Sur la structure rationnelle du calcul infini

Damian Niwiński, *Université de Varsovie*

exposé à l'occasion de la remise de la Médaille de Bronze du CNRS

à Igor Walukiewicz

Les idées mathématiques

rationnel	irrationnel
théorème fondamental de l'algèbre	insolubilité des équations d'ordre 5
continuité	fonction de Dirichlet
	courbe de Peano
	...
la mesure de Lebesgue	l'ensemble de Vitali
	la décomposition paradoxale de la boule
	$\bigcirc = \bigcirc + \bigcirc$ (Banach–Tarski)

En logique, calculabilité et complexité

rationnel	irrationnel
systèmes axiomatiques complets	incomplétude de l'arithmétique (Gödel)
machine universelle de Turing	indécidabilité d'arrêt
	théorème de Rice
	...
hiérarchies de complexité	théorème d'accélération de Blum
	...
NP-complétude	théorème de Ladner
	permanent
	...?

Jeux

rationnel

irrationnel

thm de Zermelo: les jeux finis à info

parfaite sont determinés

hex? échecs?

thm de von Neumann: les jeux probabilistes

sont determinés

thm de Martin: les jeux infinis boréliens

sont determinés

jeux indéterminés

thm de Gurevich–Harrington: les jeux rationnels

sont determinés à mémoire finie

Théorie de la définissabilité

rationnel	irrationnel
hiérarchie de Borel	contre-exemple de Suslin (1916):
	l'image continue d'un borelien
	peut ne pas l'être

Contre-exemple de Suslin,suite

$T \subseteq \omega^*$, un arbre, $u \in \omega^\omega$,

$$\{\langle T, u\rangle : u \text{ est une branche de } T\}$$

est une relation fermée, comme un sous-ensemble de

$$2^{\omega^*} \times \omega^\omega \approx \omega^\omega \times \omega^\omega \approx \omega^\omega.$$

Mais la projection

$$\{T : \text{ a une branche infinie }\}$$

n'est pas borélienne.

Les calculs infinis, ont-ils une structure rationnelle?

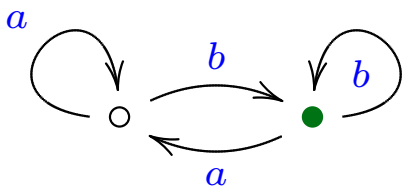
1960 — — —

Büchi, Rabin, McNaughton, Muller, Schupp, Nivat, Arnold, Courcelle, Emerson, Wagner, Mostowski, Thomas, Caucal, Janin, Walukiewicz, . . .

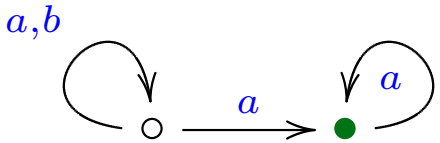
Automates de Büchi

$$\mathcal{A} = \langle \Sigma, Q, q_I, Tr, F \rangle$$

où $Tr \subseteq Q \times \Sigma \times Q$, $F \subseteq Q$.



$((a+b)^*b)^\omega$



$(a+b)^*a^\omega$

Le dernier n'est reconnu par aucun automate déterministe :

$$\xrightarrow{a}\xrightarrow{b}\xrightarrow{a}\xrightarrow{a}\xrightarrow{b}\xrightarrow{a}\xrightarrow{a}\xrightarrow{a}\xrightarrow{b}\xrightarrow{a}\xrightarrow{a}\xrightarrow{a}\xrightarrow{a}\xrightarrow{b}\xrightarrow{a} \ldots\ldots \xrightarrow{a}\xrightarrow{b}\xrightarrow{a} \ldots$$

Théorème de Büchi (1960)

En utilisant le théorème de Ramsey, Büchi a montré que ses automates sont clos par complément:

$$\mathcal{A} \mapsto \mathcal{B} \ : \ \overline{L(\mathcal{A})} = L(\mathcal{B})$$

Il est facile de voir qu'ils sont aussi clos par union et projection.

La théorie monadique du second ordre de $\langle \omega, \leq \rangle$ est décidable.

