Réécriture

Réductions abstraites

1 Quelques rappels et notations

Si R et T sont deux relations binaires sur A notées de façon infixée (c-à-d, $x\ R\ y$). On définit

- $x\ RT\ y$ ssi il existe z tel que $x\ R\ z$ et $z\ T\ y$.
- R^n par $R^0 = \{(x, x) \mid x \in A\}$ et $R^{n+1} = R\,R^n$ (donc $R^1 = R$).
- $R \subseteq T$ ssi $x\ R\ y$ implique $x\ T\ y$.
- $x\ (R \bigcup T)\ y$ ssi $x\ R\ y$ ou $x\ T\ y$.

Une relation est transitive si $x\ R\ y$ et $y\ R\ z$ impliquent $x\ R\ z$.

La fermeture transitive de R est la plus petite relation transitive qui contient R.

2 Relations et clôtures

Souvent la relation R est notée $\xrightarrow[R]{}$.

- R^{-1} est la relation converse $\{(y, x) \in A \times A \mid (x, y) \in R\}$, aussi notée $\xleftarrow[R]{}$.
- $\xleftrightarrow[R]{}$ est la clôture symétrique, c'est la relation $\xrightarrow[R]{} \cup \xleftarrow[R]{}$.
- $\xleftrightarrow[R]{*}$ est la clôture réflexive, symétrique et transitive de $\xrightarrow[R]{}$,
- $\xleftrightarrow[R]{+}$ est la clôture symétrique et transitive de $\xrightarrow[R]{}$,
- $\xrightarrow[R]{=}$ est la clôture réfle xive, c'est la relation $\xrightarrow[R]{} \cup \xrightarrow[R]{0}$ sachant que $\xrightarrow[R]{0}$ est l'égalité (c'est-à-dire que x $\xrightarrow[R]{=}$ y ssi x=y ou x $\xrightarrow[R]{}$ y).

En λ-calcul,

- $\xrightarrow[]{*}$ est noté $\twoheadrightarrow$,
- $\xleftrightarrow[]{*}$ est noté $\twoheadleftarrow\!\!\twoheadrightarrow$.

C'est culturel !

3 Diverses confluences ; notion de paire joignable

- Une relation R sur A est confluente si

$$(\forall M, N_1, N_2 \in A) M \xrightarrow[R]{*} N_1 \,\&\, M \xrightarrow[R]{*} N_2$$
$$\Rightarrow$$
$$(\exists P \in A) N_1 \xrightarrow[R]{*} P \,\&\, N_2 \xrightarrow[R]{*} P$$

autrement dit

$$\begin{tikzcd} & M \arrow[dl, "*", "R"'] \arrow[dr, "*"', "R"] & \\ N_1 & & N_2 \end{tikzcd} \Longrightarrow \exists P \begin{tikzcd} N_1 \arrow[dr, "*"', "R"] & & N_2 \arrow[dl, "*", "R"'] \\ & P & \end{tikzcd}$$

- Une relation R sur A est semi-confluente si

$$(\forall M, N_1, N_2 \in A) \;\; M \xrightarrow[R]{} N_1 \,\&\, M \xrightarrow[R]{*} N_2$$
$$\Rightarrow$$
$$(\exists P \in A) \;\; N_1 \xrightarrow[R]{*} P \,\&\, N_2 \xrightarrow[R]{*} P$$

autrement dit

$$\begin{tikzcd} & M \arrow[dl, "R"'] \arrow[dr, "*"', "R"] & \\ N_1 & & N_2 \end{tikzcd} \Longrightarrow \exists P \begin{tikzcd} N_1 \arrow[dr, "*"', "R"] & & N_2 \arrow[dl, "*", "R"'] \\ & P & \end{tikzcd}$$

- Une relation R sur A est localement confluente si

$$(\forall M, N_1, N_2 \in A) \;\; M \xrightarrow[R]{} N_1 \,\&\, M \xrightarrow[R]{} N_2$$
$$\Rightarrow$$
$$(\exists P \in A) \;\; N_1 \xrightarrow[R]{*} P \,\&\, N_2 \xrightarrow[R]{*} P$$

autrement dit

$$\begin{tikzcd} & M \arrow[dl, "R"'] \arrow[dr, "R"] & \\ N_1 & & N_2 \end{tikzcd} \Longrightarrow \exists P \begin{tikzcd} N_1 \arrow[dr, "*"', "R"] & & N_2 \arrow[dl, "*", "R"'] \\ & P & \end{tikzcd}$$

