Jeux de parité : algèbre, combinatoire

Luigi Santocanale

Laboratoire d'Informatique Fondamentale,
Centre de Mathématiques et Informatique,
39, rue Joliot-Curie - F-13453 Marseille

29 septembre 2004

Plan

Plan

Vérification des modèles

Tester les formules de la logique modale sur des systèmes de transition.

$\mathcal{S}$ système de transition, ϕ une formule logique :

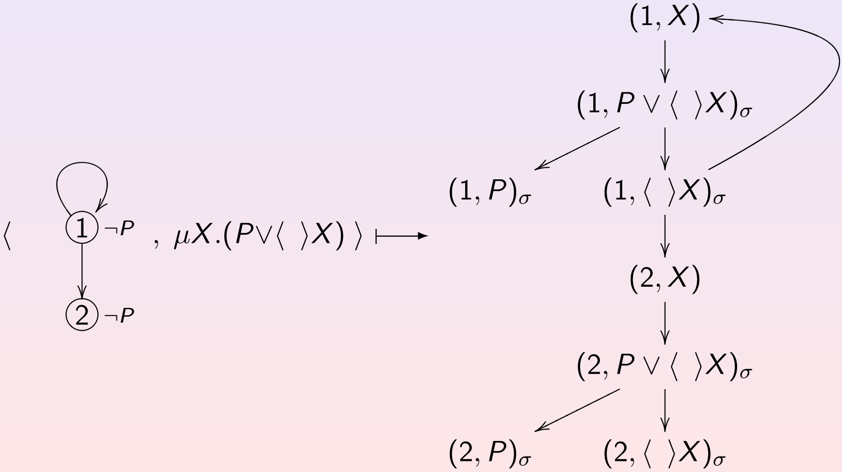
$$\langle\, \mathcal{S} \,,\, \phi \,\rangle \quad \longmapsto \quad \mathcal{G}(\mathcal{S}, \phi)$$

tel que

$$\text{Eva gagne dans } \mathcal{G}(\mathcal{S}, \phi) \qquad \text{ssi} \qquad \mathcal{S} \models \phi$$

"Model checking" se reduit au calculer des stratégies gagnantes.

Tester “tôt ou tard P”

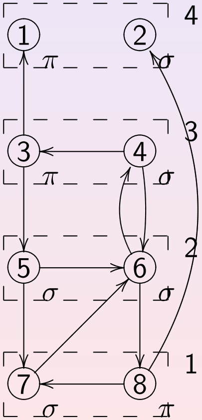


Petite variation

$$
\left\langle \quad
\begin{tikzcd}
1 \; \neg P \arrow[loop above] \arrow[d] \\
2 \; \neg P
\end{tikzcd}
\quad , \; \mu X.(P \vee [\;\,] X) \; \right\rangle
\longmapsto
\begin{tikzcd}
 & (1, X) \arrow[d] \\
 & (1, P \vee [\;\,] X)_\sigma \arrow[dl] \arrow[d] \\
(1, P)_\sigma & (1, [\;\,] X)_\pi \arrow[uu, bend right] \arrow[d] \\
 & (2, X) \arrow[d] \\
 & (2, P \vee [\;\,] X)_\sigma \arrow[dl] \arrow[d] \\
(2, P)_\sigma & (2, [\;\,] X)_\pi
\end{tikzcd}
$$

Plan

Exemple, définition



Un jeu de parité :

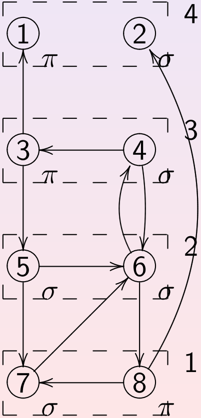
- Positions et mouvements.
- Deux joueurs : σ (Eva) et π (Adam).
- Positions partitionnées en régions : Eva gagne ssi

  la région d'hauteur maximale visitée infiniment souvent

  est pair (Eva = even = pair).

Le théorème fondamentale

Un jeu de parité . . .

