

# Démonstrations des lois algébriques utilisées en C2QL

Santiago Bautista

Juin 2017

## Structure des démonstrations

Puisque dans toutes les démonstrations qui suivent le but est de prouver, sous certaines conditions, l'égalité de deux fonctions  $f_1$  et  $f_2$  sur  $R$  (ou sur  $R^2$  ou  $R^3$  selon le cas), la structure de toutes les démonstrations sera la même : on considérera  $r$  une relation (ou une paire ou un triplet de relations, selon le cas), on commencera par montrer que  $f_1(r)$  et  $f_2(r)$  ont le même schéma relationnel, puis, on montrera que  $f_1(r) \subset f_2(r)$  et ensuite que  $f_2(r) \subset f_1(r)$ .

On aura ainsi démontré par double inclusion que  $f_1(r) = f_2(r)$ .

Dans toutes les démonstrations qui suivent, quand on dit de deux fonctions  $f$  et  $g$  qu'elles coïncident sur un ensemble  $d$ , on entend par là qu'elles coïncident sur  $D_f \cap D_g \cap d$ .

## Lois de projection

### Projection et projection

$$\pi_{\delta_1} \circ \dots \circ \pi_{\delta_n} = \pi_{\delta_1 \cap \dots \cap \delta_n} \quad (1)$$

Soit  $r$  une relation. On pose  $res_1 = \pi_{\delta_1} \circ \dots \circ \pi_{\delta_n}(r)$  et  $res_2 = \pi_{\delta_1 \cap \dots \cap \delta_n}(r)$

### Schéma relationnel

On peut démontrer par récurrence sur  $n$  que le schéma relationnel de  $res_1$  est

$$\text{sch}(res_1) = \text{sch}(r) \cap \bigcap_{i \in \{1, \dots, n\}} \delta_i$$

De même, par définition de la projection, on a

$$\text{sch}(res_2) = \text{sch}(r) \cap \bigcap_{i \in \{1, \dots, n\}} \delta_i$$

Donc  $\text{sch}(res_1) = \text{sch}(res_2)$

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Il existe  $l'$  une ligne de  $r$  telle que  $l = ((l'|_{\delta_n \cup \{id\}})|\dots)|_{\delta_1 \cup \{id\}} = l'|_{(\delta_1 \cap \dots \cap \delta_n) \cup \{id\}}$ . Or, par définition de la projection  $\pi_{\delta_1 \cap \dots \cap \delta_n}$ , on a  $l'|_{(\delta_1 \cap \dots \cap \delta_n) \cup \{id\}} \in res_2$ . Donc  $l \in res_2$ .

Ainsi,  $res_1 \subset res_2$ .

### Deuxième inclusion

De même, si  $l$  est un élément de  $res_2$ , alors il existe une ligne  $l'$  de  $r$  telle que  $l = l'|_{(\delta_1 \cap \dots \cap \delta_n) \cup \{id\}} = ((l'|_{\delta_n \cup \{id\}})|_{\dots})|_{\delta_1 \cup \{id\}}$  et, par définition de  $\pi_{\delta_1} \circ \dots \circ \pi_{\delta_n}$ , on a  $((l'|_{\delta_n \cup \{id\}})|_{\dots})|_{\delta_1 \cup \{id\}} \in res_1$ , d'où  $l \in res_1$  et  $res_2 \subset res_1$ .

### Projection et sélection

$$\pi_\delta \circ \sigma_p = \sigma_p \circ \pi_\delta \quad \text{si } \text{dom}(p) \subset \delta \quad (2)$$

Soit  $\delta$  un ensemble de noms d'attributs et  $p$  un prédicat sur les lignes tel que  $\text{dom}(p) \subset \delta$ .

Soit  $r$  une relation. On pose  $res_1 = (\pi_\delta \circ \sigma_p)(r)$  et  $res_2 = (\sigma_p \circ \pi_\delta)(r)$

### Schéma relationnel

Une sélection ne modifiant jamais le schéma relationnel d'une relation, la schéma relation de  $res_1$  et de  $res_2$  est  $\text{sch}(r) \cap \delta$ .

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Il existe une ligne  $l'$  de  $\sigma_p(res_1)$  telle que  $l = l'|_{(\text{sch}(r) \cap \delta) \cup \{id\}}$ .

Puisque  $l$  et  $l'$  coïncident sur  $\delta$  et que  $\text{dom}(p) \subset \delta$ , on a  $p(l) = p(l') = \text{true}$ .

Or, par définition de  $\pi_\delta$ ,  $l' \in \pi_\delta(r)$ , donc  $l' \in \sigma_p(\pi_\delta(r)) = res_2$ .

Ainsi,  $res_1 \subset res_2$ .

### Deuxième inclusion

De même, si  $l$  est un élément de  $res_2$ , alors  $p(l) = \text{true}$  et  $l \in \pi_\delta(r)$  donc il existe une ligne  $l'$  dans  $r$  telle que  $l = l'|_{(\text{sch}(r) \cap \delta) \cup \{id\}}$ .  $l$  et  $l'$  coïncident sur  $\delta$  qui contient le domaine de  $p$ ,  $l'$  vérifie le prédicat  $p$  donc  $l' \in \sigma_p(r)$ .

On en déduit par définition de  $\pi_\delta$  que  $l \in res_1$ .

Ainsi,  $res_2 \subset res_1$ .

