Rightarrow \mathrm{suc}(x) \in P)$
   Conclusion. alors $P = \mathbb{N}$

L'axiome (3) est l'axiome de récurrence.

Dans le cours 1 on a exprimé les axiomes de Peano
comme une condition d'initialité.

Initialité

La signature des naturels Σ_{nat} :

$$\mathbb{1} \xrightarrow{z} N \xleftarrow{s} N$$

Le modèle des naturels M_{nat} :

$$\{*\} \xrightarrow{*\mapsto 0} \mathbb{N} \xleftarrow{n \mapsto n+1} \mathbb{N}$$

Le modèle M_{nat} de Σ_{nat} est initial :

Pour tout ensemble X avec $a \in X$ et $b : X \to X$,
il existe une unique fonction $f : \mathbb{N} \to X$ telle que
$f(0) = a$ et $f(\text{suc}(n)) = b(f(n))$ pour tout $n \in \mathbb{N}$.

$$\begin{array}{ccccc}
\{*\} & \xrightarrow{0} & \mathbb{N} & \xleftarrow{\text{suc}} & \mathbb{N} \\
\downarrow{\scriptstyle \text{id}} & = & \downarrow{\scriptstyle f} & = & \downarrow{\scriptstyle f} \\
\{*\} & \xrightarrow{a} & X & \xleftarrow{b} & X
\end{array}$$

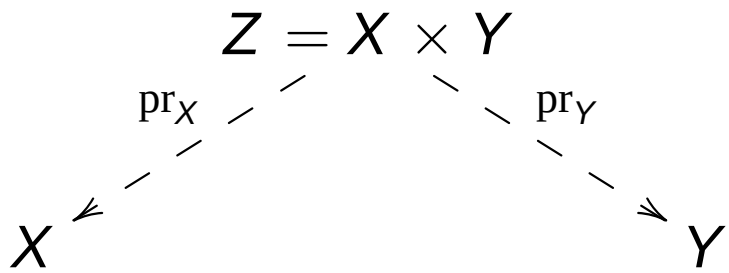
Plan

Signature

Une signature est un graphe formé
de sommets ou sortes ou types
et d'arcs ou opérations ou termes

avec des contraintes de la forme :

- $U = \mathbb{1}$ est le type unité
- $Z = X \times Y$ est le type produit de X et Y,
  avec les projections $\mathrm{pr}_X : Z \to X$ et $\mathrm{pr}_Y : Z \to Y$.



Exemples de signature

(notation simplifiée)

Σ_{nat} : $\mathbb{1} \xrightarrow{z} N \xleftarrow{s} N$

Σ_{bool} : $\mathbb{1} \xrightarrow{v} B \xleftarrow{f} \mathbb{1}$

Σ_{bin} : $\mathbb{1} \xrightarrow{e} G \xleftarrow{\star} G^2$

Σ_{list} : $\mathbb{1} \xrightarrow{e} L \xleftarrow{c} P \times L$

Σ_{flot} : $P \xleftarrow{h} F \xrightarrow{t} F$

Une grammaire est une signature

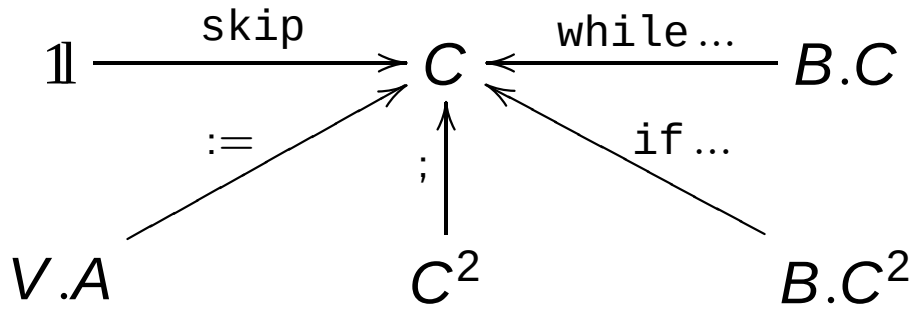
Une partie de la grammaire d'un langage impératif :

V : identificateurs de variables
A : expressions arithmétiques
B : expressions booléennes
C : commandes