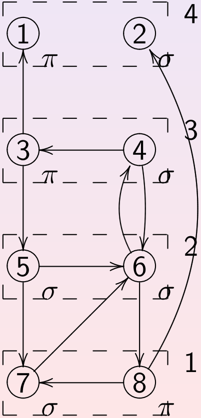


. . . son système d'equations logiques :

$$
\left\{
\begin{array}{lcl}
x_1 & = & \top \\
x_2 & = & \bot \\
\\
x_3 & = & x_1 \wedge x_5 \\
x_4 & = & x_3 \vee x_6 \\
\\
x_5 & = & x_6 \vee x_7 \\
x_6 & = & x_4 \vee x_8 \\
\\
x_7 & = & x_6 \\
x_8 & = & x_7 \wedge x_2
\end{array}
\right\}
$$

Le théorème fondamentale

Un jeu de parité . . .



. . . son système d'equations logiques :

$$
\left\{
\begin{array}{lcl}
x_1 & = & \top \\
x_2 & = & \bot \\
\\
x_3 & = & x_1 \wedge x_5 \\
x_4 & = & x_3 \vee x_6 \\
\\
x_5 & = & x_6 \vee x_7 \\
x_6 & = & x_4 \vee x_8 \\
\\
x_7 & = & x_6 \\
x_8 & = & x_7 \wedge x_2
\end{array}
\right\}
$$

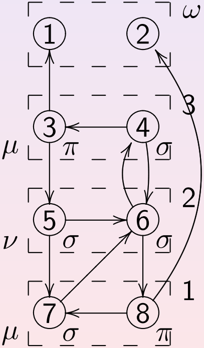
Theorem

Le joueur σ $(= Eva\ )$ a une stratégie gagnante de la position k ssi la solution du système pour x_k est $\top$.

Plan

Un jeu de parité généralisé . . .

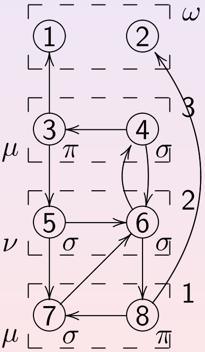
. . . est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Un jeu de parité généralisé ...

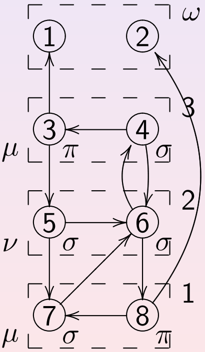
... est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Un jeu de parité généralisé . . .

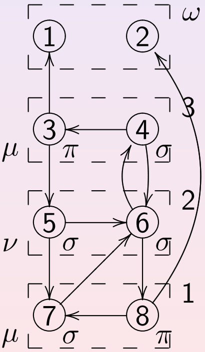
. . . est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Un jeu de parité généralisé ...

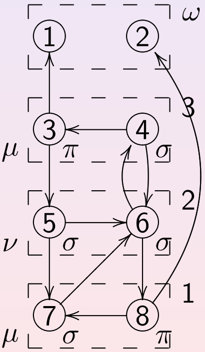
... est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Un jeu de parité généralisé ...

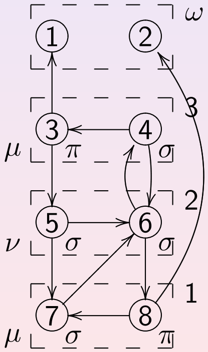
... est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Un jeu de parité généralisé ...

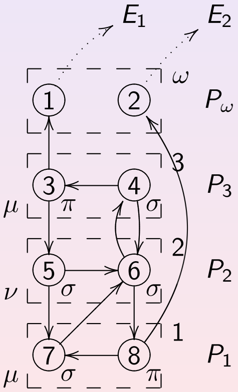
... est un tuplet $\langle P, M, \epsilon, \rho, \kappa \rangle$, où:



- $\langle P, M \rangle$ est un graphe de positions et mouvements.
- $\rho : P \longrightarrow \{1, \ldots, n, \omega\}$: les positions sont regroupées par hauteur (en régions),
- $\epsilon : \rho^{-1}(\{1, .., n\}) \longrightarrow \{\sigma, \pi\}$: les positions d'hauteur finie sont colorées par un joueur.
- On n'a pas de mouvements à partir d'une position d'hauteur inifinie.
- $\kappa : \{1, \ldots, n\} \longrightarrow \{\mu, \nu\}$: chaque region d'hauteur finie est colorée par μ ou ν.

