Théorie monadique des représentations . . .

David Janin (Bordeaux)

joint work with Anuj Dawar (Cambridge)

Réunion ACI Sécurité (VERSYDIS)

Théorie monadique des représentations finies de mots ultimement périodiques

David Janin (Bordeaux)

joint work with Anuj Dawar (Cambridge)

Réunion ACI Sécurité (VERSYDIS)

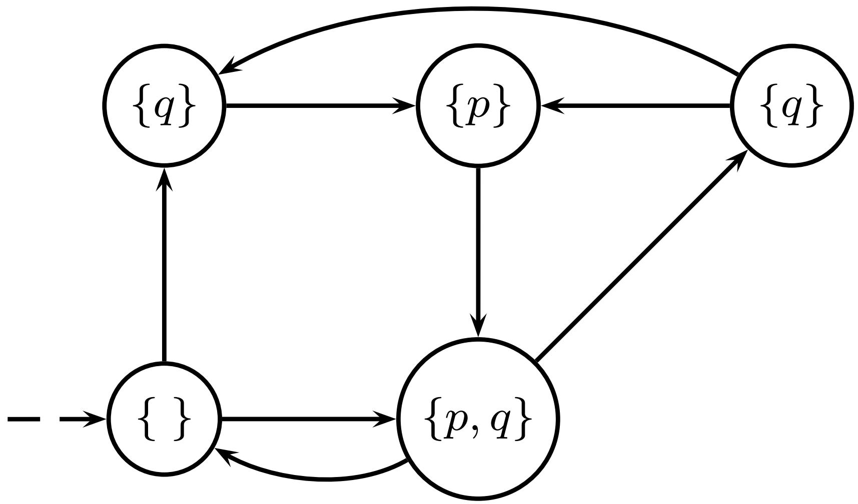
Models and Logic

Models: directed Σ-labeled graph with distinguished source

$$M = \langle V, E \subseteq V \times V, s \in V, \lambda : V \longrightarrow \Sigma = \mathcal{P}(\textbf{\textit{Prop}}) \rangle$$

Models: directed Σ-labeled graph with distinguished source

$$M = \langle V, E \subseteq V \times V, s \in V, \lambda : V \to \Sigma = \mathcal{P}(\textbf{\textit{Prop}}) \rangle$$



Models: directed Σ-labeled graph with distinguished source

$$M = \langle V, E \subseteq V \times V, s \in V, \lambda : V \to \Sigma = \mathcal{P}(\textit{\textbf{Prop}}) \rangle$$

Logic: monadic second order logic on those graphs on signature $\{E\}$ (edges) and ***Prop*** (unary predicates).

Bisimulation invariance on the finite ?

Bisimulation invariance on the finite ?

Def: An MS-sentence is (counting) bisimulation invariant in the finite when it does not distinguish any two finite (counting) bisimilar graphs.

Bisimulation invariance on the finite ?

Def: An MS-sentence is (counting) bisimulation invariant in the finite when it does not distinguish any two finite (counting) bisimilar graphs.

Question: What MSO definable properties of finite graphs are bisimulation invariant over the finite ?

Bisimulation invariance on the finite ?

Def: An MS-sentence is (counting) bisimulation invariant in the finite when it does not distinguish any two finite (counting) bisimilar graphs.

Question: What MSO definable properties of finite graphs are bisimulation invariant over the finite ?

Remark: No results on a rbitrary models can be applied

Bisimulation invariance on the finite ?

Def: An MS-sentence is (counting) bisimulation invariant in the finite when it does not distinguish any two finite (counting) bisimilar graphs.

Question: What MSO definable properties of finite graphs are bisimulation invariant over the finite ?

Partial answers and other questions:

- At least all mu-calculus definable properties !
- Other PTime definable classes of graphs ?
- NPcomplete classes of graphs ?

Known result in the finite

Theorem [Rosen 90's]: The bisimulation invariant fragment of FO on the finite equals modal logic.

Simplifying the problem. . .

Question 1: What about bisimulation invariant monadic Σ_1 in the finite ?

Simplifying the problem. . .

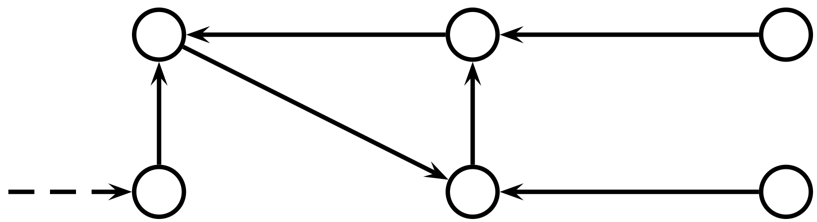
Question 1: What about bisimulation invariant monadic Σ_1 in the finite ?