- Une paire de terme (N_1, N_2) est joignable, notée $N_1 \downarrow N_2$ si

$$(\exists P \in A) \;\; N_1 \xrightarrow[R]{*} P \,\&\, N_2 \xrightarrow[R]{*} P$$

d'où

- confluence : $M \xrightarrow[R]{*} N_1 \,\&\, M \xrightarrow[R]{*} N_2 \Rightarrow N_1 \downarrow N_2$,
- semi-confluence : $M \xrightarrow[R]{} N_1 \,\&\, M \xrightarrow[R]{*} N_2 \Rightarrow N_1 \downarrow N_2$.
- confluence locale : $M \xrightarrow[R]{} N_1 \,\&\, M \xrightarrow[R]{} N_2 \Rightarrow N_1 \downarrow N_2$,

- $$\begin{tikzcd} & \cdot \arrow[dl, "*"] \arrow[dr, "*"] & \\ \cdot \arrow[dr, dotted, "*"] & & \cdot \arrow[dl, dotted, "*"'] \\ & \cdot & \end{tikzcd} \quad \begin{tikzcd} & \cdot \arrow[dl] \arrow[dr, "*"] & \\ \cdot \arrow[dr, dotted, "*"] & & \cdot \arrow[dl, dotted, "*"'] \\ & \cdot & \end{tikzcd} \quad \begin{tikzcd} & \cdot \arrow[dl] \arrow[dr] & \\ \cdot \arrow[dr, dotted, "*"] & & \cdot \arrow[dl, dotted, "*"'] \\ & \cdot & \end{tikzcd}$$

confluence — semi-confluence — confluence locale

$\overset{*}{\dashrightarrow}$ est une flèche existentielle.

4 Propriété de Church Rosser

Définition : $N_1 \xleftrightarrow[R]{*} N_2 \Rightarrow N_1 \downarrow N_2$ signifie que R a la propriété de Church Rosser.

Théorème :

$$\begin{tikzcd} {} \arrow[rr, leftrightarrow, "*"] \arrow[dr, dotted, "*"'] & & {} \arrow[dl, dotted, "*"] \\ & {} & \end{tikzcd}$$

Les conditions suivantes sont équivalentes
– R est confluente,
– R est semi-confluente,
– R a la propriété de Church-Rosser

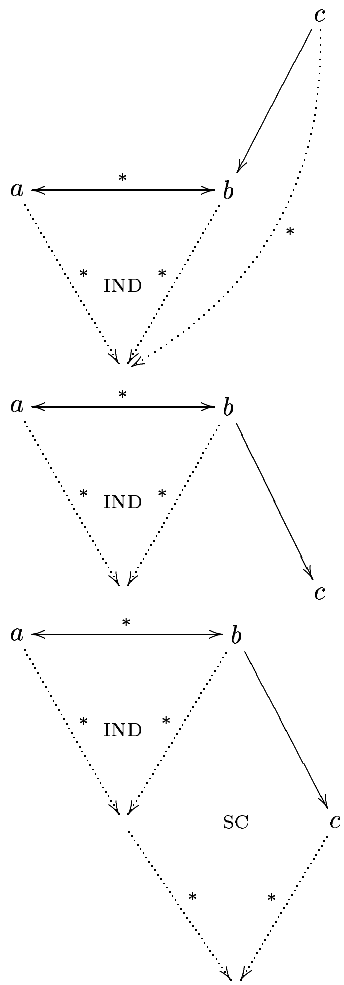
Preuve :

- Church-Rosser $\Rightarrow$ confluence $\Rightarrow$ semi-confluence est facile !
- $\boxed{\text{Semi-confluence} \Rightarrow \text{Church-Rosser}}$

  Par induction sur la longueur de $\xleftrightarrow{*}$.

$$\begin{tikzcd} a \arrow[rr, leftrightarrow, "*"] \arrow[dr, dotted, "*"'] & \arrow[d, phantom, "\textsc{ind}"] & b \arrow[r, leftrightarrow] \arrow[dl, dotted, "*"] & c \\ & {} & & \end{tikzcd}$$

$$\begin{tikzcd} & & & c \arrow[dl] \\ a \arrow[rr, leftrightarrow, "*"] \arrow[dr, dotted, "*"'] & \arrow[d, phantom, "\textsc{ind}"] & b \arrow[dl, dotted, "*"] & \\ & {} & & \end{tikzcd}$$



5 Réductibilité, forme normale

A partir de maintenant on laisse tomber les R s'il n'y a pas d'ambiguïté.