Grammaire

$$C ::= \texttt{skip} \mid (V := A) \mid C; C \mid \texttt{if}\, B\, \texttt{then}\, C\, \texttt{else}\, C \mid \texttt{while}\, B\, \texttt{do}\, C$$

Signature Σ_{IMP}



Plan

Modèles

Soit Σ une signature.

$$\cdots \quad X \xrightarrow{f} Y \quad \cdots$$

Un modèle M de Σ est
une interprétation du graphe satisfaisant les contraintes.

$$\cdots \quad M(X) \xrightarrow{M(f)} M(Y) \quad \cdots$$

c'est-à-dire :

- un ensemble $M(X)$ pour chaque X,
- une fonction $M(f) : M(X) \to M(Y)$ pour chaque $f : X \to Y$,
- avec $M(\mathbb{1}) = \{*\}$ (singleton)
- et $M(X \times Y) = M(X) \times M(Y)$ (produit cartésien)
  avec $M(p)(x, y) = x$ et $M(q)(x, y) = y$.

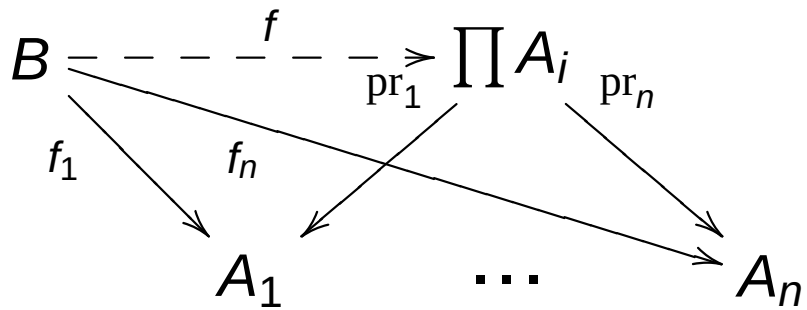
Produits cartésiens

$A_1 \times A_2 = \{\langle a_1, a_2\rangle \mid a_1 \in A_1 \wedge a_2 \in A_2\}$

$A_1 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{\langle a_1, \ldots, a_n\rangle \mid a_1 \in A_1 \wedge \cdots \wedge a_n \in A_n\}$

Caractérisation du produit cartésien.

Pour tous B et $f_i : B \to A_i$ (pour $i = 1, \ldots, n$)
il existe une unique $f : B \to A_1 \times \cdots \times A_n$
telle que $\mathrm{pr}_i \circ f = f_i$ pour tout i,
c'est le "n-uple" $f = \langle f_1, \ldots, f_n\rangle$



En C : STRUCT

Singletons

Pour $n = 0$ on définit

$$\text{“produit vide”} = \{*\} \quad \text{(singleton)}$$

Caractérisation du produit vide.

Pour tout B
il existe une unique $f : B \longrightarrow \{*\}$,
c'est le “0-uple” ou “collapsing” $f = \langle\,\rangle$

$$B \overset{\langle\,\rangle}{- - \succ} \{*\}$$

En C : `VOID` ne représente pas l'ensemble vide,
mais un singleton c'est-à-dire un produit vide !

Exemple de modèles

Signature Σ_{bin} :

$$\mathbb{1} \xrightarrow{e} G \xleftarrow{\star} G^2$$

Quelques modèles de Σ_{bin} :

$$\{*\} \xrightarrow{0} \mathbb{N} \xleftarrow{+} \mathbb{N}^2$$

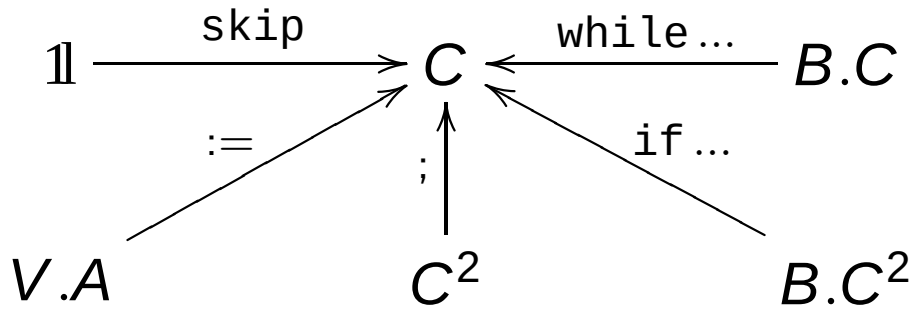
$$\{*\} \xrightarrow{1} \mathbb{N} \xleftarrow{\times} \mathbb{N}^2$$

$$\{*\} \xrightarrow{\varepsilon} \{a,b\}^* \xleftarrow{\cdot} (\{a,b\}^*)^2$$

$$\{*\} \xrightarrow{5} \mathbb{N} \xleftarrow{\hat{}} \mathbb{N}^2$$

La syntaxe est un modèle

Signature Σ_{IMP} :