Beaucoup de problèmes de vérification des systèmes informatiques non-déterministes se ramènent à l'analyse des automates de Büchi.

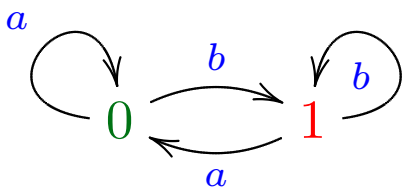
A noter que le problème de vacuité est décidable en temps polynomial.

Automates de parité

Théorème de McNaughton (1966)

Un automate non-déterministe de Büchi peut être simulé par un automate déterministe avec une condition *rank* : $Q \to \{0, 1, \ldots, n\}$

$\limsup_{i \to \infty} \mathit{rank}(q_i)$ est pair



$(a+b)^* a^\omega$

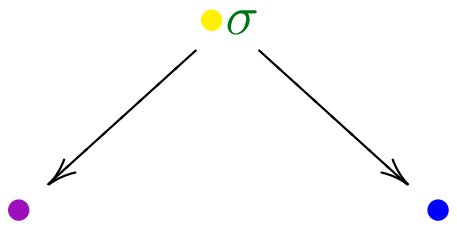
L'automate déterministe minimal n'est pas unique, mais l'index minimal n peut être calculé.

Automates d'arbres

Pour l'analyse de systèmes interactifs, ils sont mieux adaptés que les automates de mots.

$$\mathcal{A} = \langle \Sigma, Q, q_I, Tr, \mathit{rank}, \rangle$$

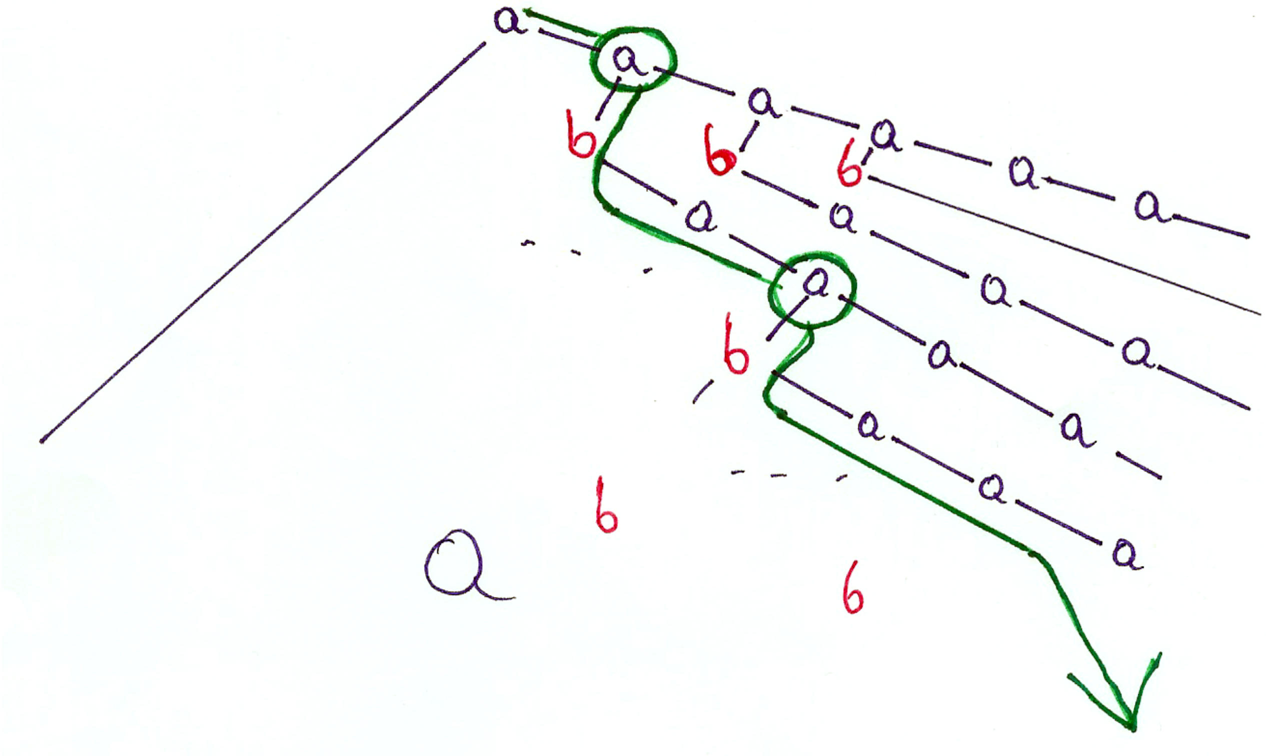
où $Tr \subseteq Q \times \Sigma \times Q \times Q$, $\mathit{rank} : Q \to \{0, 1, \ldots, n\}$.