- x est réductible ssi il existe un y tel que $x \longrightarrow y$,
- x est irréductible ssi x n'est pas réductible,
- y est une forme normale de x ssi $x \xrightarrow{*} y$ et y est irréductible.
  Si la forme normale est déterminée de façon unique on la note $x\downarrow$.

6 Terminaison, convergence, normalisation

6.1 Définitions

- Une relation R termine ou est noethérienne ssi il n'existe pas de suite infinie $x_0 \xrightarrow[R]{} x_1 \xrightarrow[R]{} \ldots x_n \xrightarrow[R]{} x_{n+1} \cdots$
- Une relation est convergente si elle termine et est confluente
- Une relation est normalisante si toute élément a une forme normale.

6.2 Quelques faits

- Si $\longrightarrow$ est confluente, chaque élément a au plus une forme normale.
- Si $\longrightarrow$ est confluente et normalisante, chaque élément a une forme normale unique.

6.3 Preuve d'égalité par normalisation

Si $\longrightarrow$ est confluente et normalisante, alors $x \xleftrightarrow{*} y \quad \Leftrightarrow \quad x\downarrow = y\downarrow$

Fort bien, mais y a-t-il un moyen simple

1. de calculer ces formes normales ?
2. de savoir si une relation est normalisante ?

7 Induction noethérienne

DÉFINITION

$$(\mathcal{IN}) \quad \frac{(\forall x \in A)((\forall y \in A)\ x \xrightarrow{+} y \Rightarrow P(y)) \ \Rightarrow P(x)}{(\forall a \in A) P(a)}$$

RÉSULTAT

$(\mathcal{IN})$ est satisfaite sur A si et seulement si $\longrightarrow$ termine.

8 Notion de branchement

- Une relation est à branchement fini ssi pour tout x il n'y a qu'un nombre fini de y tels que $x \longrightarrow y$.
- Une relation est globalement finie ssi pour tout x il n'y a qu'un nombre fini de y tels que $x \xrightarrow{+} y$.
- Une relation est acyclique ssi il n'y a pas d'élément a tel que $a \xrightarrow{+} a$.

8.1 Résultats

- $\boxed{\text{Une relation à branchement fini est globalement finie si elle termine}}$

  Démonstration (par induction noethérienne) Soit $SD(a) = \{x \in A \mid a \longrightarrow x\}$.

  Soit $S(a) = \{x \in A \mid a \xrightarrow{+} x\}$.
  Considérons la propriété «$S(a)$ est fini».
  Supposons que pour tout b tel $a \longrightarrow b$ on ait «$S(b)$ est fini», donc puisque

  $$S(a) = \bigcup_{b \in SD(a)} S(b) \cup SD(a)$$

  $S(a)$ qui est une réunion finie d'ensembles finis est finie.
  En application de $(\mathcal{IN})$, pour tout $a \in A$, «$S(a)$ est fini».

- $\boxed{\text{Une relation acyclique termine si elle est globalement finie.}}$

  Démonstration (par l'absurde) Soit $\longrightarrow$ une relation acyclique.
  Supposons qu' elle ne termine pas, alors il existe une suite
  $x_0 \longrightarrow x_1 \longrightarrow \dots x_n \longrightarrow x_{n+1} \cdots$
  Puisque la relation est acyclique, les éléments sont tous différents.
  Donc $S(x_0)$ est infini et la relation n'est pas globalement finie.

9 Lemme de Koenig

Résultat :

$\boxed{\text{Un arbre à branchement fini est infini si et seulement si il contient un chemin infini.}}$

Prouver la terminaison

10 La suite de Goodstein

Considérons la décomposition en base k d'un nombre.
Ainsi la décomposition en base 3 de 93 est $3^{3+1} + 3^2 + 3$.
Soit deux nombres n et k, on pose $n_k = n$.
On passe de n_k à n_{k+1} de la façon suivante : on pose $m_k = n_k - 1$. Dans la décomposition en base k de m_k on remplace toutes les occurrences de k par $k+1$, on obtient n_{k+1}.
Ainsi si $n_2 = 15$ alors $m_2 = 14 = 2^{2+1} + 2^2 + 2$
$n_3 = 3^{3+1} + 3^3 + 3 = 93$,
$n_4 = 4^{4+1} + 4^4 + 2 = 1282$,
$n_5 = 5^{5+1} + 5^5 + 1 = 18751$,
$n_6 = 6^{6+1} + 6^6 = 326592$,
$n_7 = 7^{7+1} + ...$,

$\vdots$

$n_{40000} = 40000^{40000+1} + ...$

$\vdots$

Le processus termine, il existe un entier p tel que $n_p = 0$ La preuve n'utilise pas l'arithmétique classique.