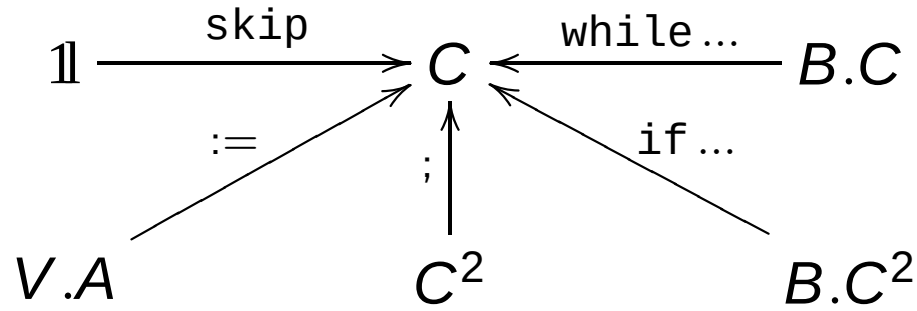


La syntaxe est le modèle I formé des termes clos :

- $I(A)$ est l'ensemble des expressions arithmétiques
  $I(A) = \{1 + 1, X + Y, \cdots : \mathbb{1} \to A\}$
- $I(C)$ est l'ensemble des commandes
  $I(C) = \{X := 1, \texttt{while true do skip}, \cdots : \mathbb{1} \to C\}$

La sémantique est un modèle

Signature Σ_{IMP} :



Soit $\mathbb{S} = \mathbb{Z}^{\mathbb{V}}$ l'ensemble des états

La sémantique est un modèle "mathématique" M :

- $M(A)$ est l'ensemble $\mathbb{Z}^{\mathbb{S}}$ (fonctions de $\mathbb{S}$ vers $\mathbb{Z}$)
  $M(A) = \{(s \mapsto 2), (s \mapsto s(X) + s(Y), \dots\}$
- $M(C)$ est l'ensemble $\mathbb{S}^{\mathbb{S},p}$ (fonctions partielles de $\mathbb{S}$ vers $\mathbb{S}$)
  $M(C) = \{(s \mapsto s[1/X]), (s \mapsto \bot), \dots\}$

Morphismes de modèles

Soit Σ une signature.

$$\cdots \quad X \xrightarrow{f} Y \quad \cdots$$

Un morphisme de modèles (de Σ) $m : M_1 \to M_2$ est :

- une fonction $m(X) : M_1(X) \to M_2(X)$ pour chaque X,
- telles que $m(Y) \circ M_1(f) = M_2(f) \circ m(X)$ pour chaque $f : X \to Y$.

$$\begin{array}{ccccc} \cdots & M_1(X) & \xrightarrow{M_1(f)} & M_1(Y) & \cdots \\ & {\scriptstyle m(X)}\downarrow & = & \downarrow{\scriptstyle m(Y)} & \\ \cdots & M_2(X) & \xrightarrow{M_2(f)} & M_2(Y) & \cdots \end{array}$$

Exemple de morphisme de modèles

Signature Σ_{bin} :

$$\mathbb{1} \xrightarrow{e} G \xleftarrow{\star} G^2$$

Un morphisme de modèles de Σ_{bin} :