### Projection et défragmentation (verticale)

En appelant  $\delta_1$  le schéma relationnel du premier argument et  $\delta_2$  le schéma relationnel du deuxième argument, on a :

$$\pi_\delta \circ \text{defrag} = \text{defrag} \circ (\pi_\delta, \pi_\delta) \quad \text{si } \delta_1 \cap \delta_2 = \emptyset \quad (3)$$

Soit  $\delta$  un ensemble de noms d'attributs. Soient  $r_1$  et  $r_2$  deux relations unifiables.

On pose  $res_1 = (\pi_\delta \circ \text{defrag})(r_1, r_2)$  et  $res_2 = \text{defrag} \circ (\pi_\delta, \pi_\delta)(r_1, r_2)$ .

**Remarque :** L'hypothèse «  $r_1$  et  $r_2$  unifiables » garantit que les  $res_1$  et  $res_2$  sont bien définies. En effet, non seulement elle garantit que  $\text{defrag}(r_1, r_2)$  existe et donc que  $res_1$  existe (la projection a été définie sur  $R$  tout entier), mais elle garantit également que  $(\delta_1 \cap \delta) \cap (\delta_2 \cap \delta) = \emptyset$  et donc (vu que les projections conservent les identifiants) que  $\pi_\delta(r_1)$  et  $\pi_\delta(r_2)$  sont unifiables, donc que  $res_2$  existe.

### Schémas relationnels

Le schéma relationnel de  $\text{defrag}(r_1, r_2)$  est  $\delta_1 \cup \delta_2$ , donc celui de  $\text{res}_1$  est  $\delta \cap (\delta_1 \cup \delta_2)$ .

Les schémas relationnels de  $\pi_\delta(r_1)$  et de  $\pi_\delta(r_2)$  sont respectivement  $\delta \cap \delta_1$  et  $\delta \cap \delta_2$ , donc le schéma relationnel de  $\text{res}_2$  est  $(\delta \cap \delta_1) \cup (\delta \cap \delta_2) = \delta \cap (\delta_1 \cup \delta_2)$

### Première inclusion

Soit  $l$  une ligne de  $\text{res}_1$ .

Il existe  $l_0$  une ligne de  $\text{defrag}(r_1, r_2)$  de schéma relationnel  $\delta_1 \cup \delta_2$  telle que  $l = l_0|_{\delta \cup \{id\}}$ . Il existe donc deux lignes  $l_1$  et  $l_2$  appartenant respectivement à  $r_1$  et  $r_2$  telles que  $l_1 = l_0|_{\delta_1 \cup \{id\}}$   $l_2 = l_0|_{\delta_2 \cup \{id\}}$

Puisque  $l_1$  appartient à  $r_1$ , il existe une ligne  $l'_1$  dans  $\pi_\delta(r_1)$  telle que  $l'_1 = l_1|_{\delta \cup \{id\}} = l_0|_{(\delta \cap \delta_1) \cup \{id\}}$ . De même, il existe une ligne  $l'_2$  dans  $\pi_\delta(r_2)$  telle que  $l'_2 = l_2|_{\delta \cup \{id\}} = l_0|_{(\delta \cap \delta_2) \cup \{id\}}$ .

De l'existence de  $l'_1$  et  $l'_2$  qui partagent même identifiant (et portent sur des schémas relationnels disjoints) on en déduit que  $l'_1.l'_2$  appartient à  $\text{res}_2$ .

Or,

$$\begin{aligned} l'_1.l'_2 &= l_0|_{((\delta \cap \delta_1) \cup \{id\}) \cup ((\delta \cap \delta_2) \cup \{id\})} \\ &= l_0|_{(\delta \cap (\delta_1 \cup \delta_2)) \cup \{id\}} \\ &= (l_0|_{\delta_1 \cup \delta_2 \cup \{id\}})|_{\delta \cup \{id\}} \\ &= l_0|_{\delta \cup \{id\}} = l \end{aligned}$$

Donc :  $l \in \text{res}_2$ .

### Deuxième inclusion

Soit  $l$  une ligne de  $\text{res}_2$ .

Il existe des lignes  $l'_1$  et  $l'_2$  appartenant respectivement à  $\pi_\delta(r_1)$  et  $\pi_\delta(r_2)$  telles que  $l = l'_1.l'_2$ .

On en déduit qu'il existe deux lignes  $l_1$  et  $l_2$  appartenant respectivement à  $r_1$  et  $r_2$  telles que  $l'_1 = l_1|_{\delta \cup \{id\}}$  et  $l'_2 = l_2|_{\delta \cup \{id\}}$ .

$r_1$  et  $r_2$  étant unifiables, et  $l_1$  et  $l_2$  ayant même identifiant,  $l_1$  et  $l_2$  sont des lignes correspondantes et on peut donc considérer  $l_1.l_2$ .

On a d'ailleurs  $l = l'_1.l'_2 = (l_1|_{\delta \cup \{id\}}).(l_2|_{\delta \cup \{id\}}) = (l_1.l_2)|_{\delta \cup \{id\}}$ .