11 Les fonctions croissantes

Soit $(A, \longrightarrow)$

On connaît $(B, >)$ est noethérien et $\varphi : A \mapsto B$ telle que $x \longrightarrow y$ implique $\varphi(x) > \varphi(y)$.

Le plus souvent on prend $(B, >)$=$(\mathbb{N}, >)$.

THÉORÈME

$\boxed{\text{Une relation à branchement fini termine si et seulement si elle est plongeable dans } \mathbb{N}.}$

12 Composition lexicographique

12.1 Composition lexicographique de deux ordres

Soient deux ordres $(A_1, >_1)$ et $(A_2, >_2)$.

On définit l'ordre $>_1 \times_{lex} >_2$ sur $A_1 \times A_2$, par

$(a_1, a_2) \quad >_1 \times_{lex} >_2 \quad (b_1, b_2)$ ssi

- $a_1 >_1 b_1$
- ou $a_1 =_1 b_1$ et $a_2 >_2 b_2$.

RÉSULTAT

$\boxed{\text{Si } >_1 \text{ et } >_2 \text{ terminent alors } >_1 \times_{lex} >_2 \text{ terminent.}}$

12.2 Composition lexicographique de n ordres

Soient $(A_n, >_n)$, ..., $(A_1, >_1)$, $(A_0, >_0)$ des ordres.

Soit $\mathbf{A}_{n+1} = A_{n+1} \times \mathbf{A}_n$

et $\mathbf{A}_0 = A_0$.

On définit l'ordre $>_n^{lex}$ sur $\mathbf{A}_n$ ainsi :

- $>_0^{lex}$ est $>_0$,
- Si $(x, \mathbf{x}), (y, \mathbf{y}) \in A_{n+1} \times \mathbf{A}_n$, alors $(x, \mathbf{x}) >_{n+1}^{lex} (y, \mathbf{y})$ ssi
  - $x >_{n+1} y$,
  - ou $x = y$ et $\mathbf{x} >_n^{lex} \mathbf{y}$.

RÉSULTAT

$\boxed{\text{Si les ordres } (A_n, >_n), \ldots, (A_1, >_1), (A_0, >_0) \text{ terminent alors } (\mathbf{A}_n, >_n^{lex}) \text{ termine}}$

12.3 Ordres stricts et lexicographie

Un ordre strict est une relation transitive et irréflexive.

RÉSULTAT : $\boxed{\text{Si les ordres } (A_n, >_n), \ldots, (A_1, >_1), (A_0, >_0) \text{ sont stricts alors } (\mathbf{A}_n, >_n^{lex}) \text{ est strict.}}$

12.4 Attention à la lexicographie !

La composition lexicographique se fait sur des relations et peut donner des résultats surprenants.

Sur $\mathbb{N} \times \mathbb{N}$,

$\geq_{\mathbb{N}} \times_{lex} \geq_{\mathbb{N}} \;\equiv\; \geq_{\mathbb{N}} \times_{lex} \mathbf{U}$

où $\mathbf{U}$ est la relation universelle $\{(x, y) \mid x \in \mathbb{N} \;\&\; y \in \mathbb{N}\}$.

FAIT :

Pour tous m, n, p, on a donc $(m, n) \geq_{\mathbb{N}} \times_{lex} \geq_{\mathbb{N}} (m, p)$.

12.5 Produit lexicographique d'ordres

Pour définir le produit lexicographique d'ordres on définit

1. le produit lexicographique de leur partie stricte[1],
2. la clôture réflexive de ce produit,

ou encore directement

$$(x, y) \geq_{A\times B} (x', y') \qquad \text{ssi} \qquad (x >_A y) \vee (x = x' \;\&\; y \geq_B y').$$

13 Multiensemble

13.1 Définitions

- Un multiensemble M sur A est une fonction $M : A \to \mathbb{N}$.
  Intuitivement : on peut s'imaginer qu'il s'agit d'«ensembles» où la répétition d'éléments est autorisée, $M(x)$ est le nombre de répétitions de x dans M.
- Un multiensemble est fini si $\{x \in A \mid M(x) \neq 0\}$ est fini.
- On note $\mathcal{M}(A)$ l'ensemble des multiensembles finis sur A.
- La notation standard est $\{a, a, b\}$, pour $\{a \mapsto 2, b \mapsto 1, c \mapsto 0\}$.

