# Langages formels : résiduel et minimisation

Stéphane Le Roux stephane.le_roux@ens-paris-saclay.fr

ENS Paris-Saclay

2023-2024

# Résiduels d'un langage

## Résiduel

Soit $L \subseteq \Sigma^*$. Pour tout $u \in \Sigma^*$ on écrit $u^{-1}L$ au lieu de $\{u\}^{-1}L = \{v \in \Sigma^* \mid uv \in L\}$, qu'on appelle résiduel de $L$ par $u$.

- Pour tout $u \in \Sigma^*$ on a $u^{-1}\emptyset = \emptyset$ et $u^{-1}\Sigma^* = \Sigma^*$.
- $L_2 := \{\epsilon\}$ a 2 résiduels : $\epsilon^{-1}L_2 = \{e\}$, et $\forall u \neq \epsilon, u^{-1}L_2 = \emptyset$.
- $L_3 := \{a\}$ a 3 résiduels : $\epsilon^{-1}L_3 = \{a\}$, $a^{-1}L_2 = \{e\}$, et $\emptyset$
- Soit $\Sigma = \{a\}$ et $L := (aa)^*$ et $K := a(aa)^*$. Alors les résiduels de $L$ (resp. $K$) sont $L$ et $K$.
- Soit $L := \{a^n b^n \mid n \in \mathbb{N}\}$.
  - Si $u = a^k$, alors $u^{-1}L = \{a^n b^{k+n} \mid n \in \mathbb{N}\} = L \cdot b^k$.
  - Si $u = a^n b^k$ avec $k \leq n$, alors $u^{-1}L = \{b^{n-k}\}$.
  - Sinon, $u^{-1}L = \emptyset$.

- Si $\forall u \in \Sigma^*, u^{-1}L = u^{-1}K$ alors $L = K$, en prenant $u := \epsilon$.
- Soit $L = \emptyset$ et $K = \{\epsilon\}$. Pour tout $u \in \Sigma^+, u^{-1}L = u^{-1}K$.

# Résiduels et opérations ensemblistes

Rappel : $u^{-1}L = \{v \in \Sigma^* \mid uv \in L\}$

**Lemme**

1. $u^{-1}(L \cap K) = u^{-1}L \cap u^{-1}K$.
2. $u^{-1}(L \cup K) = u^{-1}L \cup u^{-1}K$.
3. $u^{-1}(\Sigma^* \setminus L) = \Sigma^* \setminus u^{-1}L$

1. $v \in u^{-1}(L \cap K)$ ssi $uv \in L \cap K$ ssi $uv \in L \wedge uv \in K$ ssi $v \in u^{-1}L \cap u^{-1}K$.
2. $v \in u^{-1}(L \cup K)$ ssi $uv \in L \cup K$ ssi $uv \in L \vee uv \in K$ ssi $v \in u^{-1}L \cup u^{-1}K$.
3. $v \in u^{-1}(\Sigma^* \setminus L)$ ssi $uv \in \Sigma^* \setminus L$ ssi $uv \notin L$ ssi $v \notin u^{-1}L$ ssi $v \in \Sigma^* \setminus u^{-1}L$

# Résiduels, composition, concaténation

**Lemme**

$v^{-1}(u^{-1}L) = (uv)^{-1}L$

**Preuve**

$w \in v^{-1}(u^{-1}L)$ ssi $vw \in u^{-1}L$ ssi $uvw \in L$ ssi $w \in (uv)^{-1}L$.

**Lemme**

$u^{-1}(L \cdot K) = \left((u^{-1}L) \cdot K\right) \cup \left(\bigcup_{y \in L^{-1}\{u\}} y^{-1}K\right)$

**Preuve**

- $v \in u^{-1}(LK)$ ssi $uv \in LK$ ssi $\exists x, y \in \Sigma^*$ tels que $\left(v = xy \wedge ux \in L \wedge y \in K\right) \vee \left(u = xy \wedge x \in L \wedge yv \in K\right)$
- Or $\left(\exists x, y \in \Sigma^*, v = xy \wedge ux \in L \wedge y \in K\right)$ ssi $v \in u^{-1}L \cdot K$
- Et $\left(\exists x, y \in \Sigma^*, u = xy \wedge x \in L \wedge yv \in K\right)$ ssi $v \in y^{-1}K$ pour un $y$ tel qu'il existe un $x \in L$ tq $xy = u$, i.e. pour un $y \in L^{-1}\{u\}$.

# Résiduels et équivalence

### "Équivalence résiduelle"

Cette équivalence est définie par $u \sim_L v$ si $u^{-1}L = v^{-1}L$, i.e. si pour tout $w \in \Sigma^*$ on a $uw \in L$ ssi $vw \in L$.

### Lemme

1. $\sim_L$ est une relation d'équivalence.
2. $\sim_L$ est une "semi-congruence" à droite, i.e. $u \sim_L v \Rightarrow uw \sim_L vw$.

### Preuve

1. Facile.
2. Soit $u \sim_L v$, i.e. pour tout $w \in \Sigma^*$ on a $uw \in L$ ssi $vw \in L$. Soit $x \in \Sigma^*$. Alors $w' \in \Sigma^*$ on a $uxw' \in L$ ssi $vxw' \in L$. Donc $ux \sim_L vx$.