Or,  $l_1.l_2$  appartient à  $\text{defrag}(r_1, r_2)$  donc  $l = (l_1.l_2)|_{\delta \cup \{id\}}$  appartient à  $\text{res}_1$

### Projection et déchiffrement d'un attribut projeté ou non

$$\pi_\delta \circ \text{decrypt}_{\alpha, c} \equiv \text{decrypt}_{\alpha, c} \circ \pi_\delta \quad (4)$$

Soit  $\delta$  un ensemble de noms d'attributs et  $\alpha$  un attribut (appartenant à  $\delta$  ou pas). Soit  $r$  une relation. On pose  $\text{res}_1 = (\pi_\delta \circ \text{decrypt}_{\alpha, c})(r)$  et  $\text{res}_2 = (\text{decrypt}_{\alpha, c} \circ \pi_\delta)(r)$ .

### Schémas relationnels

Le déchiffrement ne changeant pas le schéma relationnel d'une relation, le schéma relationnel de  $\text{res}_1$  et  $\text{res}_2$  est  $\text{sch}(r) \cap \delta$ .

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Il existe  $l'$  une ligne de  $\text{decrypt}_{\alpha,c}(r)$  telle que  $l = l'|_{\delta \cup \{id\}}$ .  $l'$  étant un élément de  $\text{decrypt}_{\alpha,c}(r)$ , il existe une ligne  $l_0$  de  $r$  telle que  $l' = c^{-1}(l_0)_\alpha$  et donc  $l = c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}$ .

Puisque  $l_0$  appartient à  $r$ ,  $l_0|_{\delta \cup \{id\}}$  appartient à  $\pi_\delta(r)$  et donc  $c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$  appartient à  $res_2$ .

Montrons que  $c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}} = c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$ . Les deux fonctions en question sont définies sur  $(\text{sch}(r) \cap \delta) \cup \{id\}$ .

Soit :  $\beta \in (\text{sch}(r) \cap \delta) \cup \{id\}$ .

Si  $\beta \neq \alpha$ , on a :

$$\begin{cases} c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}(\beta) &= c^{-1}(l_0)_\alpha(\beta) = l_0(\beta) \\ c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha(\beta) &= l_0|_{\delta \cup \{id\}}(\beta) = l_0(\beta) \end{cases}$$

Si  $\alpha \in \text{sch}(r) \cap \delta$ , on a :

$$\begin{cases} c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}(\alpha) &= c^{-1}(l_0)_\alpha(\alpha) = c^{-1}(l_0(\alpha)) \\ c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha(\alpha) &= c^{-1}(l_0|_{\delta \cup \{id\}}(\alpha)) = c^{-1}(l_0(\alpha)) \end{cases}$$

Ainsi,  $c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}} = c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$  donc  $l$  appartient à  $res_2$ .

### Deuxième inclusion

Soit  $l$  une ligne de  $res_2$ .

Il existe une ligne  $l'$  de  $\pi_\delta(r)$  telle que  $l = c^{-1}(l')_\alpha$ .

Puisque  $l'$  appartient à  $\pi_\delta(r)$ , il existe  $l_0$  dans  $r$  telle que  $l' = l_0|_\delta$  et donc telle que  $l = c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$ .

Vu que  $l_0$  appartient à  $r$ ,  $c^{-1}(l_0)_\alpha$  appartient à  $\text{decrypt}_{\alpha,c}(r)$  et  $c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}$  appartient à  $res_1$ .

Or,  $l_0$  étant une ligne de  $r$ , d'après la démonstration faite pour la première inclusion, on a :  $c^{-1}(l_0)_\alpha|_{\delta \cup \{id\}} = c^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$ .

On en déduit que  $l$  appartient à  $res_1$ .

### Projection et déchiffrement d'un attribut non projeté

$$\pi_\delta \circ \text{decrypt}_{\alpha,c} \equiv \pi_\delta \quad \text{si } \alpha \notin \delta \quad (5)$$

Soit  $\delta$  un ensemble de noms d'attributs et  $\alpha$  un attribut n'appartenant pas à  $\delta$ . Soit  $r$  une relation. On pose  $res_1 = (\pi_\delta \circ \text{decrypt}_{\alpha,c})(r)$  et  $res_2 = (\text{decrypt}_{\alpha,c} \circ \pi_\delta)(r)$ .

### Schémas relationnels

Le déchiffrement ne changeant pas le schéma relationnel d'une relation, le schéma relationnel de  $res_1$  et  $res_2$  est  $\text{sch}(r) \cap \delta$ .

## Inclusions

La seule chose qui change est la démonstration du fait que pour toute ligne  $l_0$  de  $r$   $\mathbf{c}^{-1}(l_0)_\alpha|_{\delta \cup \{id\}} = \mathbf{c}^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$ .

En effet, si on suppose  $\alpha \notin \delta$ , un seul cas se présente, à savoir  $\beta \in (\text{sch}(r) \cap \delta) \cup \{id\} \wedge \beta \neq \alpha$ , et on a alors

$$\begin{cases} \mathbf{c}^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}(\beta) &= \mathbf{c}^{-1}(l_0)_\alpha(\beta) = l_0(\beta) \\ \mathbf{c}^{-1}(l_0|_{\delta \cup \{id\}})_\alpha(\beta) &= l_0|_{\delta \cup \{id\}}(\beta) = l_0(\beta) \end{cases}$$

d'où l'égalité voulue.

À partir de là, si  $l$  est une ligne de  $res_1$ , elle s'écrit  $\mathbf{c}^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}$  avec  $l_0 \in r$  et  $\mathbf{c}^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$  appartient à  $res_2$  donc  $l$  appartient à  $res_2$ .