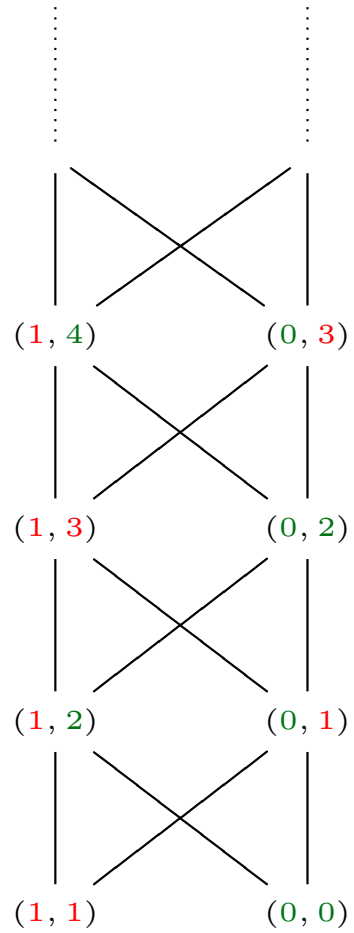
Par exemple $\{q/p \xrightarrow{a} (q, q),\ \ q/p \xrightarrow{b} (p, p)\}$, $\mathit{rank}(q) = 0$, $\mathit{rank}(p) = 1$ reconnait l'ensemble des arbres tels que sur chaque branche, b n'apparaît qu'un nombre fini de fois.

La condition de Büchi, même en présence de non-déterminisme, ne suffit pas.

Le contre-exemple de Suslin 1916 retrouvé.



L'indice de Mostowski



Hiérarchie stricte (N 1986 non-déterministe; Bradfield, Arnold 1999, alternante).

L'indice est calculable pour les automates déterministes (N & Walukiewicz 2004).

Théorème *de l'arbre* de Rabin (1969)

La théorie monadique de l'arbre $\langle \{l, r\}^*, \leq \rangle$ est décidable.

Un grand nombre d'applications.

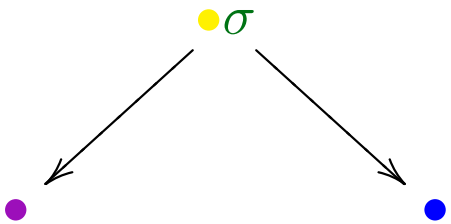
La preuve du lemme de complément est extrémement difficile.

Historique des preuves

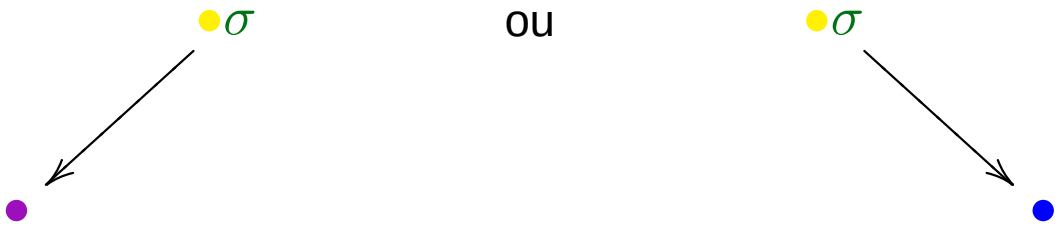
Rabin 1969	les ordinaux
Gurevich & Harrington 1982	jeux à mémoire finie
Muchnik 1984	...
Mostowski 1991	jeux sans mémoire
Emerson & Jutla 1991	$+$ μ-calcul
Arnold 1995	...
Walukiewicz 1996*	$+$ signatures