# Intersection de relations d'équivalence

### Lemme

Soit $\sim_1$ et $\sim_2$ deux relations d'équivalence sur un ensemble $E$. Alors

1. $\sim_1 \cap \sim_2$ est une relation d'équivalence
2. et $f : E/(\sim_1 \cap \sim_2) \to (E/\sim_1) \times (E/\sim_1)$ telle que $f([x]_{\sim_1 \cap \sim_2}) := ([x]_{\sim_1}, [x]_{\sim_2})$ est bien définie et injective.

### Preuve

1. Facile : e.g. si $x(\sim_1 \cap \sim_2)y$ alors $x \sim_1 y$ et $x \sim_2 y$, puis $y \sim_1 x$ et $y \sim_2 x$ par symétrie, d'où $y(\sim_1 \cap \sim_2)x$.
2. 
   - $f$ est bien définie car si $x(\sim_1 \cap \sim_2)y$, alors $x \sim_1 y$ et $x \sim_2 y$.
   - $f$ est injective car si $x \sim_1 y$ et $x \sim_2 y$, alors $x(\sim_1 \cap \sim_2)y$.

# "Équivalence résiduelle" et opérations ensemblistes

**Rappel**

1. $u^{-1}(L \cup K) = u^{-1}L \cup u^{-1}K$.
2. $u^{-1}(L \cap K) = u^{-1}L \cap u^{-1}K$.
3. $u^{-1}(\Sigma^* \setminus L) = \Sigma^* \setminus u^{-1}L$

**Lemme**

1. $\sim_L \cap \sim_K \subseteq \sim_{L \cap K}$
2. $\sim_L \cap \sim_K \subseteq \sim_{L \cup K}$
3. $\sim_L = \sim_{\Sigma^* \setminus L}$

1. Si $u \sim_L v$ et $u \sim_K v$, alors $u^{-1}L = v^{-1}L$ et $u^{-1}K = v^{-1}K$, alors $u^{-1}L \cup u^{-1}K = v^{-1}L \cup v^{-1}K$, alors $u^{-1}(L \cup K) = v^{-1}(L \cup K)$, alors $u \sim_{L \cup K} v$.
2. Similaire.
3. $u \sim_{\Sigma^* \setminus L} v$ ssi $u^{-1}(\Sigma^* \setminus L) = v^{-1}(\Sigma^* \setminus L)$, ssi $\Sigma^* \setminus u^{-1}L = \Sigma^* \setminus v^{-1}L$ ssi $u^{-1}L = v^{-1}L$ ssi $u \sim_L v$.

# Finitude résiduelle et opérations ensemblistes

## Lemme (rappel)

1. $\sim_L = \sim_{\Sigma^* \setminus L}$
2. $\sim_L \cap \sim_K \subseteq \sim_{L \cap K}$
3. $\sim_L \cap \sim_K \subseteq \sim_{L \cup K}$

## Lemme

1. Si $L$ a un nombre fini de résiduels alors de même pour $\Sigma^* \setminus L$.
2. Si $L$ et $K$ ont un nombre fini de résiduels alors de même pour $L \cap K$ et $L \cup K$.

## Preuve

1. $L$ et $\Sigma^* \setminus L$ ont les mêmes résiduels. (cf le rappel ci-dessus)
2. D'après un lemme précédent, $|\Sigma^*/(\sim_L \cap \sim_K)| \leq |(\Sigma^*/\sim_L) \times (\Sigma^*/\sim_K)| = |\Sigma^*/\sim_L| \cdot |\Sigma^*/\sim_K|$. Or d'après le rappel ci-dessus $|\Sigma^*/\sim_{L \cup K}| \leq |\Sigma^*/(\sim_L \cap \sim_K)|$. Donc si $\Sigma^*/\sim_L$ et $\Sigma^*/\sim_K$ sont finis, $\Sigma^*/\sim_{L \cup K}$ aussi.

# Finitude résiduelle, langage résiduel, concaténation

## Lemme

$\sim_L \subseteq \sim_{u^{-1}L}$, donc si $L$ a un nombre fini de résiduels, $u^{-1}L$ aussi.

## Preuve

Supposons que $x \sim_L y$, i.e. $x^{-1}L = y^{-1}L$, i.e. $\forall v \in \Sigma^*, xv \in L \Leftrightarrow yv \in L$.
Alors pour tout $u \in \Sigma^*$ on a $\forall v \in \Sigma^*, xuv' \in L \Leftrightarrow yuv' \in L$

Rappel : $u^{-1}(L \cdot K) = \big((u^{-1}L) \cdot K\big) \cup \big(\bigcup_{y \in L^{-1}\{u\}} y^{-1}K\big)$

## Lemme

Si $L$ et $K$ ont un nombre fini de résiduels, $u^{-1}(LK)$ aussi.