Jeux parametrisés

G jeu de parité généralisé G, $E = \{E_p\}_{p \in P_\omega}$ collection d'ensembles

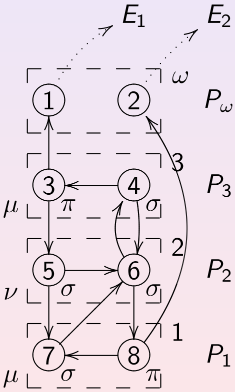


Le jeu $G(E)$:

- Deux joueurs σ, π doivent choisir un mouvement.
- De la position $p \in P_\omega$ le joueur σ doit choisir un element de E_p.
- Si un joueur doit choisir et il ne peut pas choisir, alors il perd.
- Une partie inifinie est gagnante pour σ ssi la région d'hauteur maximale visitée infiniment souvent est colorée par ν.

Jeux parametrisés

G jeu de parité généralisé G, $E = \{E_p\}_{p \in P_\omega}$ collection d'ensembles

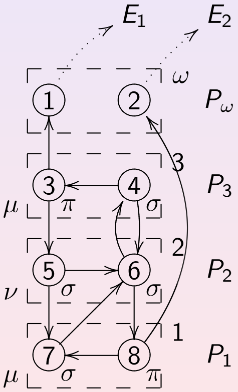


Le jeu $G(E)$:

- Deux joueurs σ, π doivent choisir un mouvement.
- De la position $p \in P_\omega$ le joueur σ doit choisir un element de E_p.
- Si un joueur doit choisir et il ne peut pas choisir, alors il perd.
- Une partie inifinie est gagnante pour σ ssi la région d'hauteur maximale visitée infiniment souvent est colorée par ν.

Jeux parametrisés

G jeu de parité généralisé G, $E = \{E_p\}_{p \in P_\omega}$ collection d'ensembles

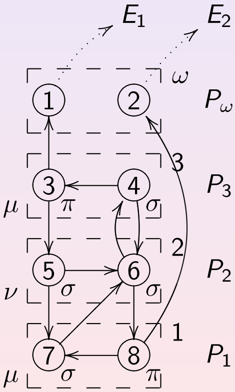


Le jeu $G(E)$:

- Deux joueurs σ, π doivent choisir un mouvement.
- De la position $p \in P_\omega$ le joueur σ doit choisir un element de E_p.
- Si un joueur doit choisir et il ne peut pas choisir, alors il perd.
- Une partie inifinie est gagnante pour σ ssi la région d'hauteur maximale visitée infiniment souvent est colorée par ν.

Jeux parametrisés

G jeu de parité généralisé G, $E = \{E_p\}_{p \in P_\omega}$ collection d'ensembles

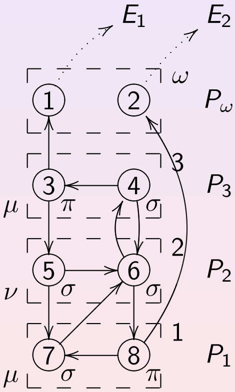


Le jeu $G(E)$:

- Deux joueurs σ, π doivent choisir un mouvement.
- De la position $p \in P_\omega$ le joueur σ doit choisir un element de E_p.
- Si un joueur doit choisir et il ne peut pas choisir, alors il perd.
- Une partie inifinie est gagnante pour σ ssi la région d'hauteur maximale visitée infiniment souvent est colorée par ν.