Inversement, si  $l$  est une ligne de  $res_2$ , elle s'écrit  $\mathbf{c}^{-1}(l_0|_{\delta \cup \{id\}})_\alpha$  avec  $l_0 \in r$  et  $\mathbf{c}^{-1}(l_0)_\alpha|_{\delta \cup \{id\}}$  appartient à  $res_1$  donc  $l$  appartient à  $res_1$ .

## Projection et jointure

En appelant  $\delta_1$  le schéma relationnel du premier argument et  $\delta_2$  le schéma relationnel du deuxième argument, on a :

$$\pi_\delta \circ \bowtie = \bowtie \circ (\pi_\delta, \pi_\delta) \quad \text{si } \delta_1 \cap \delta_2 \subset \delta \quad (6)$$

Soit  $\delta$  un ensemble de noms d'attributs, et  $r_1$  et  $r_2$  des relations. On pose  $res_1 = (\pi_\delta \circ \bowtie)(r_1, r_2)$  et  $res_2 = (\bowtie \circ (\pi_\delta, \pi_\delta))(r_1, r_2)$ .

## Schémas relationnels

Le schéma relationnel de  $r_1 \bowtie r_2$  est  $\text{sch}(r_1) \cup \text{sch}(r_2)$  donc celui de  $res_1$  est  $(\text{sch}(r_1) \cup \text{sch}(r_2)) \cap \delta$ .

Les schémas relationnels respectifs de  $\pi_\delta(r_1)$  et  $\pi_\delta(r_2)$  sont  $\text{sch}(r_1) \cap \delta$  et  $\text{sch}(r_2) \cap \delta$  donc celui de  $res_2$  est  $(\text{sch}(r_1) \cap \delta) \cup (\text{sch}(r_2) \cap \delta) = (\text{sch}(r_1) \cup \text{sch}(r_2)) \cap \delta$ .

## Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Il existe une ligne  $l'$  de  $r_1 \bowtie r_2$  telle que  $l = l'|_{\delta \cup \{id\}}$ . Puisque  $l'$  appartient à  $r_1 \bowtie r_2$ , il existe deux lignes  $l_1$  et  $l_2$  appartenant respectivement à  $r_1$  et  $r_2$  telles que  $l' = l_1.l_2$ . Ainsi,  $l = (l_1.l_2)|_{\delta \cup \{id\}}$ .

Puisque  $l_1$  et  $l_2$  se correspondent et que  $\delta_1 \cap \delta_2 \subset \delta$ ,  $l_1|_{\delta \cup \{id\}}$  et  $l_2|_{\delta \cup \{id\}}$  se correspondent aussi. Or,  $l_1|_{\delta \cup \{id\}}$  (respectivement  $l_2|_{\delta \cup \{id\}}$ ) appartient à  $\pi_\delta(r_1)$  (resp.  $\pi_\delta(r_2)$ ), donc  $l_1|_{\delta \cup \{id\}}.l_2|_{\delta \cup \{id\}}$  appartient à  $res_2$ .

Montrons que  $(l_1.l_2)|_{\delta \cup \{id\}} = l_1|_{\delta \cup \{id\}}.l_2|_{\delta \cup \{id\}}$ . Ces deux fonctions sont définies sur  $((\delta_1 \cup \delta_2) \cap \delta) \cup \{id\}$ . Soit  $\beta$  un élément de  $(\delta_1 \cup \delta_2) \cap \delta$ .

$$(l_1.l_2)|_{\delta \cup \{id\}}(\beta) = l_1.l_2(\beta) = \begin{cases} l_1(\beta) & \text{si } \beta \in \delta_1 \\ l_2(\beta) & \text{si } \beta \in \delta_2 \end{cases}$$

$$l_1|_{\delta \cup \{id\}}.l_2|_{\delta \cup \{id\}}(\beta) = \begin{cases} l_1|_{\delta \cup \{id\}}(\beta) = l_1(\beta) & \text{si } \beta \in \delta_1 \\ l_2|_{\delta \cup \{id\}}(\beta) = l_2(\beta) & \text{si } \beta \in \delta_2 \end{cases}$$

De plus,  $(l_1.l_2)|_{\delta \cup \{id\}}(id) = l_1|_{\delta \cup \{id\}}.l_2|_{\delta \cup \{id\}}(id) = l_1(id).l_2(id)$ . Donc on a bien l'égalité souhaitée et on en déduit que  $l$  appartient à  $res_2$ .

## Deuxième inclusion

Soit  $l$  une ligne de  $res_2$ .

Il existe deux lignes  $l'_1$  et  $l'_2$  de  $\pi_\delta(r_1)$  et  $\pi_\delta(r_2)$  respectivement telles que  $l = l'_1.l'_2$ . Or, il existe deux lignes  $l_1$  et  $l_2$  appartenant respectivement à  $r_1$  et  $r_2$  telles que  $l'_1 = l_1|_{\delta \cup \{id\}}$  et  $l'_2 = l_2|_{\delta \cup \{id\}}$ .

Donc  $l = l_1|_{\delta \cup \{id\}}.l_2|_{\delta \cup \{id\}}$ .

D'autre part, vu que  $l_1|_{\delta \cup \{id\}}$  et  $l_2|_{\delta \cup \{id\}}$  se correspondent,  $l_1|_{\delta \cup \{id\}}$  et  $l_2|_{\delta \cup \{id\}}$  coïncident sur  $((\delta_1 \cap \delta) \cap (\delta_2 \cap \delta))$ . Or,  $\delta_1 \cap \delta_2 \subset \delta$ , donc  $l_1$  et  $l_2$  coïncident sur  $\delta_1 \cap \delta_2$  donc  $l_1$  et  $l_2$  se correspondent et donc  $l_1.l_2$  appartient à  $r_1 \bowtie r_2$ .