Jeux de Gurevich & Harrington

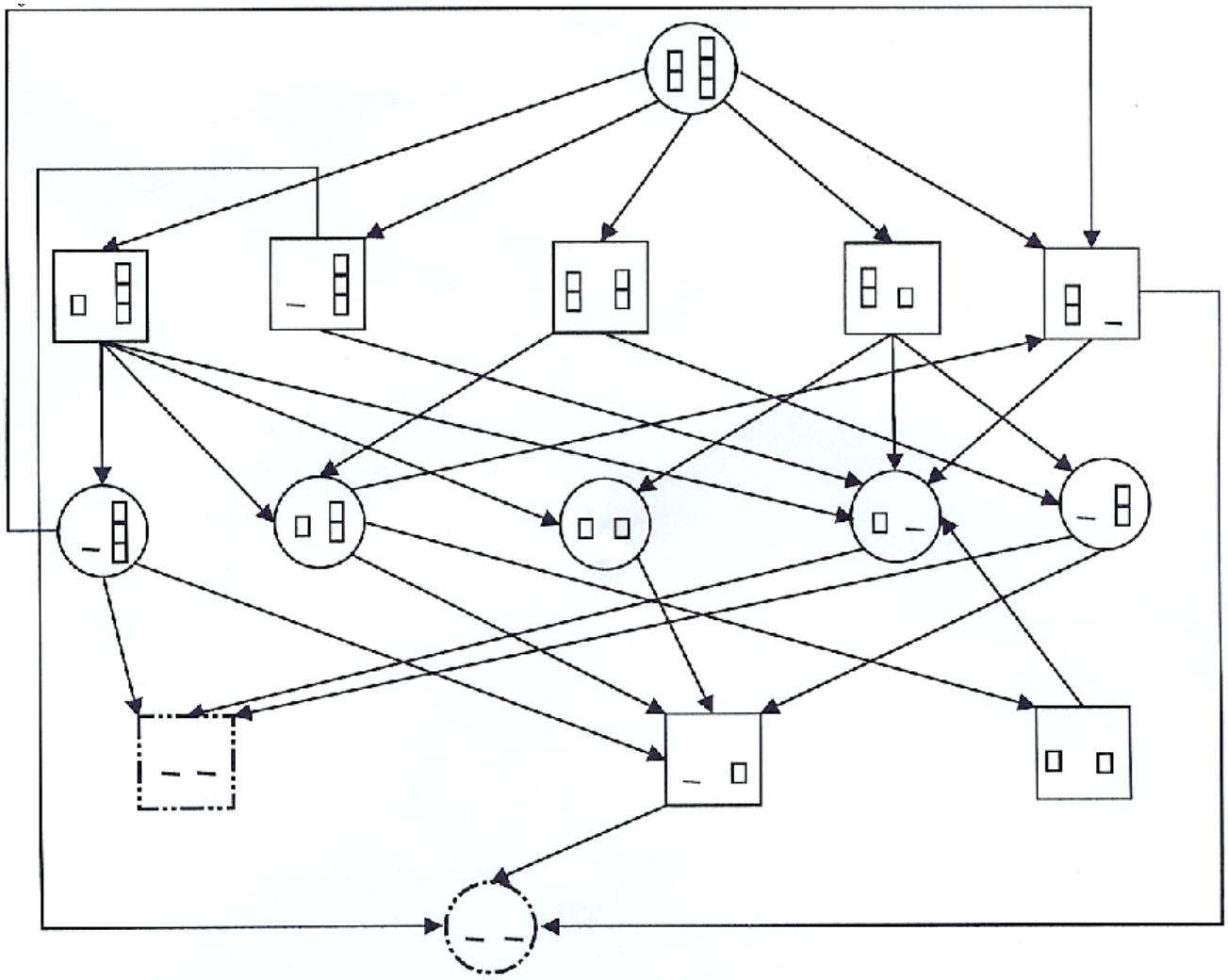
Automate :