Jeux parametrisés

G jeu de parité généralisé G, $E = \{E_p\}_{p \in P_\omega}$ collection d'ensembles



Le jeu $G(E)$:

- Deux joueurs σ, π doivent choisir un mouvement.
- De la position $p \in P_\omega$ le joueur σ doit choisir un element de E_p.
- Si un joueur doit choisir et il ne peut pas choisir, alors il perd.
- Une partie inifinie est gagnante pour σ ssi la région d'hauteur maximale visitée infiniment souvent est colorée par ν.

Stratégies déterministes gagnantes

Pour toute collection $E = \{E_p\}_{p \in P_\omega}$ et toute position p définissons:

$$\mathcal{S}_{G,p}(E) \quad = \quad \text{l'ensemble des stratégies déterministes gagnantes pour le joueur } \sigma \text{ dans } G(E) \text{ de la position } p.$$

La correspondance $\mathcal{S}_{G,p}$ est définie aussi sur une collection de fonctions. C.-à.d.

$$\mathcal{S}_{G,p} : Set^{P_\omega} \longrightarrow Set$$

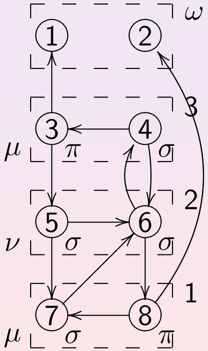
est une sorte de fonction monotone (=foncteur).

Soit $P_{\leq n} = P \setminus P_\omega$ et

$$\mathcal{S}_G(E) = \langle\, \mathcal{S}_{G,p}(E)\, \rangle_{p \in P_{\leq n}} : Set^{P_\omega} \longrightarrow Set^{P_{\leq n}}\,.$$

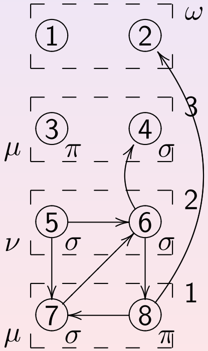
Le jeu prédécesseur $P(G)$

...défini en effaçant toute arète se départant de la région d'hauteur finie maximale:



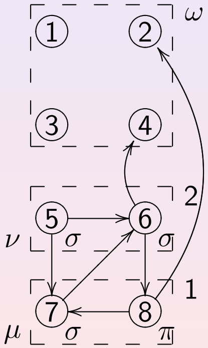
Le jeu prédécesseur $P(G)$

... défini en effaçant toute arète se départant de la région d'hauteur finie maximale:



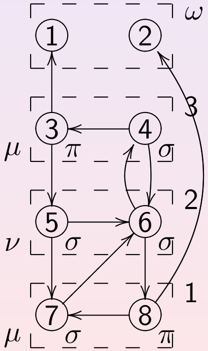
Le jeu prédécesseur $P(G)$

...défini en effaçant toute arète se départant de la région d'hauteur finie maximale:



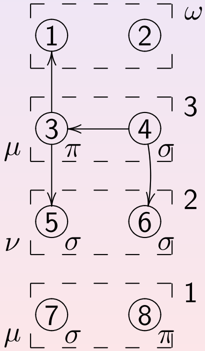
Le jeu "un seul coup" $O(G)$

…défini en effaçant toutes les arètes qui ne se départent pas de la region d'hauteur finie maximale:



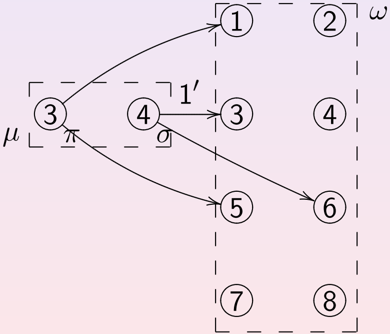
Le jeu "un seul coup" $O(G)$

...défini en effaçant toutes les arètes qui ne se départent pas de la region d'hauteur finie maximale:



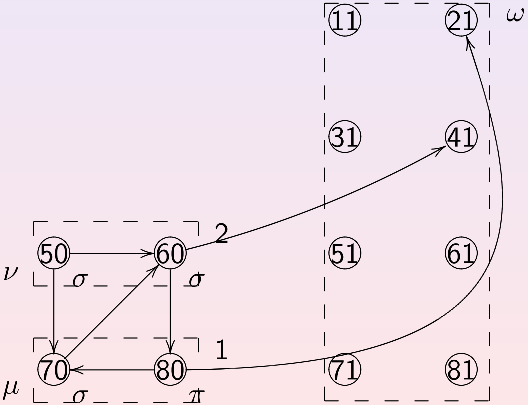
Le jeu "un seul coup" $O(G)$

...défini en effaçant toutes les arètes qui ne se départent pas de la region d'hauteur finie maximale:



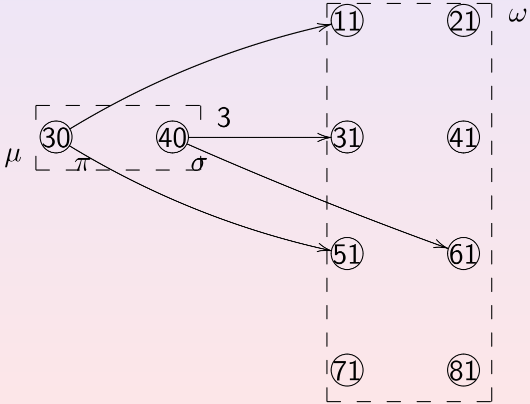
Le jeu "découpage des cycles" $D(G)$

...défini en recollant $P(G)$ et $O(G)$:



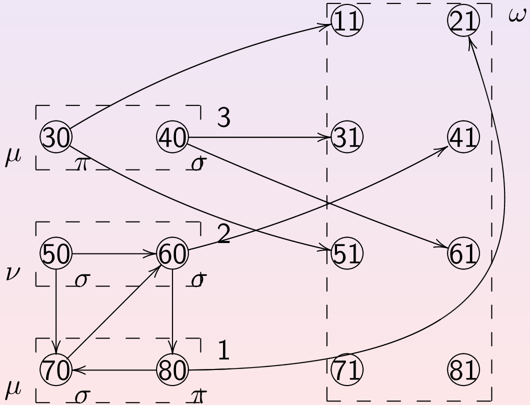
Le jeu "découpage des cycles" $D(G)$

. . . défini en recollant $P(G)$ et $O(G)$:

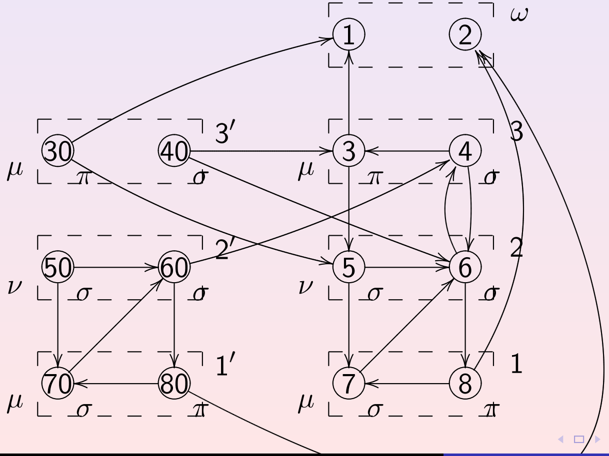


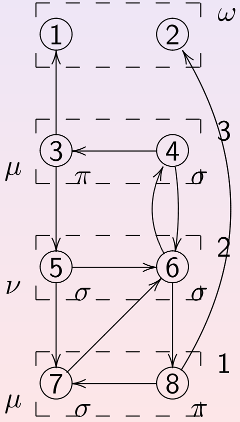
Le jeu "découpage des cycles" $D(G)$

...défini en recollant $P(G)$ et $O(G)$:



Construction/de-construction des stratégies gagnantes





Nous avons montré qu'il y a une bijection

$$\mathcal{S}_{D(G)}(\mathcal{S}_G(E), E) \longrightarrow \mathcal{S}_G(E)\,.$$

Theorem

$$\mathcal{S}_G = \begin{cases} \textit{plus petit point fixe de} \\ \qquad Set^{P_{\leq n}} \times Set^{P_\omega} \xrightarrow{\mathcal{S}_{D(G)}} Set^{P_{\leq n}} \\ \qquad\qquad \textit{si la couleur de } P_n \textit{ est } \mu. \\ \textit{plus grand point fixe de ce foncteur,} \\ \qquad\qquad \textit{si la couleur de } P_n \textit{ est } \nu. \end{cases}$$