Preuve : Il y a un nombre fini de $u^{-1}L$, donc un nombre fini (inférieur ou égal) de $(u^{-1}L)K$. Il y a un nombre fini de $y^{-1}K$, donc un nombre fini d'unions de plusieurs $y^{-1}K$. Ainsi, par le rappel ci-dessus, il y a un nombre fini de $u^{-1}(L \cdot K)$,

# Résiduels dans un automate

**"Résiduel d'un état"**

Soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet. Pour tout $q \in Q$, soit $\mathcal{L}(q) := \mathcal{L}(\mathcal{A}[i \leftarrow q]) = \{u \in \Sigma^* \mid \delta^*(q, u) \in F\}$.

**Lemme**

Soit $L \subseteq \Sigma^*$ et $\mathcal{A}$ un AD complet tel que $\mathcal{L}(\mathcal{A}) = L$.

1. $\mathcal{L}(i) = L$
2. $\mathcal{L}(\delta^*(q, u)) = u^{-1}\mathcal{L}(q)$
3. $\mathcal{L}(\delta^*(i, u)) = u^{-1}L$
4. $\delta^*(i, u) = \delta^*(i, v) \Rightarrow u \sim_L v$

1. $\mathcal{L}(i) = \{u \in \Sigma^* \mid \delta^*(i, u) \in F\} = \mathcal{L}(\mathcal{A})$
2. $\mathcal{L}(\delta^*(q, u)) = \{v \in \Sigma^* \mid \delta^*(\delta^*(q, u), v) \in F\} = \{v \in \Sigma^* \mid \delta^*(q, uv) \in F\} = \{v \in \Sigma^* \mid uv \in \mathcal{L}(q)\} = u^{-1}\mathcal{L}(q)$
3. Par les deux résultats ci-dessus.
4. Car $\mathcal{L}(\delta^*(i, u)) = u^{-1}L$.

## Résiduels dans un automate (II)

Rappel : Soit $L \subseteq \Sigma^*$ et $\mathcal{A} = (Q, \delta, i, F)$ un AD complet tq $\mathcal{L}(\mathcal{A}) = L$.

- "Résiduel d'un état" : Pour tout $q \in Q$, soit $\mathcal{L}(q) := \mathcal{L}(\mathcal{A}[i \leftarrow q]) = \{u \in \Sigma^* \mid \delta^*(q, u) \in F\}$.
- $\mathcal{L}(i) = L$
- $\mathcal{L}(\delta^*(q, u)) = u^{-1}\mathcal{L}(q)$
- $\mathcal{L}(\delta^*(i, u)) = u^{-1}L$
- $\delta^*(i, u) = \delta^*(i, v) \Rightarrow u \sim_L v$

**Lemme**

1. $\mathcal{L}[Access(Q)] = \Sigma^*/\sim_L$
2. Tout AD complet reconnaissant $L$ a au moins $|\Sigma^*/\sim_L|$ états.
3. Tout langage rationnel a un nombre fini de résiduels.

1.
   - $\mathcal{L}[Access(Q)] \subseteq \Sigma^*/\sim_L$ par l'avant-dernier rappel.
   - Soit $u^{-1}L \in \Sigma^*/\sim_L$. Alors $u^{-1}L = \mathcal{L}(\delta^*(i, u))$, par l'avant-dernier rappel.
2. $|\Sigma^*/\sim_L| = |\mathcal{L}[Access(Q)]| \leq |Access(Q)| \leq |Q|$
3. Par le résultat ci-dessus.

# Automate des résiduels

Soit $L \subseteq \Sigma^*$. L'automate des résiduels, déterministe, complet, pas nécessairement fini, $\mathcal{R}_L := (\Sigma, Q_L, \delta_L, i_L, F_L)$ est défini comme suit.

- $Q_L := \Sigma^*/\sim_L = \{u^{-1}L \mid u \in \Sigma^*\} = \{[u]_{\sim_L} \mid u \in \Sigma^*\}$
- $\delta_L(u^{-1}L, a) := (ua)^{-1}L$. Dit autrement, $\delta_L([u]_{\sim_L}, a) := [ua]_{\sim_L}$(bien défini par semi-congruence à droite)
- $i_L := L = \epsilon^{-1}L = [\epsilon]_{\sim_L}$
- $F_L := \{u^{-1}L \mid u \in L\} = \{[u]_{\sim_L} \mid u \in L\}$

## Lemme

1. $\forall u, w \in \Sigma^*, \delta_L^*(u^{-1}L, w) = (uw)^{-1}L$
2. $\forall w \in \Sigma^*, \delta_L^*(i_L, w) = w^{-1}L$

## Preuve

1. Soit $u \in \Sigma^*$. Mq $\forall w \in \Sigma^*, \delta_L^*(u^{-1}L, w) = (uw)^{-1}L$, par réc. sur $w$.
   - $\delta_L^*(u^{-1}L, \epsilon) = u^{-1}L = (u\epsilon)^{-1}L$.
   - $\delta_L^*(u^{-1}L, wa) = \delta(\delta_L^*(u^{-1}L, w), a) \overset{HR}{=} \delta((uw)^{-1}L, a) = (uwa)^{-1}L$.
2. En prenant $u := \epsilon$, i.e. $u^{-1}L = L = i_L$.