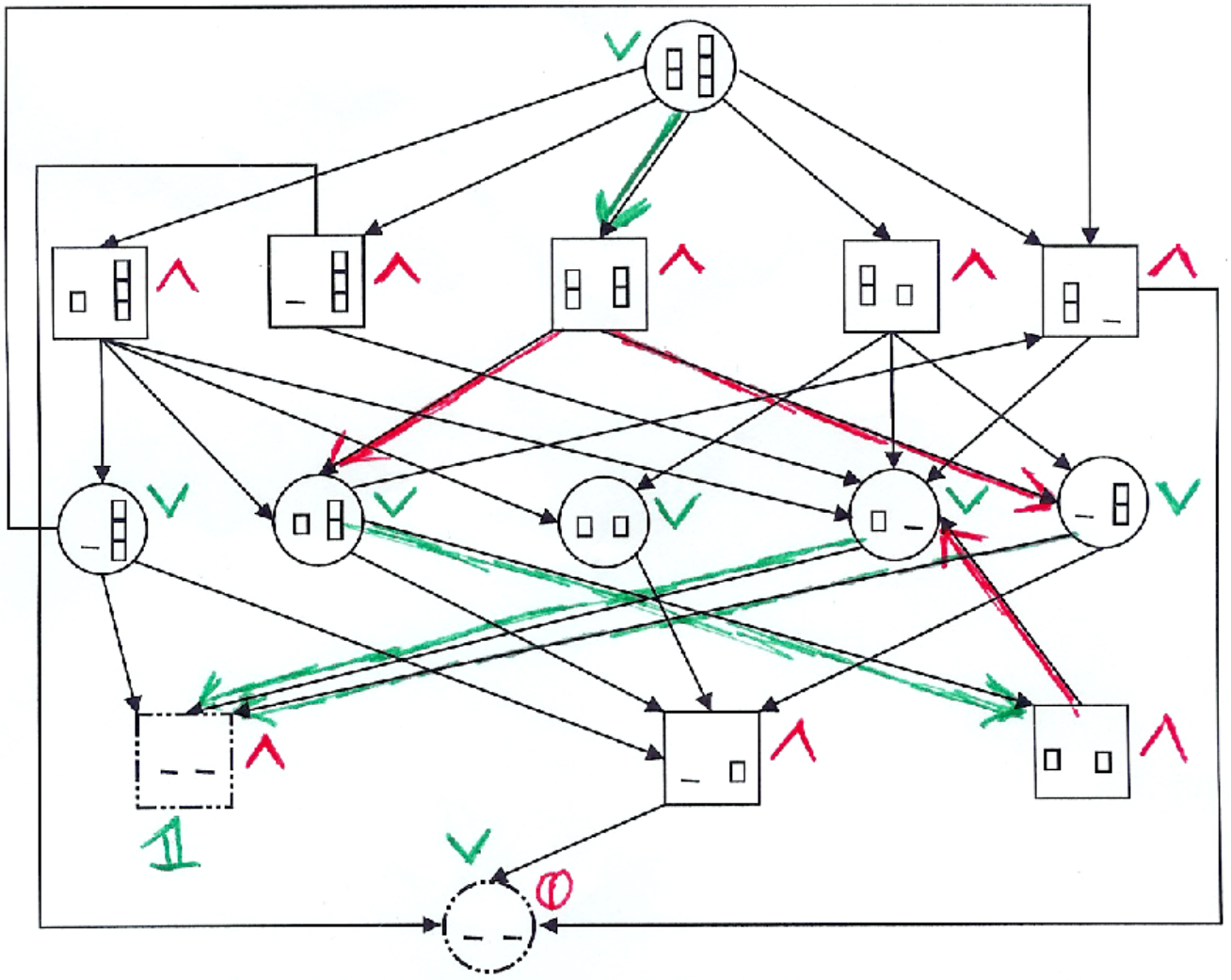
Pathfinder :



Graphe d’un jeu



Stratégie gagnante



Le μ-calcul au travers des jeux

$V = V_e \dot\cup V_a, \qquad \rightarrow \subseteq V \times V,$

$\mathit{rank} : V \rightarrow \omega \qquad Win_e \subseteq \omega^\omega$

Hypothèse naturelle : $Win_e = \omega\, Win_e$.