On en déduit que  $(l_1.l_2)|_{\delta \cup \{id\}}$  appartient à  $res_1$ .

Grâce à l'égalité prouvée lors de la preuve de l'autre inclusion, on en déduit que  $l$  appartient à  $res_1$ .

## Projection et agrégation

$$\text{group}_\delta \circ \pi_{\delta'} \equiv \pi_{\delta'} \circ \text{group}_\delta \quad \text{si } \delta \subset \delta'$$

Soient  $\delta$  et  $\delta'$  deux ensembles de noms d'attributs.

Soit  $\delta_1$  le schéma relationnel de l'argument.

Soit  $r$  une relation. On pose  $res_1 = (\text{group}_\delta \circ \pi_{\delta'})(r)$  et  $res_2 = (\pi_{\delta'} \circ \text{group}_\delta)(r)$ .

## Schémas relationnels

La fonction  $\text{group}$  préserve les schémas relationnels, donc  $res_1$  et  $res_2$  ont tous deux pour schémas relationnels  $\delta_1 \cap \delta'$ .

### Premier cas : si $\delta$ est vide

Dans ce cas-là, pour montrer que  $res_1 = res_2$ , on va directement calculer  $res_1$  et  $res_2$ .

#### Calcul de $res_1$ :

Le seul nom de groupe minimal de  $\pi_{\delta'}(r)$  pour  $\delta = \emptyset$  est l'application vide qu'on notera également  $\emptyset$ .

Donc,  $res_1$  a une seule ligne, à savoir  $\text{lg}_{\pi_{\delta'}(r), \emptyset}$ , qu'on appellera, pour simplifier les notations,  $l_1$ .

$l_1$  est définie sur  $(\delta_1 \cap \delta') \cup \{id\}$  et est entièrement déterminée par

$$\forall \alpha \in (\delta_1 \cap \delta') \cup \{id\}, l_1(\alpha) = r_\emptyset(\alpha)$$

#### Calcul de $res_2$ :

De même, le seul nom de groupe minimal de  $r$  pour  $\emptyset$  est  $\emptyset$  donc  $\text{group}_\delta(r)$  a un seul élément, que nous appellerons  $l'_2$  qui est défini sur  $\delta_1 \cup \{id\}$  par  $\forall \alpha \in \delta_1 \cup \{id\}, l'_2(\alpha) = r_\emptyset(\alpha)$ .

On en déduit que  $res_2$  a une seule ligne, que nous appellerons  $l_2$ .

$l_2$  est définie sur  $(\delta_1 \cap \delta) \cup \{id\}$  par

$$\forall \alpha \in (\delta_1 \cap \delta) \cup \{id\}, l_2(\alpha) = r_\emptyset(\alpha)$$

Donc on a  $l_1 = l_2$  et on en déduit  $res_1 = res_2$ .

## Deuxième cas : si $\delta$ est non vide

### Première inclusion :

Soit  $l$  une ligne de  $res_1$ .

Soit  $n$  un nom de groupe sur  $\delta$  associé (i. e.  $n = l|_\delta$ ).

Pour simplifier les notations, on pose  $r' = \pi_{\delta'}(r)$ .

Il existe  $l'_1, \dots, l'_m$  des lignes distinctes de  $r'$  telles que  $r'_n = \{l'_1, \dots, l'_m\}$ .

Les  $l'_i$  appartenant à  $r'$ , il existe des lignes  $l_1, \dots, l_m$  de  $r$  telles que

$$\forall i \in \{1, \dots, n\}, l'_i = l_i|_{\delta' \cup \{id\}}$$

Montrons par double inclusion que  $\{l_1, \dots, l_m\} = r_n$ .

Les  $l'_1, \dots, l'_m$  sont les restriction des  $l_1, \dots, l_m$  à  $\delta'$  et elles coïncident entre elles sur  $\delta$ . Or  $\delta \subset \delta'$  donc les  $l_1, \dots, l_m$  coïncident sur  $\delta$ . On en déduit que  $\{l_1, \dots, l_m\} \subset r_n$ .

Soit maintenant  $l_0$  un élément de  $r_n$ . Puisque  $l_1$  appartient à  $r_n$ ,  $l_0$  coïncide avec  $l_1$  sur  $\delta$ ; donc  $l_0|_{\delta' \cup \{id\}}$  coïncide sur  $\delta$  avec  $l_1|_{\delta' \cup \{id\}}$ , et par conséquent avec  $n$  donc  $l_0|_{\delta' \cup \{id\}} \in r'_n$ .

On en déduit qu'il existe  $i \in \{1, \dots, n\}$  tel que  $l_0|_{\delta' \cup \{id\}} = l'_i$ .

$l_0$  coïncide donc avec  $l_i$  sur  $\delta' \cup \{id\}$  donc en particulier  $l_0(id) = l_i(id)$  et, comme l'identifiant de chaque ligne dans une relation est supposé unique et  $l_0$  et  $l_1$  appartiennent tous les deux à la relation  $r$ , on a :  $l_0 = l_i$ .

Ainsi,  $l_0 \in \{l_1, \dots, l_m\}$ .