# Automate des résiduels (II)

Soit $L \subseteq \Sigma^*$. L'automate des résiduels, déterministe, complet, pas nécessairement fini, $\mathcal{R}_L := (\Sigma, Q_L, \delta_L, i_L, F_L)$ est défini comme suit.

- $Q_L := \Sigma^* / \sim_L = \{u^{-1}L \mid u \in \Sigma^*\} = \{[u]_{\sim_L} \mid u \in \Sigma^*\}$
- $\delta_L(u^{-1}L, a) := (ua)^{-1}L$. Dit autrement, $\delta_L([u]_{\sim_L}, a) := [ua]_{\sim_L}$, bien défini par semi-congruence à droite.
- $i_L := L = \epsilon^{-1}L = [\epsilon]_{\sim_L}$
- $F_L := \{u^{-1}L \mid u \in L\} = \{[u]_{\sim_L} \mid u \in L\}$

Rappel : $\delta_L^*(i_L, u) = u^{-1}L$ $(\forall u, w \in \Sigma^*, \delta_L^*(u^{-1}L, w) = (uw)^{-1}L)$

**Lemme**

1. Pour tout $L \subseteq \Sigma^*$, on a $\mathcal{L}(\mathcal{R}_L) = L$.
2. $\mathcal{R}_L$ est accessible.
3. Tout langage avec un nombre fini de résiduel est rationnel.

1. $\delta_L^*(i_L, u) \in F_L$ ssi $u^{-1}L \in F_L$ ssi $u \in L$.
2. Car $\delta_L^*(i_L, u) = u^{-1}L$.
3. Car $\mathcal{L}(\mathcal{R}_L) = L$ et $Q_L = \Sigma^* / \sim_L = \{u^{-1}L \mid u \in \Sigma^*\}$

# Automate des résiduels : exemple

Soient $\Sigma := \{a, b\}$ et $L := \Sigma^* ab \Sigma^*$.

- Pour tout $u \in L$, on a $u^{-1}L = \Sigma^*$
- Pour tout $u \in b^* a^+$, on a $u^{-1}L = b\Sigma^* \cup L$
- Pour tout $u \in b^*$, on a $u^{-1}L = L$

Rappel : $\mathcal{R}_L := (\Sigma, Q_L, \delta_L, i_L, F_L)$ est défini comme suit.

- $Q_L := \Sigma^* / \sim_L = \{u^{-1}L \mid u \in \Sigma^*\} = \{[u]_{\sim_L} \mid u \in \Sigma^*\}$
- $\delta_L(u^{-1}L, a) := (ua)^{-1}L$.
- $i_L := L$
- $F_L := \{u^{-1}L \mid u \in L\}$

- $Q_L := \{L, b\Sigma^* \cup L, \Sigma^*\}$
- $i_L := L$
- $F_L := \{u^{-1}L \mid u \in L\}$
-

| $\delta_L$ | $L$ | $b\Sigma^* \cup L$ | $\Sigma^*$ |
|---|---|---|---|
| $a$ | $a^{-1}L = b\Sigma^* \cup L$ | $b\Sigma^* \cup L$ | $\Sigma^*$ |
| $b$ | $b^{-1}L = L$ | $\Sigma^*$ | $\Sigma^*$ |

# Caractérisation de $\mathrm{Rec}(\Sigma^*)$ par résiduels

## Lemme (rappel)

1. $\mathcal{L}[Access(Q)] = Q_L$
2. Tout AD complet reconnaissant $L$ a au moins $|\Sigma^*/\sim_L|$ états.
3. Tout langage rationnel a un nombre fini de résiduels.

## Lemme (rappel)

1. Pour tout $L \subseteq \Sigma^*$, on a $\mathcal{L}(\mathcal{R}_L) = L$.
2. Tout langage avec un nombre fini de résiduel est rationnel.

## Corollaire

1. Tout AD complet reconnaissant $L$ a au moins $|\Sigma^*/\sim_L|$ états, et il en existe un avec $|\Sigma^*/\sim_L|$ états.
2. $L \subseteq \Sigma^*$ est rationnel ssi $L$ a un nombre fini résiduels, i.e. ssi $\sim_L$ a un nombre fini de classes d'équivalence.

# Congruence d'un automate

Soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet. Une relation d'équivalence $\sim \subseteq Q \times Q$ est une congruence sur $\mathcal{A}$ si

- $\forall q, q' \in Q, \forall a \in \Sigma, q \sim q' \Rightarrow \delta(q, a) \sim \delta(q', a)$ (Préservation)
- $F$ est saturé par $\sim$, i.e. si $q \sim q'$ alors $q \in F \Leftrightarrow q' \in F$.

L'AD quotient est $\mathcal{A}_\sim := (Q/\sim, \delta_\sim, [i]_\sim, F_\sim)$, où $\delta_\sim([q]_\sim, a) := [\delta(q, a)]_\sim$ et $F_\sim := \{S \in Q/\sim \mid S \subseteq F\}$.