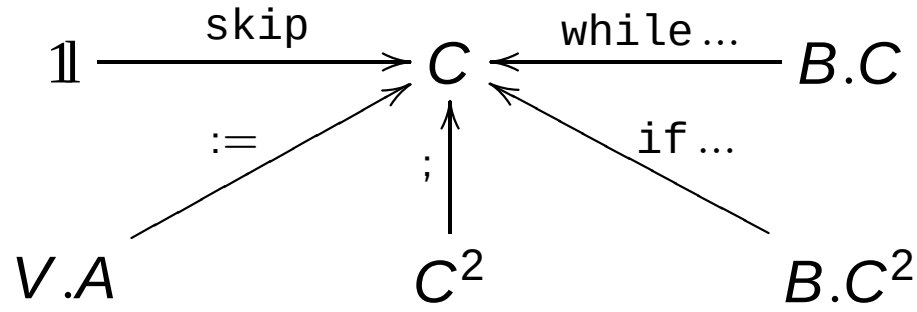
$$\begin{array}{ccccc}
\{*\} & \xrightarrow{0} & \mathbb{R} & \xleftarrow{+} & \mathbb{R}^2 \\
\downarrow{\scriptstyle \text{id}} & = & \downarrow{\scriptstyle \exp} & = & \downarrow{\scriptstyle \exp^2} \\
\{*\} & \xrightarrow{1} &]0,\infty[& \xleftarrow{\times} &]0,\infty[^2
\end{array}$$

L'exponentielle est un morphisme de modèles de Σ_{bin}

$\exp : (\mathbb{R}, +, 0) \to (]0, \infty[, \times, 1)$.

L'interprétation est un morphisme de modèles

Signature Σ_{IMP} :



L'interprétation de la syntaxe dans la sémantique est le morphisme de modèles $m : I \to M$:

- $I(A) \to M(A)$:
  $(1 + 1) \mapsto (s \mapsto 2)$,
  $(X + Y) \mapsto (s \mapsto s(X) + s(Y))$, ...
- $I(C) \to M(C)$:
  $(X := 1) \mapsto (s \mapsto s[1/X])$,
  $(\texttt{while true do skip}) \mapsto (s \mapsto \bot)$, ...

Plan

Modèle initial

Soit Σ une signature.

Définition. Un modèle M_0 de Σ est initial si
pour tout modèle M de Σ
il existe un unique morphisme $m : M_0 \to M$.

$$\begin{array}{ccccc} \cdots & M_0(X) & \xrightarrow{M_0(f)} & M_0(Y) & \cdots \\ & {\scriptstyle m(X)}\downarrow & = & \downarrow{\scriptstyle m(Y)} & \\ \cdots & M(X) & \xrightarrow{M(f)} & M(Y) & \cdots \end{array}$$

Exemples.

- Pour Σ_{nat} : le modèle M_{nat} (des naturels) est initial
- Pour Σ_{IMP} : le modèle I (de la syntaxe) est initial

Théorème d'initialité

Théorème d'initialité (pour les signatures).
Toute signature Σ a un modèle initial,
il est unique à iso près,
et c'est le modèle des termes clos engendrés par Σ.

Définition. Les termes clos engendrés par Σ sont les "chemins" de source $\mathbb{1}$ de Σ.
Ex. : $s(s(0)) : \mathbb{1} \to N$ dans Σ_{nat} ,
$*(e, e) : \mathbb{1} \to G$ dans Σ_{bin}

Slogan. *"no confusion, no junk".*

Exemples de modèles initiaux

Ex. La signature Σ_{nat} et le modèle des naturels :

$$\begin{array}{ccccc} \mathbb{1} & \xrightarrow{z} & N & \xleftarrow{s} & N \\ \{*\} & \xrightarrow{0} & \mathbb{N} & \xleftarrow{\text{suc}} & \mathbb{N} \end{array}$$

Ex. La signature Σ_{bool} et le modèle des booléens :

$$\begin{array}{ccccc} \mathbb{1} & \xrightarrow{v} & B & \xleftarrow{f} & \mathbb{1} \\ \{*\} & \xrightarrow{0} & \{0,1\} & \xleftarrow{1} & \{*\} \end{array}$$

Induction

Rappel. Théorème d'initialité

Toute signature Σ *a un modèle initial*,

c'est-à-dire un modèle M_0 tel que
pour tout modèle M de Σ
il existe un unique morphisme $m : M_0 \to M$.

Conséquence

L'induction est définie pour toute signature.

- définition par induction : il existe m
- preuve par induction : m est unique

Exemple. Sur Σ_{nat}, l'induction est appelée récurrence.

Généralisations

On a vu que le théorème d'initialité s'applique à :

- Toute signature Σ.