Question 2: What about bisimulation invariant monadic Σ_1 on finite unary graphs ?

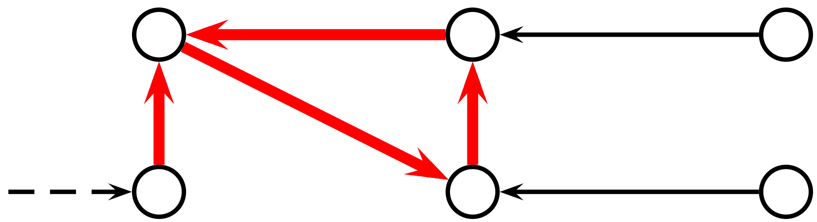
Unary graphs or lassos

Def. Unary graph : graphs with functionnal edge relation.

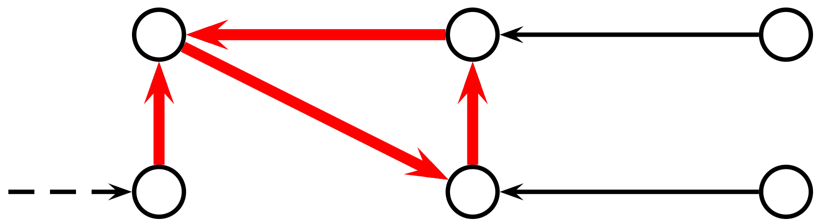
Def. Unary graph : graphs with functionnal edge relation.



Def. Unary graph : graphs with functionnal edge relation.



Def. Unary graph : graphs with functionnal edge relation.



Def.: Lasso : unary graph where every vertex is reachable from the root and the root has no predecessor.

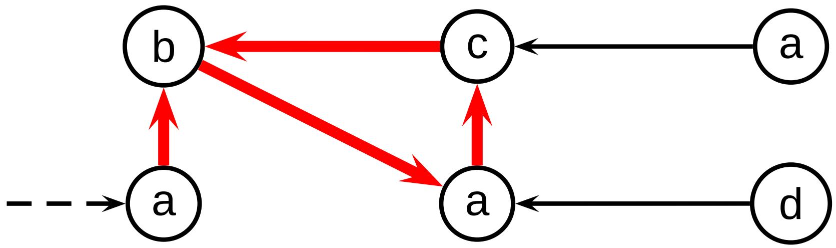
Simple facts on lassos

Facts:

- Every finite unary graph M is bisimilar to a lasso (i.e. induced by the set of reachable vertices. . .).

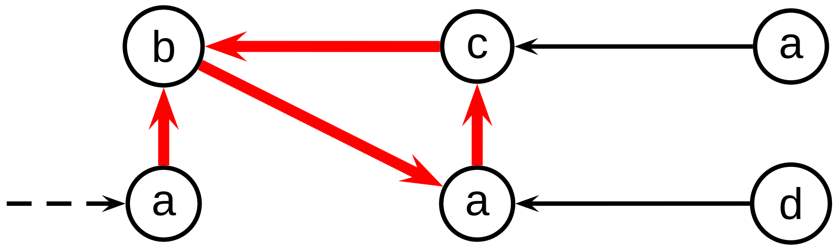
Facts:

- Every finite unary graph M is bisimilar to a lasso (i.e. induced by the set of reachable vertices…).



Facts:

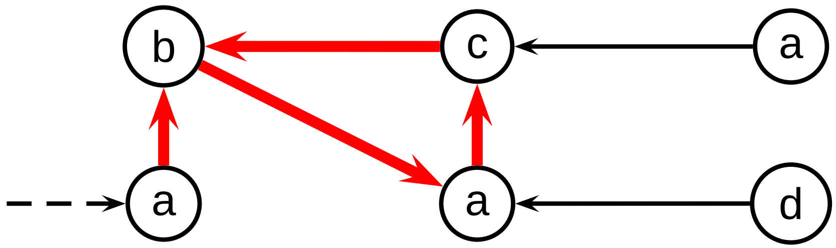
- Every finite unary graph M is bisimilar to a lasso (i.e. induced by the set of reachable vertices...).