On en déduit que  $r_n \subset \{l_1, \dots, l_m\}$  et on a donc l'égalité.

On pose  $l' = (lg_{r,n})|_{\delta' \cup \{id\}}$ , qui est donc un élément de  $res_2$ .

Montrons que  $l' = l$ .

Ces deux fonctions sont définies sur  $\delta' \cup \{id\}$ , et pour  $\alpha \in \delta' \cup \{id\}$  on a :

$$\begin{cases} l'(\alpha) = n(\alpha) = l(\alpha) & \text{si } \alpha \in \delta \\ l'(\alpha) = r_n(\alpha) = r'_n(\alpha) = l(\alpha) & \text{si } \alpha \notin \delta \end{cases}$$

d'où l'égalité.

On en déduit que  $l$  appartient à  $res_2$ , d'où la première inclusion.

### Deuxième inclusion :

Soit  $l$  une ligne de  $res_2$ .

Soit  $n$  un nom de groupe pour  $\delta$  tel que  $l = lg_{r,n}|_{\delta' \cup \{id\}}$ .

Il existe des lignes  $l_1, \dots, l_m$  telles que  $r_n = \{l_1, \dots, l_m\}$ .

En appelant  $r'$  la relation  $\pi_{\delta'}(r)$  et en appelant, pour  $i$  dans  $\{1, \dots, m\}$ ,  $l'_i = l_i|_{\delta' \cup \{id\}}$  montrons par double inclusion que  $r'_n = \{l'_1, \dots, l'_m\}$ .

Puisque les  $l_1, \dots, l_m$  et  $n$  coïncident sur  $\delta$ , leurs restrictions  $l'_1, \dots, l'_m$  coïncident sur  $\delta$  également et coïncident sur  $\delta$  avec  $n$ , donc  $\{l'_1, \dots, l'_m\} \subset r'_n$ .

Dans l'autre sens, soit  $l'_0$  un élément de  $r'_n$ . Il existe  $l_0$  élément de  $r$  tel que  $l'_0 = l_0|_{\delta' \cup \{id\}}$ . Puisque  $l'_0$  coïncide avec  $n$  sur  $\delta$ , que  $\delta \subset \delta'$  et que  $l_0$  coïncide avec  $l'_0$  sur  $\delta'$ ,  $l_0$  coïncide avec  $n$  sur  $\delta$ , d'où  $l_0 \in r_n$ .

On en déduit qu'il existe  $i$  dans  $\{1, \dots, m\}$  tel que  $l_0 = l_i$ . Par définition de  $l_0$  et des  $l'_i$ , on en déduit que  $l'_0 = l'_i$ , donc que  $l'_0 \in \{l'_1, \dots, l'_m\}$ .

Ainsi,  $r'_n \subset \{l'_1, \dots, l'_m\}$ , d'où l'égalité.

## Projection et réduction d'un attribut projeté ou non

$$\text{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \circ \text{fold}_{\alpha,f,z} \quad (7)$$

Soit  $\delta$  un ensemble de noms d'attributs,  $\alpha$  un attribut,  $f$  une fonction de  $\mathcal{V}$  dans  $val$  et  $z$  un élément de  $\mathcal{V}$ .

Soit  $r$  une relation. On pose  $res_1 = (\text{fold}_{\alpha,f,z} \circ \pi_\delta)(r)$  et  $res_2 = (\pi_\delta \circ \text{fold}_{\alpha,f,z})(r)$ .

### Schémas relationnels

Ni la projection ni la réduction ne changent les schémas relationnels, donc  $res_1$ ,  $r$  et  $res_2$  ont tous les trois le même schéma relationnel.

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Il existe  $l'$  dans  $\pi_\delta(r)$  telle que  $l = \text{red}_{\alpha,f,z,l'}(l')$  et  $l''$  dans  $r$  telle que  $l' = l''|_{\delta \cup \{id\}}$ .

$l''$  appartient à  $r$  donc  $\text{red}_{\alpha,f,z,l''}(l'')$  appartient à  $\text{fold}_{\alpha,f,z}(r)$  et, en posant  $\tilde{l} = \text{red}_{\alpha,f,z,l''}(l'')$ ,  $\tilde{l}$  appartient à  $res_2$ .

Montrons que  $l = \tilde{l}$ .

Soit  $\beta \in (\text{sch}(r) \cap \delta) \cup \{id\}$ .

Si  $\beta \neq \alpha$ , on a :

$$\tilde{l}(\beta) = \text{red}_{\alpha,f,z,l''}(\beta) = l''(\beta) = l'(\beta) = \text{red}_{\alpha,f,z,l'}(\beta) = l(\beta)$$

Si  $\beta = \alpha$ , on a :

$$\tilde{l}(\alpha) = \text{red}_{\alpha,f,z,l''}(\alpha) = \text{red}_{f,z}(l''(\alpha)) = \text{red}_{f,z}(l'(\alpha)) = \text{red}_{\alpha,f,z,l'}(\alpha) = l(\alpha)$$

Puisqu'on a l'égalité souhaitée, on peut en déduire que  $l$  appartient à  $res_2$ , d'où la première inclusion.

### Deuxième inclusion

Puisque la projection comme la réduction préservent le nombre de lignes dans la relation,  $res_1$  et  $res_2$  sont des ensembles finis ayant tous les deux le même cardinal (à savoir le cardinal de  $r$ ). Donc la première inclusion implique la deuxième.