- $Q/\sim$, $[i]_\sim$ et $F_\sim$ sont bien définis car $\sim$ est une relation d'équiv.
- $\delta_\sim$ est bien définie par préservation.
- Soit $(q, a) \in Q \times \Sigma$. On a seulement $\{\delta(q', a) \mid q' \sim q\} = \delta([q]_\sim, a) \subseteq [\delta(q, a)]_\sim$

## Lemme

1. (Juste rel d'éq) $F$ saturé par $\sim$ ssi $\forall q \in Q, [q]_\sim \subseteq F \vee [q]_\sim \cap F = \emptyset$
2. (Juste rel d'éq) $[q]_\sim \in F_\sim$ ssi $[q]_\sim \subseteq F$ ssi $[q]_\sim \in F/\sim$

1. Reformulation de la saturation.
2. Définition de $F_\sim$ plus définition d'une restriction de relation binaire.

# Congruence d'un automate (II)

Rappel : $\sim$ est une congruence sur l'AD complet $\mathcal{A} = (Q, \delta, i, F)$ si

- $\forall q, q' \in Q, \forall a \in \Sigma, q \sim q' \Rightarrow \delta(q, a) \sim \delta(q', a)$ (Préservation)
- $F$ est saturé par $\sim$, i.e. si $q \sim q'$ alors $q \in F \Leftrightarrow q' \in F$.

L'AD quotient est $\mathcal{A}_\sim := (Q/\sim, \delta_\sim, [i]_\sim, F_\sim)$, où
$\delta_\sim([q]_\sim, a) := [\delta(q, a)]_\sim$ et $F_\sim := \{S \in Q/\sim \mid S \subseteq F\}$.

- (Juste rel d'éq) $F$ saturé par $\sim$ ssi $\forall q \in Q, [q]_\sim \subseteq F \vee [q]_\sim \cap F = \emptyset$
- (Juste rel d'éq) $[q]_\sim \in F_\sim$ ssi $[q]_\sim \subseteq F$ ssi $[q]_\sim \in F/\sim$

## Lemme

1. (Avec saturation) $[q]_\sim \in F_\sim$ ssi $q \in F$
2. (Avec préservation) $\delta^*_\sim([q]_\sim, u) = [\delta^*(q, u)]_\sim$
3. (Avec les deux) $\delta^*(q, u) \in F$ ssi $\delta^*_\sim([q]_\sim, u)]_\sim \in F_\sim$
4. (Avec les deux) Si $q \sim q'$ alors $\mathcal{L}(q) = \mathcal{L}(q')$. (Compatibilité)

1. $[q]_\sim \in F_\sim$ ssi $[q]_\sim$ par le 2ème rappel, puis $[q]_\sim$ ssi $q \in F$ par le 1er.
2. Par récurrence sur $u$.
3. Par 1. et 2.
4. Par 3.

# Congruence d'un automate (III)

Rappel : $\sim$ est une congruence sur l'AD complet $\mathcal{A} = (Q, \delta, i, F)$ si

- $\forall q, q' \in Q, \forall a \in \Sigma, q \sim q' \Rightarrow \delta(q, a) \sim \delta(q', a)$ (Préservation)
- $F$ est saturé par $\sim$, i.e. si $q \sim q'$ alors $q \in F \Leftrightarrow q' \in F$.

L'AD quotient est $\mathcal{A}_\sim := (Q/\sim, \delta_\sim, [i]_\sim, F_\sim)$, où
$\delta_\sim([q]_\sim, a) := [\delta(q, a)]_\sim$ et $F_\sim := \{S \in Q/\sim \mid S \subseteq F\}$.

## Lemme (rappel)

$\delta^*(q, u) \in F$ ssi $\delta^*_\sim([q]_\sim, u)]_\sim \in F_\sim$

## Lemme (vers la minimisation)

Pour toute congruence $\sim$ d'un AD complet $\mathcal{A}$, on a $\mathcal{L}(\mathcal{A}/\sim) = \mathcal{L}(\mathcal{A})$.

## Preuve

$u \in \mathcal{L}(\mathcal{A})$ ssi $\delta^*(i, u) \in F$ ssi (cf rappel) $\delta^*_\sim([i]_\sim, u) \in F_\sim$ ssi $u \in \mathcal{L}(\mathcal{A}/\sim)$

## Morphisme d'automates

Soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet et **accessible**. Soit $L := \mathcal{L}(A)$.

Par accessibilité, $\forall q \in Q \exists u \in \Sigma^*$ tel que $\mathcal{L}(q) = \mathcal{L}(\delta^*(i, u)) = u^{-1}L$.

Soit $\sim$ une congruence de $\mathcal{A}$. On sait que $\sim$ et $\mathcal{L}$ sont compatibles, i.e. $q \sim q' \Rightarrow \mathcal{L}(q) = \mathcal{L}(q')$. La compatibilité de la rel. d'éq. permet de factoriser $\mathcal{L} : Q \to (\Sigma^* / \sim_L)$ (codomaine correct par accessibilité) en $\mathcal{L}_\sim : (Q/\sim) \to (\Sigma^* / \sim_L)$ définie par $\mathcal{L}_\sim([q]_\sim) := \mathcal{L}(q)$. Montrons que $\mathcal{L}_\sim$ est un "morphisme d'automate" surjectif.