A finite word to the cycle: $u = a$.
A finite word on the cycle: $v = bac$.
A inf. encoded word: $w = a.(bac)^\omega$.

Facts:

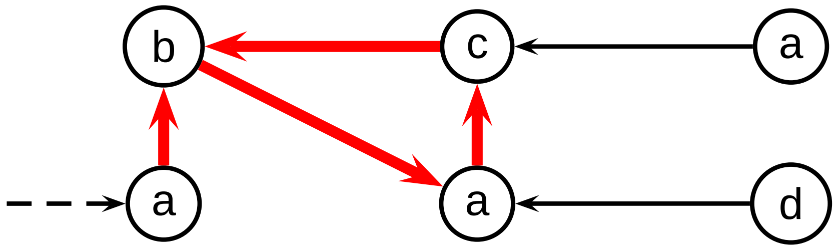
- Every finite unary graph M is bisimilar to a lasso (i.e. induced by the set of reachable vertices…).



- Every lasso is uniquely defined by a pair of word $(u, v) \in \Sigma^+ \times \Sigma^+$ where u describe the word written from the root to the cycle, and v describe the word written on the cycle.

Facts:

- Every finite unary graph M is bisimilar to a lasso (i.e. induced by the set of reachable vertices…).



- Every lasso is uniquely defined by a pair of word $(u, v) \in \Sigma^+ \times \Sigma^+$ where u describe the word written from the root to the cycle, and v describe the word written on the cycle.

- Write $M_{u,v}$ for such a lassos.

The simple problem

Def.: Let φ be an MS-formula on unary graphs and let

$$L_\varphi = \{u.v^\omega : M_{u,v} \models \varphi\}$$

Def.: Let φ be an MS-formula on unary graphs and let

$$L_\varphi = \{u.v^\omega : M_{u,v} \models \varphi\}$$

Lemma: When φ is bisimulation invariant, then for any finite word u and v, $u.v^\omega \in L_\varphi$ iff $M_{u,v} \models \varphi$.

Def.: Let φ be an MS-formula on unary graphs and let

$$L_\varphi = \{u.v^\omega : M_{u,v} \models \varphi\}$$

Lemma: When φ is bisimulation invariant, then for any finite word u and v, $u.v^\omega \in L_\varphi$ iff $M_{u,v} \models \varphi$.

Question: Other properties ?

Main result

Def.: For $L \subseteq \Sigma^\omega$, let $kern(L) = \{u.v^\omega \in L : u \in \Sigma^+, v \in \Sigma^+\}$.

Def.: For $L \subseteq \Sigma^\omega$, let $kern(L) = \{u.v^\omega \in L : u \in \Sigma^+, v \in \Sigma^+\}$.

Theorem: For any bis. inv. formula φ on unary graph:

- L_φ is the kernel of an ω-regular language,
- φ is equivalent to a monadic Σ_1 formula.

Reg. to monadic Σ_1 (1)

Lemma 1: For every regular ω-language L there is a bis. invariant monadic Σ_1 formula φ such that $kern(L) = L_\varphi$

Reg. to monadic Σ_1 (2)

Reg. to monadic Σ_1 (2)

- Take a normalized non deterministic Buchi automaton $\mathcal{A}$ that recognizes L, i.e. such that $u.v^\omega \in L$ if and only if there is an accepting state q s.t.

$$q_0 \xrightarrow{u} q \text{ and } q \xrightarrow{v} q$$

Reg. to monadic Σ_1 (2)

- Take a normalized non deterministic Buchi automaton $\mathcal{A}$ that recognizes L, i.e. such that $u.v^\omega \in L$ if and only if there is an accepting state q s.t.

$$q_0 \xrightarrow{u} q \text{ and } q \xrightarrow{v} q$$

- Then translate into monadic Σ_1.

Remark: Automata normalization makes extensive use of ω-semigroup characterization of regular languages.

Reg. to monadic Σ_1 (2)

- Take a normalized non deterministic Buchi automaton $\mathcal{A}$ that recognizes L, i.e. such that $u.v^\omega \in L$ if and only if there is an accepting state q s.t.

$$q_0 \xrightarrow{u} q \text{ and } q \xrightarrow{v} q$$

- Then translate into monadic Σ_1.

Remark: Automata normalization makes extensive use of ω-semigroup characterization of regular languages.