Une partie infinie $v_0 \rightarrow v_1 \rightarrow v_2 \rightarrow \ldots$ est gagnée par Eva si

$$(\mathit{rank}(v_0)\, \mathit{rank}(v_1)\, \mathit{rank}(v_2) \ldots) \in Win_e$$

L'équation de jeu :

$$X = (E \cap \Diamond X) \cup (A \cap \Box X)$$

où $E = V_e \qquad \Diamond X = \{v : (\exists v')\,(v \rightarrow v') \text{ et } v' \in X\}$

$A = V_a \qquad \Box Y = \{v : (\forall v')\,(v \rightarrow v') \Rightarrow v' \in Y\}$

Le μ-calcul au travers des jeux, suite

Si W_e est l'ensemble des positions gagnantes pour Eva, alors

$$W_e = \underbrace{(E \cap \Diamond W_e) \cup (A \cap \Box W_e)}_{Eva(W_e)}$$

En particulier,

$$\mu X.Eva(X) \subseteq W_e \subseteq \nu X.Eva(X)$$

Le dual pour Adam.

Mais si le graphe de jeu n'a pas de boucle, nous avons

$$\mu X.Eva(X) = \overline{\mu X.Adam(X)}$$

Théorème de Zermelo (1913): Les jeux finis sont déterminés.

Les stratégies gagnantes sont positionnelles.

Jeux de Büchi (*de répétition*)

Dans un jeu *de persistence*, où Eva gagne toute partie infinie, la stratégie "rester dans $\nu X.Eva(X)$" est gagnante pour Eva, d'où

$$W_e = \nu X.Eva(X) = \overline{\mu X.Adam(X)}.$$

Ces jeux sont donc aussi positionnellement determinés.

Dans les jeux de Büchi, $Win_e = (1^*2)^\omega$

$$W_e = \nu Y.\mu X.(E_1 \cap \Diamond X) \cup (E_2 \cap \Diamond Y) \cup (A_1 \cap \Box X) \cup (A_2 \cap \Box Y)$$

$$W_a = \mu Y.\nu X.(E_1 \cap \Box X) \cup (E_2 \cap \Box Y) \cup (A_1 \cap \Diamond X) \cup (A_2 \cap \Diamond Y)$$

Jeux de parité

$$\{0,1,\ldots,n\}^\omega \supseteq Win_e = \{u : \limsup_{i\to\infty} \mathit{rank}(u_i) \text{ est pair}\}$$

Le vainqueur est déterminé par :

$$W_e = \vartheta X_n \ldots \nu X_2 . \ldots \mu X_1 . \nu X_0 . \bigcup_i (E_i \cap \Diamond X) \cup \bigcup_i (A_i \cap \Box Y)$$

$$W_a = \bar{\vartheta} X_n \ldots \mu X_2 . \ldots \nu X_1 . \mu X_0 . \bigcup_i (E_i \cap \Box X) \cup \bigcup_i (A_i \cap \Diamond Y)$$