## Projection et réduction d'un attribut non projeté

$$\text{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \quad \text{si } \alpha \notin \delta \cup \{id\} \quad (8)$$

Soit  $\delta$  un ensemble de noms d'attributs,  $\alpha$  un attribut,  $f$  une fonction de  $\mathcal{V}$  dans  $val$  et  $z$  un élément de  $\mathcal{V}$ .

Soit  $r$  une relation. On pose  $res_1 = (\text{fold}_{\alpha,f,z} \circ \pi_\delta)(r)$  et  $res_2 = \pi_\delta(r)$



## Schéma et cardinal

Pour les mêmes raisons que lors de la démonstration précédente,  $res_1$  et  $res_2$  ont tous les deux le même schéma relationnel et le même cardinal que  $r$ .

### Inclusion de $res_2$ dans $res_1$

Soit  $l$  une ligne de  $res_2$ .

On pose  $l' = \text{red}_{\alpha, f, z, l}$ , qui est un élément de  $res_1$ .

Montrons que  $l = l'$ .

Ces deux lignes là sont définies sur  $(\text{sch}(r) \cap \delta) \cup \{id\}$ .

Pour  $\beta \in (\text{sch}(r) \cap \delta) \cup \{id\}$ , on a forcément  $\beta \neq \alpha$  car  $\alpha \notin \delta \cup \{id\}$ , donc

$$l'(\beta) = l(\beta)$$

d'où l'égalité entre  $l$  et  $l'$  et l'appartenance de  $l$  à  $res_1$ .

Ainsi,  $res_2 \subset res_1$ . Vu que de plus les deux ensembles sont finis de même cardinal, on en déduit qu'ils sont égaux.

## Lois de sélection

### Sélection et sélection

$$\sigma_{p_1} \circ \dots \circ \sigma_{p_n} \equiv \sigma_{p_1 \wedge \dots \wedge p_n} \quad (9)$$

Vu que le ET logique est associatif, pour démontrer cette loi, il suffit de le démontrer pour deux sélections.

Soient  $p_1$  et  $p_2$  deux prédicats et  $r$  une relation.

On pose  $res_1 = (\sigma_{p_1} \circ \sigma_{p_2})(r)$  et  $res_2 = \sigma_{p_1 \wedge p_2}(r)$ .

### Schémas relationnels

La sélection préserve le schéma relationnel, donc  $res_1$  et  $res_2$  ont tous les deux le même schéma relationnel que  $r$ .

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

Puisque  $l$  appartient à  $res_1$ ,  $l$  appartient à  $\sigma_{p_2}(r)$  et  $l$  vérifie  $p_1$ .

Or, si  $l$  appartient à  $\sigma_{p_2}(r)$ ,  $l$  appartient à  $r$  et vérifie  $p_2$ .

Donc  $l$  appartient à  $r$  et vérifie à la fois  $p_1$  et  $p_2$ , donc vérifie  $p_1 \wedge p_2$ .

Par conséquent,  $l$  appartient à  $res_2$ .

On en déduit que  $res_1 \subset res_2$ .

### Deuxième inclusion

Soit  $l$  un élément de  $res_2$ .

Puisque  $l$  appartient à  $res_2$ ,  $l$  appartient à  $r$  et vérifie  $p_1 \wedge p_2$ .

On en déduit que  $l$  vérifie  $p_1$  et  $p_2$ .

Comme  $l$  appartient à  $r$  et vérifie  $p_2$ ,  $l$  appartient aussi à  $\sigma_{p_2}(r)$ . Or  $l$  vérifie  $p_1$ , donc  $l$  appartient à  $\sigma_{p_1}(\sigma_{p_2}(r))$ , autrement connue sous le nom de  $res_1$ .

On en déduit que  $res_2 \subset res_1$ .

### Sélection et défragmentation

En appelant  $\delta_1$  le schéma relationnel du premier argument, et  $\delta_2$  le schéma relationnel du deuxième argument,

$$\sigma_p \circ \text{defrag} \equiv \text{defrag} \circ (\sigma_p, \text{id}) \quad \text{si } \text{dom}(p) \subset \delta_1 \quad (10)$$

$$\sigma_p \circ \text{defrag} \equiv \text{defrag} \circ (\text{id}, \sigma_p) \quad \text{si } \text{dom}(p) \subset \delta_2 \quad (11)$$

Les démonstrations des deux lois étant tout à fait analogues, je ne démontrerai que la loi (10).

Soit  $p$  un prédicat sur les lignes. Soient  $r_1$  et  $r_2$  deux relations unifiables.

On pose  $res_1 = \sigma_p(\text{defrag}(r_1, r_2))$  et  $res_2 = \text{defrag}(\sigma_p(r_1), r_2)$ .

### Schémas relationnels et unifiabilité

La sélection préserve le schéma relationnel, donc  $r_1$  et  $r_2$  sont unifiables si et seulement si  $\sigma_p(r_1)$  et  $r_2$  le sont.

De plus, le schéma relationnel après défragmentation est l'union des schémas relationnels initiaux, donc les schémas relationnels de  $res_1$  et  $res_2$  sont tous les deux  $\delta_1 \cup \delta_2$ .

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

$l$  vérifie la propriété  $p$  et appartient aussi à  $\text{defrag}(r_1, r_2)$ . Or, puisque  $\text{dom}(p) \subset \delta_1$ , toute ligne coïncidant avec  $l$  sur  $\delta_1$  vérifie la propriété  $p$ .