Peut-on le généraliser à :

- Toute signature avec des équations ?
  oui : monoïdes, groupes, anneaux,
  Ex. Application aux entiers relatifs avec 0, `succ`, `pred`,
  tels que $\forall x\ \texttt{pred}(\texttt{succ}(x)) = x$, $\forall x\ \texttt{succ}(\texttt{pred}(x)) = x$
- Toute signature avec des axiomes du 1er ordre ?
  en général non : corps
- Toute signature "paramétrée" ?
  "souvent" oui : listes, arbres, . . . (voir la suite)

Exemple : signature avec des équations

Soit Σ_{mon} la signature (comme Σ_{bin}):

$$\mathbb{1} \xrightarrow{e} G \xleftarrow{\star} G^2$$

avec en plus les équations de monoïde :

$\forall x, y, z,\ *(x, *(y, z)) = *(*(x, y), z)$
$\forall x,\ *(x, e) = x$
$\forall x,\ *(e, x) = x$

Les modèles de Σ_{mon} sont les monoïdes

Les morphismes de modèles de Σ_{mon} sont les morphismes de monoïdes (comme dans les cours d'algèbre)

Le modèle initial de Σ_{mon} est le modèle "singleton" :

$$\{*\} \xrightarrow{*} \{*\} \xleftarrow{\langle *,* \rangle \mapsto *} \{*\}$$

Signature paramétrée

Soit une signature Σ avec un type P “distingué”
(type des paramètres).

Choisissons un ensemble $\mathbb{A}$
(ensemble des arguments).

Les modèles de Σ où P vaut $\mathbb{A}$
sont les modèles M de Σ tels que $M(P) = \mathbb{A}$
avec les morphismes de modèles m tels que $m(P) = \mathrm{id}_{\mathbb{A}}$.

Théorème d’initialité (pour les signatures paramétrées).
Une signature paramétrée a un modèle initial
si toutes ses opérations sont de la forme
$f_i : P_i \times X^i \to X$ *avec* P_i *paramètres et* $i \in \mathbb{N}$

Exemple : listes

Soit la signature Σ_{list}, paramétrée par P :

$$\mathbb{1} \xrightarrow{e} L \xleftarrow{c} P \times L$$

Soit $\mathbb{A}$ un ensemble fixé.

Considérons la catégorie des modèles de Σ_{list} où P vaut $\mathbb{A}$.

Son modèle initial est le modèle des listes sur $\mathbb{A}$

$$\{*\} \xrightarrow{\text{empty}} \mathbb{A}^* \xleftarrow{\text{cons}} \mathbb{A} \times \mathbb{A}^*$$

Exemple : bégayer

Notons :

$\mathrm{cons}^{(1)} = \langle \mathrm{pr}_{\mathbb{A}}, \mathrm{cons} \rangle : \mathbb{A} \times \mathbb{A}^* \to \mathbb{A} \times \mathbb{A}^*$ $\boxed{\mathrm{cons}^{(1)}(x,l) = (x, \mathrm{cons}(x,l))}$

$\mathrm{cons}^{(2)} = \mathrm{cons} \circ \mathrm{cons}^{(1)} : \mathbb{A} \times \mathbb{A}^* \to \mathbb{A}^*$ $\boxed{\mathrm{cons}^{(2)}(x,l) = \mathrm{cons}(x, \mathrm{cons}(x,l))}$

Considérons le modèle de Σ_{list}:

$$\{*\} \xrightarrow{\text{empty}} \mathbb{A}^* \xleftarrow{\mathrm{cons}^{(2)}} \mathbb{A} \times \mathbb{A}^*$$

Définition par induction.

Il existe une unique fonction $r : \mathbb{A}^* \to \mathbb{A}^*$ telle que

$\boxed{r(\mathrm{empty}) = \mathrm{empty} \text{ et } r(\mathrm{cons}(x,l)) = \mathrm{cons}(x, \mathrm{cons}(x,l))}$

$$\begin{array}{ccccc}
\{*\} & \xrightarrow{\text{empty}} & \mathbb{A}^* & \xleftarrow{\mathrm{cons}} & \mathbb{A} \times \mathbb{A}^* \\
\downarrow{\scriptstyle \mathrm{id}} & = & \downarrow{\scriptstyle r} & = & \downarrow{\scriptstyle \mathrm{id} \times r} \\
\{*\} & \xrightarrow{\text{empty}} & \mathbb{A}^* & \xleftarrow{\mathrm{cons}^{(2)}} & \mathbb{A} \times \mathbb{A}^*
\end{array}$$

Exemple : longueur d'une liste

La fonction $\lg$ (longueur) pour les listes sur $\mathbb{A}$ peut être définie par induction sur Σ_{list}.