$\mathcal{L}_\sim$ est surjective, car $\mathcal{L}$ l'est, car $\mathcal{L}[Access(Q)] = Q_L$.

**Lemme**

$\mathcal{L}_\sim$ envoie l'état initial de $\mathcal{A}/\sim$ sur l'état initial de $\mathcal{R}_L$

Preuve :

- $i(\mathcal{A}/\sim) \stackrel{def}{=} [i]_\sim$
- $i(\mathcal{R}_L) \stackrel{def}{=} i_L \stackrel{def}{=} L$
- $\mathcal{L}_\sim([i]_\sim) \stackrel{def}{=} \mathcal{L}(i) \stackrel{prop}{=} L$

# Morphisme d'automates (II)

Rappel : soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet, **accessible**. Soit $L := \mathcal{L}(A)$.

Par accessibilité, $\forall q \in Q \exists u \in \Sigma^*$ tel que $\mathcal{L}(q) = \mathcal{L}(\delta^*(i, u)) = u^{-1}L$.

Rappel : soit $\mathcal{L}_\sim : (Q/\sim) \to (\Sigma^*/\sim_L)$ définie par $\mathcal{L}_\sim([q]_\sim) := \mathcal{L}(q)$.
Montrons que $\mathcal{L}_\sim$ est un "morphisme d'automate" surjectif.

**Lemme**

$\mathcal{L}_\sim$ envoie les états finaux de $\mathcal{A}/\sim$ sur les états finaux de $\mathcal{R}_L$. (De manière surjective.)

- $F(\mathcal{A}/\sim) \overset{def}{=} \{[q]_\sim \mid [q]_\sim \subseteq F\} \overset{prop}{=} \{[q]_\sim \mid q \in F\}$
- $F_L \overset{def}{=} \{u^{-1}L \mid u \in L\}$
- Soient $q \in Q$ et $u \in \Sigma^*$ tels que $\delta^*(i, u) = q$, donc $\mathcal{L}(q) = u^{-1}L$. Ainsi $[q]_\sim \in F(\mathcal{A}/\sim)$ ssi $q \in F$ ssi $u \in L$ ssi $u^{-1}L \in F_L$ ssi $\mathcal{L}_\sim([q]_\sim) \in F_L$. Le sens droite-gauche de l'équivalence donne la surjectivité.

# Morphisme d'automates (III)

Rappel : soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet, **accessible**. Soit $L := \mathcal{L}(A)$.

Par accessibilité, $\forall q \in Q \exists u \in \Sigma^*$ tel que $\mathcal{L}(q) = \mathcal{L}(\delta^*(i, u)) = u^{-1}L$.

Rappel : soit $\mathcal{L}_\sim : (Q/\sim) \to (\Sigma^*/\sim_L)$ définie par $\mathcal{L}_\sim([q]_\sim) := \mathcal{L}(q)$.
Montrons que $\mathcal{L}_\sim$ est un "morphisme d'automate" surjectif.

### Lemme (le diagramme commute, fin de preuve de morphisme)

$$\begin{array}{ccccc}
[q]_\sim & \xrightarrow{\delta_\sim, a} & \delta_\sim([q]_\sim, a) & & \\
\mathcal{L}_\sim \downarrow & & \downarrow \mathcal{L}_\sim & & \\
\mathcal{L}_\sim([q]_\sim) & \xrightarrow{\delta_L, a} & \delta_L(\mathcal{L}_\sim([q]_\sim), a) & = & \mathcal{L}_\sim(\delta_\sim([q]_\sim, a))
\end{array}$$

Soit $(q, a) \in Q \times \Sigma$. Soit $u \in \Sigma^*$ tel que $\delta(i, u) = q$. Alors

- $\mathcal{L}_\sim([q]_\sim) = \mathcal{L}(q) = u^{-1}L$
- $\delta_L(\mathcal{L}_\sim([q]_\sim), a) = \delta_L(u^{-1}L, a) = (ua)^{-1}L$
- $\delta_\sim([q]_\sim, a) = [\delta(q, a)]_\sim$
- $\mathcal{L}_\sim(\delta_\sim([q]_\sim, a)) = \mathcal{L}_\sim([\delta(q, a)]_\sim) = \mathcal{L}(\delta(q, a)) = \mathcal{L}(\delta^*(i, ua)) = (ua)^{-1}L$

# Équivalence de Nérode

- Rappel : $\mathcal{L}(q) := \{u \in \Sigma^* \mid \delta^*(q,u) \in F\}$
- Rappel : $\mathcal{L}(\delta^*(q,u)) = u^{-1}\mathcal{L}(q)$

Soit $\mathcal{A} = (Q, \delta, i, F)$ un AD complet. L'équivalence de Nérode est définie par $q \sim_N q'$ si $\mathcal{L}(q) = \mathcal{L}(q')$.

**Lemme**

1. Préservation : si $q \sim_N q'$ alors $\delta^*(q,u) \sim_N \delta^*(q',u)$.
2. Saturation : si $q \sim_N q'$, alors $q \in F$ ssi $q' \in F$.
3. L'équivalence du Nérode est une congruence d'automate.