13.2 Opérations sur les multiensembles

$x \in M$ ssi $M(x) > 0$
$M \supseteq N$ ssi $(\forall x \in A) M(x) \leq N(x)$
$(M \cup N)(x) = M(x) + N(x)$
$(M - N)(x) = M(x) \dot{-} N(x)$ où $m \dot{-} n = max(m - n, 0)$.

[1] la partie stricte de $\geq$ est l'ordre défini par $x > y$ ssi $x \geq y \;\&\; x \neq y$

Dans la suite, on prend des multi-ensembles *finis*.

13.3 Ordre multiensemble

Soit $>$ un ordre strict sur A.
L'extension multiensemble $>_{mult}$ sur $M(A)$ est définie par

$M >_{mult} N$ ssi

il existe X et Y tels que
- $\emptyset \neq X \subseteq M$ et
- $N = (M - X) \cup Y$ et
- $(\forall y \in Y)(\exists x \in X) x > y$

13.4 Propriété de l'ordre multiensemble I

Résultat :

$\boxed{\text{Si } > \text{ est strict sur A, alors } >_{mult} \text{ est strict sur M(A).}}$

Démonstration :

1. irréflexivité facile .
2. transitivité facile.

13.5 Propriété de l'ordre multiensemble II

Résultat :

$\boxed{\text{Si } > \text{ termine, alors } >_{mult} \text{ termine.}}$

Démonstration

- Puisque A est plongé dans $\mathcal{M}(A)$ par $a \mapsto \{a\}$, clairement la terminaison sur $\mathcal{M}(A)$ implique celle sur A.
- Réciproquement, supposons que $>_{mult}$ ne termine pas sur $\mathcal{M}(A)$. Alors il existe une suite infinie décroissante de multiensembles.

$$M_0 >_{mult} M_1 >_{mult} ...M_n >_{mult} M_{n+1}$$

On veut construire un arbre étiqueté qui contredit le lemme de Koenig, à savoir :
- infini,
- à branchement fini,
- tous ses chemins sont finis.

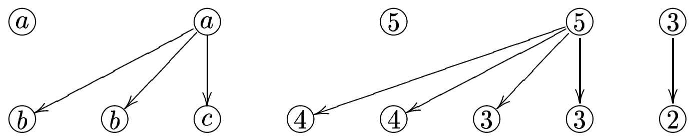
On construit l'arbre par niveau. On peut aussi dire que l'on a une canopée croissante qui tend vers l'infini (pour faire décroître l'effet de serre).
Au niveau -1, on met un élément arbitraire que l'on relie à des noeuds étiquetés par des éléments de M_0.

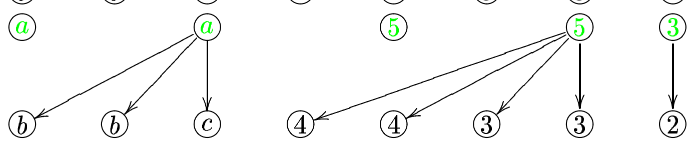
Au niveau n, on trouve des noeuds étiquetés par les éléments de M_n.
Les noeuds du niveau $n+1$ sont

- les noeuds étiquetés par les éléments de M_n inchangés,
- moins ceux étiquetés par les éléments du X_n utilisés,
- plus ceux étiquetés par les éléments du Y_n utilisé, c-à-d le nouveaux venus dans M_{n+1}.

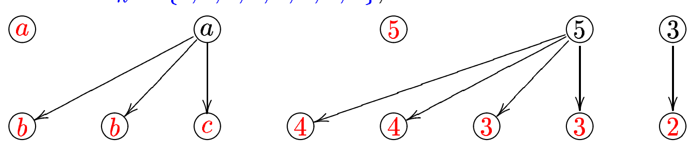
Par exemple : Soit

- $M_n = \{a, a, 5, 5, 3\}$
- $M_{n+1} = \{a, b, b, c, 5, 4, 4, 3, 3, 2\}$,
- $X_n = \{a, 5, 3\}$,
- $Y_n = \{b, b, c, 4, 4, 3, 3, 2\}$,





- $M_n = \{a, a, 5, 5, 3\}$
- $M_{n+1} = \{a, b, b, c, 5, 4, 4, 3, 3, 2\}$,
- $X_n = \{a, 5, 3\}$,
- $Y_n = \{b, b, c, 4, 4, 3, 3, 2\}$,