Il existe une unique fonction $\lg : \mathbb{A}^* \to \mathbb{N}$ telle que

$$\boxed{\lg(\text{empty}) = 0 \text{ et } \lg(\text{cons}(x, l)) = \text{suc}(\lg(l)).}$$

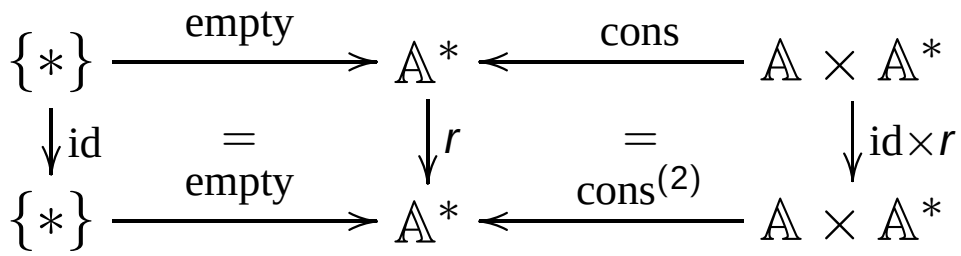
c'est-à-dire telle que

$$\boxed{\lg(\text{empty}) = 0 \text{ et } \lg(\text{cons}(x, l)) = \text{suc}(\text{pr}(x, \lg(l))).}$$

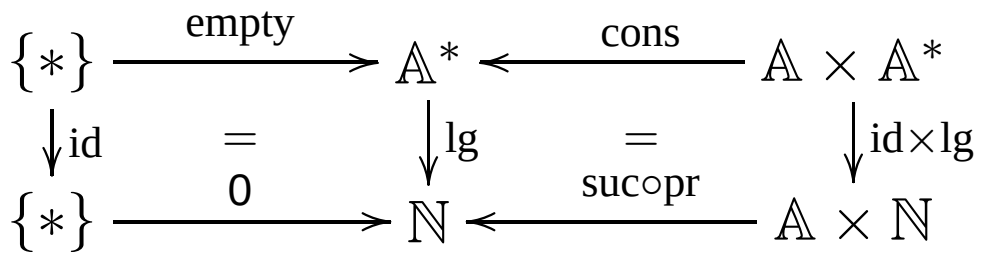
$$\begin{array}{ccccc}
\{*\} & \xrightarrow{\text{empty}} & \mathbb{A}^* & \xleftarrow{\text{cons}} & \mathbb{A} \times \mathbb{A}^* \\
\downarrow{\scriptstyle \text{id}} & = & \downarrow{\scriptstyle \lg} & = & \downarrow{\scriptstyle \text{id}\times\lg} \\
\{*\} & \xrightarrow{0} & \mathbb{N} & \xleftarrow{\text{suc}\circ\text{pr}} & \mathbb{A} \times \mathbb{N}
\end{array}$$

Exemple : bégaiement et doublement

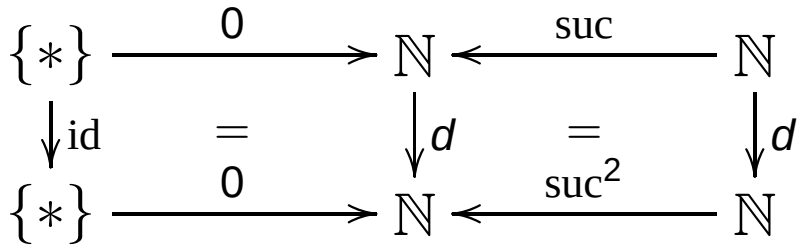
Bégaiement



Longueur



Doublement



Preuve par induction. *(à terminer...)*

$$\boxed{\forall l \in \mathbb{A}^* \quad d(\lg(l)) = \lg(r(l))}$$