Reg. to monadic Σ_1 (3)

Remark: If L is not a reg. closed language, i.e. $(a+b)^*.b^\omega$, φ_L is not definable in the ν level NC_1 of the (counting) mu-calculus.

Reg. to monadic Σ_1 (3)

Remark: If L is not a reg. closed language, i.e. $(a+b)^*.b^\omega$, φ_L is not definable in the ν level NC_1 of the (counting) mu-calculus.

Corollary: on finite unary graphs, $NC_1 \subset$ bis.inv. Σ_1 and the inclusion is strict !

Lemma 2: For any bis. inv. MS-formula φ on unary graphs there is an ω-regular language L such that

$$kern(L) = L_\varphi$$

.

Lemma: There is a finite collection of regular languages $\{U_i, V_i\}_{i\in I}$ such that:

$$M_{u,v} \models \varphi \text{ iff } u \in U_i \text{ and } v \in V_i \text{ for some } i \in I$$

Lemma: There is a finite collection of regular languages $\{U_i, V_i\}_{i \in I}$ such that:

$$M_{u,v} \models \varphi \text{ iff } u \in U_i \text{ and } v \in V_i \text{for some } i \in I$$

proof. By a Shelah-like decomposition argument (see Makowski-Ravve 95).

Lemma: There is a finite collection of regular languages $\{U_i, V_i\}_{i\in I}$ such that:

$$M_{u,v} \models \varphi \text{ iff } u \in U_i \text{ and } v \in V_i \text{for some } i \in I$$

proof. By a Shelah-like decomposition argument (see Makowski-Ravve 95).

Remark: We do have $L_\varphi \subseteq \bigcup_{i\in I} U_i.V_i^\omega$.

Lemma: There is a finite collection of regular languages $\{U_i, V_i\}_{i \in I}$ such that:

$$M_{u,v} \models \varphi \text{ iff } u \in U_i \text{ and } v \in V_i \text{for some } i \in I$$

proof. By a Shelah-like decomposition argument (see Makowski-Ravve 95).

Remark: We do have $L_\varphi \subseteq \bigcup_{i \in I} U_i.V_i^\omega$.

Conversely ? If $w \in U_i.V_i^\omega$ ultimately periodic we have:

$$w = \underbrace{u_1.v_1.\cdots.v_n}_{\in U_i.V_i{}^*}.(\underbrace{v_{n+1}.\cdots.v_{n+m}}_{\in V_i{}^+})^\omega$$

Lemma: There is a finite collection of regular languages $\{U_i, V_i\}_{i \in I}$ such that:

$$M_{u,v} \models \varphi \text{ iff } u \in U_i \text{ and } v \in V_i \text{for some } i \in I$$

proof. By a Shelah-like decomposition argument (see Makowski-Ravve 95).

Remark: We do have $L_\varphi \subseteq \bigcup_{i \in I} U_i.V_i^\omega$.

Conversely ? If $w \in U_i.V_i^\omega$ ultimately periodic we have:

$$w = \underbrace{u_1.v_1.\cdots.v_n}_{\in U_i.V_i{}^*}.\big(\underbrace{v_{n+1}.\cdots.v_{n+m}}_{\in V_i{}^+}\big)^\omega$$

And then ...?

Lemma: For each $M_{u,v}$, there a triple $(j,r,s) \in I \times \Sigma^+ \times \Sigma^+$ such that:

- $u.v^\omega = r.s^\omega$, i.e.
- for all k, $r.s^k \in U_j$ and $s.s^k \in V_j$.

Lemma: For each $M_{u,v}$, there a triple $(j, r, s) \in I \times \Sigma^+ \times \Sigma^+$ such that:

- $u.v^\omega = r.s^\omega$, i.e.
- for all k, $r.s^k \in U_j$ and $s.s^k \in V_j$.

Proof. φ is bis. inv. hence $M_{u.v^k, v^{k+1}} \models \varphi \ \ (k > 1)$

Lemma: For each $M_{u,v}$, there a triple $(j, r, s) \in I \times \Sigma^+ \times \Sigma^+$ such that:

- $u.v^\omega = r.s^\omega$, i.e.
- for all k, $r.s^k \in U_j$ and $s.s^k \in V_j$.

Proof. φ is bis. inv. hence $M_{u.v^k, v^{k+1}} \models \varphi \quad (k > 1)$

Hence, there is some j such that $u.v^k \in U_j$ and $v^{k+1} \in V_j$ for inf. many k.