1. Soit $q \sim_N q'$ et $u \in \Sigma^*$. Alors $\mathcal{L}(q) = \mathcal{L}(q')$, donc $u^{-1}\mathcal{L}(q) = u^{-1}\mathcal{L}(q')$, i.e. $\mathcal{L}(\delta^*(q,u)) = \mathcal{L}(\delta^*(q',u))$, i.e. $\delta^*(q,u) \sim_N \delta^*(q',u))$.
2. Soit $q \sim_N q'$. On a $q \in F$ ssi $\delta^*(q,\epsilon) \in F$ ssi $\epsilon \in \mathcal{L}(q)$ ssi $\epsilon \in \mathcal{L}(q')$ ssi $\delta^*(q',\epsilon) \in F$ ssi $q' \in F$.
3. Par les deux résultats ci-dessus, en prenant $|u| = 1$.

# Équivalence de Nérode et résiduels

Soient $L \subseteq \Sigma^*$ et $\mathcal{A}$ un AD complet tel que $\mathcal{L}(\mathcal{A}) = L$.

**Lemme**

1. $\mathcal{L}$ est compatible avec $\sim_N$, i.e. $q \sim_N q' \Rightarrow \mathcal{L}(q) = \mathcal{L}(q')$.
2. $\sim_N$ est la plus grande relation d'équivalence compatible avec $\mathcal{L}$.
3. $\sim_N$ est la plus grande congruence de $\mathcal{A}$.

**Preuve**

1. Par définition $q \sim_N q' \Leftrightarrow \mathcal{L}(q) = \mathcal{L}(q')$.
2. Soit $\sim$ compatible avec $\mathcal{L}$, i.e. $q \sim q' \Rightarrow \mathcal{L}(q) = \mathcal{L}(q')$. Si $q \sim q'$, alors $\mathcal{L}(q) = \mathcal{L}(q')$, donc $q \sim_N q'$. Ainsi $\sim \subseteq \sim_N$.
3. Toute congruence est compatible avec $\mathcal{L}$.

# Équivalence de Nérode et résiduels (II)

Soient $L \subseteq \Sigma^*$ et $\mathcal{A}$ un AD complet et **accessible** tel que $\mathcal{L}(\mathcal{A}) = L$.

**Lemme**

$\mathcal{L}_{\sim_N} : Q/\sim_N \rightarrow \Sigma^*/\sim_L$ telle que $\mathcal{L}_{\sim_N}([q]_{\sim_N}) := \mathcal{L}(q)$ est un isomorphisme d'automate.
Autrement dit : à renommage des états près, $\mathcal{A}/\sim_N$ est égal à $\mathcal{R}_L$

- $\mathcal{L}_{\sim_N}$ est un morphisme surjectif car $\sim_N$ est une congruence d'automate.
- $\mathcal{L}_{\sim_N}$ est injectif (classique) : par définition, si $\mathcal{L}(q) = \mathcal{L}(q')$ alors $q \sim_N q'$, i.e. $[q]_{\sim_N} = [q']_{\sim_N}$.

# AD complet minimal

## Lemme (rappel)

Soient $L \subseteq \Sigma^*$ et $\mathcal{A}$ un AD complet et accessible tel que $\mathcal{L}(\mathcal{A}) = L$. À renommage des états près, $\mathcal{A}/\sim_N$ est égal à $\mathcal{R}_L$.

## Corollaire

Si $L \subseteq \Sigma^*$, à renommage des états près $\mathcal{R}_L$ est le plus petit (en terme de nombre d'états) AD complet reconnaissant $L$.

## Preuve

Soit $\mathcal{A}$ un AD tel que $\mathcal{L}(\mathcal{A}) = L$. Alors $\mathcal{L}(Access(\mathcal{A})) = L$. D'après le lemme précédent $Access(\mathcal{A})/\sim_N$ est isomorphe à $\mathcal{R}_L$, donc $\mathcal{R}_L$ n'a pas plus d'état que $\mathcal{A}$.

# AD minimal non complet

**Lemme**

Soit $L \subseteq \Sigma^*$.

1. $\mathcal{R}_L$ a au plus un état non co-accessible (la "poubelle")
2. Les trois assertions suivantes sont équivalentes.
   1. $\mathcal{R}_L$ est co-accessible.
   2. $\emptyset$ n'est pas un résiduel de $L$.
   3. $Pref(L) = \Sigma^*$

# Calcul de l'AFD minimal, algorithme de Moore

## Relations de Nérode tronquées

Soit $\mathcal{A} = (\Sigma, Q, \delta, i, F)$ un AFD complet. Pour tout $n \in \mathbb{N}$ et $p, q \in Q$ on pose $p \sim_n q$ si $\mathcal{L}(p) \cap \Sigma^{\leq n} = \mathcal{L}(q) \cap \Sigma^{\leq n}$.
(Rappel : $\mathcal{L}(p) := \{u \in \Sigma^* \mid \delta^*(q, u) \in F\}$)