Plan

PpPF d'un foncteur

Soit *Set* la catégorie des ensembles et

$$F : Set \longrightarrow Set$$

un foncteur.
Le Plus Petit Point Fixe de F est un couple $(F^\dagger, x)$ tel que:

$$\begin{tikzcd} F(F^\dagger) \arrow[d, "x"] \\ F^\dagger \end{tikzcd} \qquad \begin{tikzcd} F(F^\dagger) \arrow[r, "F(f)"] \arrow[d, "x"] & F(A) \arrow[d, "\alpha"] \\ F^\dagger \arrow[r, "\exists ! f"] & A \end{tikzcd}$$

Il est univoquement determinée à isomorphisme près.

PGPF d'un foncteur

Le Plus Grand Point Fixe de F est un couple $(F^\dagger, x)$ tel que:

$$
\begin{tikzcd}
F(F^\dagger) \\
F^\dagger \arrow[u, "x"]
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
F(F^\dagger) & F(A) \arrow[l, "F(f)"'] \\
F^\dagger \arrow[u, "x"] & A \arrow[l, "\exists! f"'] \arrow[u, "\alpha"']
\end{tikzcd}
$$

Meme type de definition pour les foncteurs

$$F :^n \longrightarrow {}^n$$

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Exemples

- $\mathbb{N}$ est le PpPF $F(X) = 1 + X$.
- Pour tout ensemble Y, $Y \times \mathbb{N}$ est le PpPF de $F(X) = Y + X$.
- $L(\Sigma)$ (c.à.d., les mots sur l'alphabet Σ) est le PpPF de $F(X) = 1 + (X \times \Sigma)$.
- Les ensembles définis par *induction* sont des algèbres initiaux pour quelque foncteur.
- $\mathbb{N} \cup \{\infty\}$ est le PGPF de $F(X) = 1 + X$.
- L'ensemble $\Sigma^{\mathbb{N}}$ des suites infinies (streams, flots) sur un alphabet Σ, est le PGPF de $F(X) = \Sigma \times X$.
- $B(\Sigma)$ (c.à.d., les arbres binaires infinis tels que chaque sommet est étiqueté par une lettre dans Σ) est la coalgèbre finale de $F(X) = \Sigma \times X \times X$.
- Les ensembles définis par *coinduction* sont des PGPF pour quelque foncteur.

Les ensembles inductifs implémentés (comme types inductifs) dans (presque) tout langage de programmation fonctionnel.

Les ensembles coinductifs implémentés (comme types coinductifs) dans le langage de programmation Charity et dans l'assistant de preuves Coq.

Tout ensemble inductif/coinductif construit par $\times, 1, +, \emptyset$ est de la forme

$$\text{stratégies gagnantes dans } G$$

pour quelque jeu de parité G.

Les ensembles inductifs implémentés (comme types inductifs) dans (presque) tout langage de programmation fonctionnel.

Les ensembles coinductifs implémentés (comme types coinductifs) dans le langage de programmation Charity et dans l'assistant de preuves Coq.

Tout ensemble inductif/coinductif construit par $\times, 1, +, \emptyset$ est de la forme

$$\text{stratégies gagnantes dans } G$$

pour quelque jeu de parité G.

Les ensembles inductifs implémentés (comme types inductifs) dans (presque) tout langage de programmation fonctionnel.

Les ensembles coinductifs implémentés (comme types coinductifs) dans le langage de programmation Charity et dans l'assistant de preuves Coq.

Tout ensemble inductif/coinductif construit par $\times, 1, +, \emptyset$ est de la forme

$$\text{stratégies gagnantes dans } G$$

pour quelque jeu de parité G.