- $M_n = \{a, a, 5, 5, 3\}$
- $M_{n+1} = \{a, b, b, c, 5, 4, 4, 3, 3, 2\}$,
- $X_n = \{a, 5, 3\}$,
- $Y_n = \{b, b, c, 4, 4, 3, 3, 2\}$,

Le cas où $Y_n = \emptyset$ ne peut pas arriver une infinité de fois car, les M_n étant finis, cela serait contradictoire avec le fait que la suite est infinie.
Donc il y a une infinité d'étapes où l'on ajoute vraiment de nouveaux noeuds. Donc l'arbre est infini.
La construction montre que l'arbre est à branchement fini.
Les etiquettes sur un chemin forme une suite decroissante d'éléments de A. Comme $(A, >)$ termine, il n'y a pas chemins infinis.

N.B.Je n'ai pas utilisé $(A_\perp, >_\perp)$ comme au cours du 23-01-01 et dans le All that.

14 Le lemme de Newman

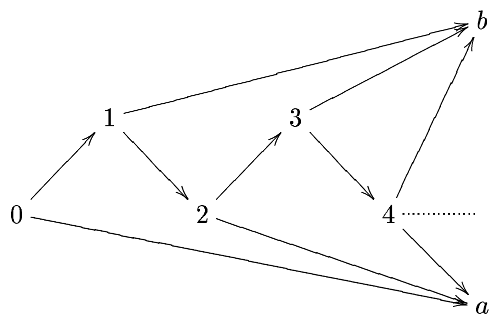
THÉORÈME :

$\boxed{\text{Si une relation termine et est localement confluente, alors elle est confluente.}}$

REMARQUE :

La terminaison est importante. Ces deux relations sont localement confluentes :

$$\begin{tikzcd} a & b \arrow[l] \arrow[r, bend left] & c \arrow[l, bend left] \arrow[r] & d \end{tikzcd}$$



14.1 Preuve du lemme de Newman

Démonstration

$$P(x) = (\forall y, z) y \xleftarrow{*} x \xrightarrow{*} z \Rightarrow y \downarrow z.$$

La confluence c'est $(\forall x) P(x)$.

$$\begin{tikzcd} x \arrow[r] \arrow[d] \arrow[dr, phantom, "CL"] & z_1 \arrow[r, "*"] \arrow[d, dotted, "*"] & z \arrow[dd, dotted, "*"] \\ y_1 \arrow[r, dotted, "*"] \arrow[d, "*"] \arrow[dr, phantom, "Ind"] & u \arrow[d, dotted, "*"] \arrow[r, phantom, "Ind"] & {} \\ y \arrow[r, dotted, "*"] & v \arrow[r, dotted, "*"] & w \end{tikzcd}$$

15 Forte confluence

Une relation est fortement confluente ssi

$$y_1 \longleftarrow x \longrightarrow y_2 \qquad \Rightarrow \qquad (\exists z) y_1 \xrightarrow{*} z \xleftarrow{=} y_2.$$

Résultat :

$\boxed{\text{Une relation fortement confluence est confluente.}}$

Démonstration : On prouve que si une relation est fortement confluence alors elle est semi-confluente. On fait une récurrence sur la longueur de la branche $\xrightarrow{*}$.

$$\begin{tikzcd}
\cdot \arrow[r] \arrow[d] \arrow[dr, phantom, "\mathrm{FC}"] & \cdot \arrow[r, "*"] \arrow[d, dotted, "="] & \cdot \\
\cdot \arrow[r, dotted, "*"] & \cdot &
\end{tikzcd}$$

Deux cas :

1. Cas $\xrightarrow{=} \; = \; \longrightarrow$.

$$\begin{tikzcd}
\cdot \arrow[r] \arrow[d] \arrow[dr, phantom, "\mathrm{FC}"] & \cdot \arrow[r, "*"] \arrow[d, dotted] \arrow[dr, phantom, "\mathrm{IND}"] & \cdot \arrow[d, dotted, "*"] \\
\cdot \arrow[r, dotted] & \cdot \arrow[r, dotted, "*"] & \cdot
\end{tikzcd}$$

2. Cas $\xrightarrow{=} \; = \; \xrightarrow{0}$.

$$\begin{tikzcd}
\cdot \arrow[r] \arrow[d] & \cdot \arrow[r, "*"] & \cdot \\
\cdot \arrow[ur, dotted, "*"] \arrow[ur, phantom, "\mathrm{FC}"'] & &
\end{tikzcd}$$

——————————————————-