## Lemme

1. $\sim_n$ est une relation d'équivalence.
2. $p \sim_n q$ ssi $\forall w \in \Sigma^{\leq n}, \delta^*(p, w) \in F \Leftrightarrow \delta^*(q, w) \in F$
3. $\sim_0$ a pour classes d'équivalence $F$ et $Q \setminus F$.
4. $\sim_{n+1} \subseteq \sim_n$, i.e. $\sim_{n+1}$ est plus fine que $\sim_n$.
5. $\sim_N = \bigcap_{n \in \mathbb{N}} \sim_n$

## Preuve (Pour $\sim_N = \bigcap_{n \in \mathbb{N}} \sim_n$)

$p \sim_N q$ ssi $\mathcal{L}(p) = \mathcal{L}(q)$ ssi $\forall w \in \Sigma^*, \delta^*(p, w) \in F \Leftrightarrow \delta^*(q, w) \in F$
$\forall n \in \mathbb{N} \forall w \in \Sigma^{\leq n}, \delta^*(p, w) \in F \Leftrightarrow \delta^*(q, w) \in F$ ssi
$\forall n \in \mathbb{N}, \mathcal{L}(p) \cap \Sigma^{\leq n} = \mathcal{L}(q) \cap \Sigma^{\leq n}$ ssi $\forall n \in \mathbb{N}, p \sim_n q$.

# Calcul de l'AFD complet minimal, algorithme de Moore (II)

Rappel : $p \sim_n q$ si $\mathcal{L}(p) \cap \Sigma^{\leq n} = \mathcal{L}(q) \cap \Sigma^{\leq n}$.

**Lemme**

Les trois assertions suivantes sont équivalentes.

1. $p \sim_{n+1} q$
2. $p \sim_n q$ et $\forall a \in \Sigma, \delta(p,a) \sim_n \delta(q,a)$
3. $p \sim_0 q$ et $\forall a \in \Sigma, \delta(p,a) \sim_n \delta(q,a)$

- 2. $\Rightarrow$ 3. Car $\sim_n \subseteq \sim_0$
- 1. $\Rightarrow$ 2. D'une part $p \sim_n q$ car $\sim_{n+1} \subseteq \sim_n$. D'autre part, soit $a \in \Sigma$ et $w \in \Sigma^{\leq n}$, d'où $aw \in \Sigma^{\leq n+1}$. Alors $\delta^*(\delta(p,a), w) \in F$ ssi $\delta^*(p, aw) \in F$ ssi (par $\sim_{n+1}$) $\delta^*(q, aw) \in F$ ssi $\delta^*(\delta(q,a), w) \in F$.
- 3. $\Rightarrow$ 1. Soit $w \in \Sigma^{\leq n+1}$. Mq $\delta^*(p,w) \in F$ ssi $\delta^*(q,w) \in F$
  - Si $w = \epsilon$ alors $p \sim_0 q$ implique $\delta^*(p,w) = p \in F \Leftrightarrow \delta^*(q,w) = q \in F$.
  - Si $w \neq \epsilon$, soit $(a,u) \in \Sigma \times \Sigma^{\leq n}$ tq $w = au$. On a $\delta^*(p,w) \in F$ ssi $\delta^*(\delta(p,w_1), w_2 \dots w_{|w|}) \in F$ ssi $\delta^*(\delta(q,w_1), w_2 \dots w_{|w|}) \in F$ ssi $\delta^*(q,w) \in F$.

# Calcul de l'AFD minimal, algorithme de Moore (III)

- Rappel : $p \sim_n q$ si $\mathcal{L}(p) \cap \Sigma^{\leq n} = \mathcal{L}(q) \cap \Sigma^{\leq n}$.
- Rappel : $p \sim_{n+1} q$ ssi $p \sim_n q$ et $\forall a \in \Sigma, \delta(p, a) \sim_n \delta(q, a)$

## Lemme

1. Si $\sim_{n+1} = \sim_n$, alors $\sim_N = \sim_n$.
2. $F \in \{\emptyset, Q\}$ ssi $\mathcal{L}(\mathcal{A}) \in \{\emptyset, \Sigma^*\}$ ssi $\sim_N = \sim_0 = Q \times Q$.
3. Si $F \notin \{\emptyset, Q\}$ alors $\sim_N = \sim_{|Q|-2}$.

1. Si $\sim_{n+1} = \sim_n$, alors $p \sim_{n+2} q$ ssi $p \sim_{n+1} q$ et $\forall a \in \Sigma, \delta(p, a) \sim_{n+1} \delta(q, a)$ ssi $p \sim_n q$ et $\forall a \in \Sigma, \delta(p, a) \sim_n \delta(q, a)$ ssi $p \sim_{n+1} q$.
2. Facile.
3. Si $\sim_{n+1} \neq \sim_n$, alors $|Q/\sim_n| < |Q/\sim_{n+1}|$. Supposons que $\sim_{|Q|-2} \neq \sim_N$. Alors $|Q/\sim_0| < \cdots < |Q/\sim_{|Q|-2}| < |Q/\sim_{|Q|-1}|$. Or $|Q/\sim_0| = 2$, donc $|Q| + 1 \leq |Q/\sim_{|Q|-1}|$. Or $|Q/\sim_n| \leq |Q|$, contradiction.

# Non-unicité des AFN minimaux

Soit $L := (a + b)aaa + b(a + b)(a + b)b$.