Lemma: For each $M_{u,v}$, there a triple $(j, r, s) \in I \times \Sigma^+ \times \Sigma^+$ such that:

- $u.v^\omega = r.s^\omega$, i.e.
- for all k, $r.s^k \in U_j$ and $s.s^k \in V_j$.

Proof. φ is bis. inv. hence $M_{u.v^k, v^{k+1}} \models \varphi \quad (k > 1)$

Hence, there is some j such that $u.v^k \in U_j$ and $v^{k+1} \in V_j$ for inf. many k.

And both u_j and V_j are regular...

Def.: for such a special triple $t = (j, r, s)$ let

$$D_t = [r]_{U_j}.([s]_{U_j} \cap [s]_{V_j}) \text{ and } E_t = ([s]_{U_j} \cap [s]_{V_j})$$

with $[u]_L = \{v \in \Sigma^* : \forall w_1, w_2 \in \Sigma^*, w_1.u.w_2 \in L \text{ iff } w_1.v.w_2 \in L\}$.

Def.: for such a special triple $t = (j, r, s)$ let

$$D_t = [r]_{U_j}.([s]_{U_j} \cap [s]_{V_j}) \text{ and } E_t = ([s]_{U_j} \cap [s]_{V_j})$$

with $[u]_L = \{v \in \Sigma^* : \forall w_1, w_2 \in \Sigma^*, w_1.u.w_2 \in L$ iff $w_1.v.w_2 \in L\}$.

Lemma:

- $D_t \subseteq U_j$, $E_t \subseteq V_j$ hence for any u and $v \in \Sigma^+$, if $u \in D_t$ and $v \in E_t$ then $M_{u,v} \models \varphi$,
- $D_t.E_t^+ \subseteq D_t$ and $E_t^+ \subseteq E_t$.

Lemma: $kern(L_\varphi) = \bigcup_{t \text{ spec. triple}} D_t.(E_t)^\omega$.

Lemma: $kern(L_\varphi) = \bigcup_{t \text{ spec. triple}} D_t.(E_t)^\omega$.

$\subseteq$. By construction of D_js and E_js...

$\supseteq$.

- Let $w \in D_t.E_t^\omega$ for some special triple $t = (j, r, s)$ with w ultim. per. We must show that $w \in L_\varphi$, i.e. decompose w in $u.v^\omega$ with $M_{u,v} \models \varphi$.

$\supseteq$.

- Let $w \in D_t.E_t^\omega$ for some special triple $t = (j, r, s)$ with w ultim. per. We must show that $w \in L_\varphi$, i.e. decompose w in $u.v^\omega$ with $M_{u,v} \models \varphi$.

- We have $w = u_1.w_1$ with $u_1 \in D_t$ and $w_1 \in E_t^\omega$ ultim. per.

$\supseteq$.

- Let $w \in D_t.E_t^\omega$ for some special triple $t = (j, r, s)$ with w ultim. per. We must show that $w \in L_\varphi$, i.e. decompose w in $u.v^\omega$ with $M_{u,v} \models \varphi$.

- We have $w = u_1.w_1$ with $u_1 \in D_t$ and $w_1 \in E_t^\omega$ ultim. per.

- Since E_t is regular, $w_1 = v_1.v_2.\cdots.v_n.(v_{n+1}.\cdots.v_m)^\omega$ with v_is in E_t.

$\supseteq$.

- Let $w \in D_t.E_t^\omega$ for some special triple $t = (j, r, s)$ with w ultim. per. We must show that $w \in L_\varphi$, i.e. decompose w in $u.v^\omega$ with $M_{u,v} \models \varphi$.

- We have $w = u_1.w_1$ with $u_1 \in D_t$ and $w_1 \in E_t^\omega$ ultim. per.

- Since E_t is regular, $w_1 = v_1.v_2.\cdots.v_n.(v_{n+1}.\cdots.v_m)^\omega$ with v_is in E_t.

- Take $u = u_1.v_1.\cdots.v_n$ in D_t (by prop. of D_t) and $v = v_{n+1}.\cdots.v_m$ in E_t (by prop. of E_t) so that $M_{u,v} \models \varphi$.

Infinite vs finite in unary case ?

Remark: On arbitrary finite and inf. unary models bis. inv. mon Σ_1 defined closed regular languages while on finite models it defines all ω-regular languages.

Theorem: On unary graphs the following formalisms are expressively equivalent:

- (bis. inv.) monadic Σ_1,
- (bis. inv.) MSO,
- μ-calculus.