Il existe deux lignes  $l_1$  et  $l_2$  appartenant respectivement à  $r_1$  et  $r_2$  telles que  $l = \text{Unif}(l_1, l_2)$ .  $l_1$  coïncide avec  $l$  sur  $\delta_1 \cup \{\text{id}\}$  donc sur  $\delta_1$ , donc  $l_1$  vérifie la propriété  $p$ .

On en déduit que  $l_1$  appartient à  $\sigma_p(r_1)$ . Or  $l_2$  appartient à  $r_2$  et, par définition,  $l_1$  et  $l_2$  sont unifiables, donc  $l = \text{Unif}(l_1, l_2)$  appartient à  $\text{defrag}(\sigma_p(r_1), r_2) = res_2$ .

### Deuxième inclusion

Soit  $l$  une ligne de  $res_2$ .

Il existe  $l_1$  et  $l_2$  unifiables appartenant respectivement à  $\sigma_p(r_1)$  et  $r_2$  telles que  $l = \text{Unif}(l_1, l_2)$ .

Puisque  $l_1$  appartient à  $\sigma_p(r_1)$ ,  $l_1$  vérifie la condition  $p$  et appartient à  $r_1$ .

Or  $l_2$  appartient à  $r_2$  et  $l_1$  et  $l_2$  sont unifiables, donc  $l = \text{Unif}(l_1, l_2)$  appartient à  $\text{defrag}(r_1, r_2)$ .

Puisque  $l_1$  coïncide avec  $l$  sur son domaine de définition qui contient  $\delta_1$  qui lui même contient  $\text{dom}(p)$  et que  $l_1$  vérifie  $p$ ,  $l$  vérifie  $p$ .

On en déduit que  $l$  appartient à  $\sigma_p(\text{defrag}(r_1, r_2)) = res_1$ .

## Sélection et déchiffrement non sélectif

$$\sigma_p \circ \text{decrypt}_{\alpha, c} = \text{decrypt}_{\alpha, c} \circ \sigma_p \quad \text{si } \alpha \notin \text{dom}(p) \quad (12)$$

Soit  $p$  un prédicat sur les lignes,  $c$  un chiffrement et  $\alpha$  un attribut n'étant pas contenu dans le domaine de  $p$ .

Soit  $r$  une relation et  $\delta_1$  son schéma relationnel.

On pose  $res_1 = \sigma_p(\text{decrypt}_{\alpha, c}(r))$  et  $res_2 = \text{decrypt}_{\alpha, c}(\sigma_p(r))$ .

### Schémas relationnels

La sélection et le déchiffrement préservant tous deux les schémas relationnels,  $res_1$  et  $res_2$  ont tous deux pour schéma relationnel  $\delta_1$ .

### Première inclusion

Soit  $l$  une ligne de  $res_1$ .

$l$  appartient à  $\text{decrypt}_{\alpha, c}(r)$  et  $l$  vérifie la propriété  $p$ .

Il existe une ligne  $l'$  de  $r$  telle que  $l = c^{-1}(l')_\alpha$ .

Puisque  $l$  et  $l'$  (qui sont toutes deux définies sur  $\delta_1 \cup \{id\}$ ) coïncident partout sauf éventuellement sur  $\alpha$  mais que le domaine de  $p$  ne contient pas  $\alpha$ , on a  $l|_{\text{dom}(p)} = l'|_{\text{dom}(p)}$ . De plus,  $l$  vérifie la propriété  $p$  donc  $l'$  vérifie la propriété  $p$ .

On en déduit que  $l'$  appartient à  $\sigma_p(r)$ .

Par conséquent,  $l = c^{-1}(l')_\alpha$  appartient à  $\text{decrypt}_{\alpha, c}(\sigma_p(r)) = res_2$ .

### Deuxième inclusion

Soit  $l$  une ligne de  $res_2$ .

Il existe  $l'$  dans  $\sigma_p(r)$  telle que  $l = c^{-1}(l')_\alpha$ .

$l'$  appartient à  $r$  et vérifie  $p$ .

Pour les mêmes raisons que précédemment,  $l$  et  $l'$  coïncident sur le domaine de  $p$  et donc  $l$  vérifie la propriété  $p$ .

Or, puisque  $l'$  appartient à  $r$ ,  $l$  appartient à  $\text{decrypt}_{\alpha, c}(r)$ , donc  $l$  appartient à  $\sigma_p(\text{decrypt}_{\alpha, c}(r)) = res_1$ .

## Sélection et déchiffrement d'un attribut sélectif

$$\sigma_p \circ \text{decrypt}_{\alpha, c} = \text{decrypt}_{\alpha, c} \circ \sigma_{c \Rightarrow p} \quad \text{si } p \text{ est compatible avec } c \quad (13)$$

On dit d'un prédicat  $p$  est compatible avec un chiffrement  $c$  pour l'attribut  $\alpha$  s'il existe un autre prédicat  $c_\alpha \Rightarrow p$  ne dépendant que de  $p$ ,  $c$  et du nom  $\alpha$  tel que

$$\forall l \in L, p(l) = (c_\alpha \Rightarrow p)(c(l)_\alpha)$$

Soit  $p$  un prédicat, soit  $\alpha$  un nom d'attribut, soit  $c$  un chiffrement compatible avec  $p$  pour  $\alpha$ ,  $r$  une relation et  $\delta_1$  son schéma relationnel.