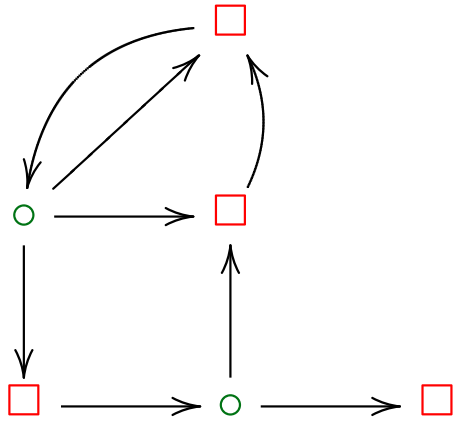
Emerson & Jutla 1991, Mostowski 1991

Walukiewicz 1995: la structure des stratégies gagnantes

La structure des stratégies gagnantes, suite

Pour $v \in \mu X.Eva(X)$,

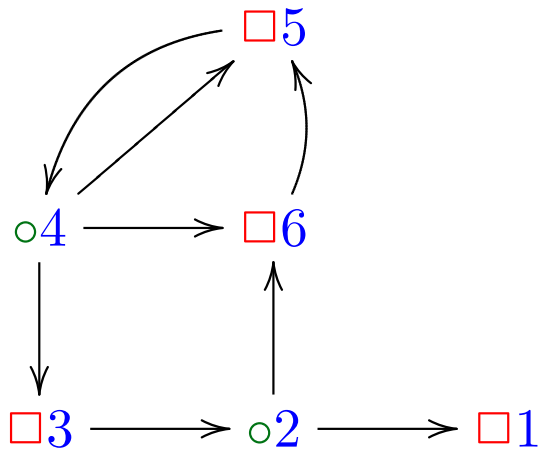
$$\mathsf{ord}(v) = \mathsf{min}\{\xi : v \in Eva^{\xi}(\emptyset)\}$$



La structure des stratégies gagnantes, suite

Pour $v \in \mu X.Eva(X)$,

$$\text{ord}(v) = \min\{\xi : v \in Eva^{\xi}(\emptyset)\}$$



Stratégie: faire décroître ord(v).

Pour $v \in \mu X_n \ldots \nu X_2 \ldots \mu X_1 . \nu X_0 .\, Eva(X_0, X_1, \ldots, X_n)$,

$$\text{ord}(v) \quad = \quad \langle \alpha_n, \alpha_{n-2}, \ldots, \alpha_3, \alpha_1 \rangle$$

où

$$Eva_i(X_{i+1}, \ldots, X_n) = \vartheta X_i \ldots \nu X_2 \ldots \mu X_1 . \nu X_0 .\, Eva$$

Pour i impair, $\alpha_i = \min\{\xi : v \in Eva^{\xi}(\emptyset)\}$

$$U_i = Eva_{i-1}^{\alpha_i}(\emptyset, U_{i+1}, \ldots, U_n)$$

Pour i pair, $U_i = Eva_i(U_{i+1}, \ldots, U_n)$

Stratégie: faire décroître $\text{ord}(v)$.

Ainsi les jeux de parité sont devenus une technique très puissante pour construire des algorithmes pour les problèmes logiques, notamment de *model checking*.

Les applications abondent. . .

Logique du jour . . . ?

- logique du second ordre monadique (MSO)
- le μ-calcul L μ
- logiques temporelles LTL, CTL, CTL*
- logiques dynamiques PDL, PDL Δ, logique algorithmique
- . . . ?

$$\mathcal{M} \models \varphi$$

— capacité de discernement

— facilité algorithmique

μ-calcul vs. logique monadique

Walukiewicz 1996 $L\mu \equiv$ MSO, si un modèle est un arbre

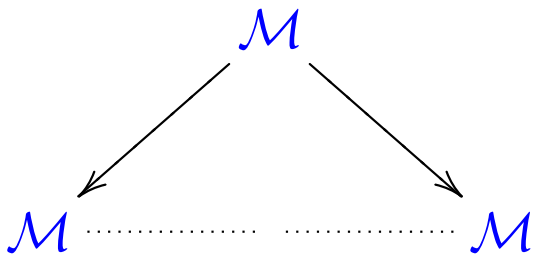
van Benthem 1991 FO $\equiv$ ML , pour des propriétés closes par bissimulation

Janin & Walukiewicz 1996 $L\mu \equiv$ MSO, pour des propriétés closes par bissimulation (ce qui est le cas pour les propriétés temporelles de programmes)

Décidabilité de MSO sur les structures arborescentes

Pour une structure logique $\mathcal{M} = \langle D, r, \ldots \rangle$, on forme la structure $\mathcal{M}^* = \langle D^*, son, cl, r^*, \ldots \rangle$, où

$son(w, wd)$, $cl(wdd)$, $r^*(wd_1, \ldots, wd_k)$ ssi $r(d_1, \ldots, d_k)$.



Walukiewicz 1996: La théorie MSO($\mathcal{M}^*$) se réduit à MSO($\mathcal{M}$).

En particulier, elle est décidable si MSO($\mathcal{M}$) l'est.

Exemple

$\langle \omega, succ, square \rangle$ interprété dans $\langle \omega^*, son, cl, succ^* \rangle$

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

0, 1 2 3 4 5 6 7 8 9 . . .

. . .

Autres applications

Courcelle & Walukiewicz 1998 : La théorie MSO d'un développement arborescent d'un graphe se réduit à la théorie MSO de ce graphe.

Walukiewicz 1996 : Le problème de *model checking* pour Lμ dans les graphes de transitions des automates à pile est décidable dans EXPTIME.

Une stratégie gagnante peut elle–même être engendrée par un automate à pile.

Arnold, Vincent, Walukiewicz 2003 : Synthèse de controleurs.

Logique du premier ordre gardée

Peut–on trouver une logique ML $\subseteq$????? $\subseteq$ FO , plus forte que ML , mais avec des propriétés aussi bonnes (décidabilité efficace, modèle fini)?

Andréka, van Benthem, Németi 1996, suivant la traduction ML $\rightsquigarrow$ FO

$$\Diamond \varphi \quad \rightsquigarrow \quad \exists y\, \alpha(x,y) \wedge \varphi'(y)$$
$$\Box \varphi \quad \rightsquigarrow \quad \forall y\, \alpha(x,y) \rightarrow \varphi'(y)$$

ont proposé le fragment gardé (GF) de FO :

$$\exists \mathbf{y} \alpha(\mathbf{x},\mathbf{y}) \wedge \psi(\mathbf{x},\mathbf{y})$$

$$\forall \mathbf{y} \alpha(\mathbf{x},\mathbf{y}) \rightarrow \psi(\mathbf{x},\mathbf{y})$$

où *free*(ψ) $\subseteq$ *free* (α) = $\{\mathbf{x},\mathbf{y}\}$.

Logique du premier ordre gardée, suite

Andréka, van Benthem, Németi 1996 : GF est décidable (en 2EXPTIME).

Grädel 1999: GF satisfait la propriété de modèle fini, et de modèle arborescent.

Grädel & Walukiewicz 1999 : L'extension de GF par μ et ν,

μ-GF

est elle même décidable en 2EXPTIME.

μ-GF est une logique d'une grande puissance. Elle admet des axiomes d'infinité, mais garde la propriété de modèle arborescent.

Système de preuve pour le μ-calcul

Kozen 1982 a proposé le système suivant :

l'axiomatisation de la logique modale K

$$\alpha(\mu X.\alpha(X)) \Rightarrow \mu X.\alpha(X)$$

$$\frac{\alpha(\varphi) \Rightarrow \varphi}{\mu X.\alpha \Rightarrow \varphi}$$

ce qui exprime le principe de Tarski :

$$\mu X.f(X) = \bigwedge\{d : f(d) \leq d\}$$

Système de preuve pour le μ-calcul, suite

Walukiewicz 1995, 2000 :

Théorème de complétude du système de Kozen

$$\vdash \varphi \iff \models \varphi$$

Qui simplifiera la preuve. . . ?

Théorèmes de complétude et leurs méthodes

premier ordre	Gödel 1929	modèle de constantes
	Gentzen 1934	
	Henkin 1949	
premier ordre intuitioniste	Rasiowa 1951	topologie
logique dynamique (PDL)	Gabbay 1977,Parikh 1978	filtration
L μ	Walukiewicz 1995	automates et jeux

Conclusion

rationnel	irrationnel
complétude de L μ	
décidabilité robuste de *model checking*	
décidabilité de MSO($\mathcal{M}^*$)	
méthode de jeux	complexité?
	...?