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 $f_1(r) = f_2(r)$.

Lois de projection

Projection et projection

$$\pi_{\delta_1} \circ \cdots \circ \pi_{\delta_n} = \pi_{\delta_1 \cap \cdots \cap \delta_n} \tag{1}$$

Soit r une relation. On pose $r_1 = \pi_{\delta_1} \circ \cdots \circ \pi_{\delta_n}(r)$ et $r_2 = \pi_{\delta_1 \cap \cdots \cap \delta_n}(r)$

Schéma relationnel

On peut démontrer par récurrence sur n que le schéma relationnel de r_1 est

$$\mathrm{sch}(r_1) = \mathrm{sch}(r) \cap \bigcap_{i \in \{1,\ldots,n\}} \delta_i$$

De même, par définition de la projection, on a

$$\mathrm{sch}(r_2) = \mathrm{sch}(r) \cap \bigcap_{i \in \{1,\ldots,n\}} \delta_i$$

Donc $\mathrm{sch}(r_1) = \mathrm{sch}(r_2)$

Première inclusion

Soit l une ligne de r_1.

Il existe l' une ligne de r telle que $l = \big((l'|_{\delta_n \cup \{id\}})|_{\ldots}\big)|_{\delta_1 \cup \{id\}} = l'|_{(\delta_1 \cap \cdots \cap \delta_n) \cup \{id\}}$. Or, par définition de la projection $\pi_{\delta_1 \cap \cdots \cap \delta_n}$, on a $l'|_{(\delta_1 \cap \cdots \cap \delta_n) \cup \{id\}} \in r_2$. Donc $l \in r_2$.

Ainsi, $r_1 \subset r_2$.

Deuxième inclusion

De même, si l est un élément de r_2, alors il existe une ligne l' de r telle que $l = l'|_{(\delta_1 \cap \cdots \cap \delta_n) \cup \{id\}} = \big((l'|_{\delta_n \cup \{id\}})|_{\ldots}\big)|_{\delta_1 \cup \{id\}}$ et, par définition de $\pi_{\delta_1} \circ \cdots \circ \pi_{\delta_n}$, on a $\big((l'|_{\delta_n \cup \{id\}})|_{\ldots}\big)|_{\delta_1 \cup \{id\}} \in r_1$, d'où $l \in r_1$ et $r_2 \subset r_1$.

Projection et sélection

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

Soit δ un ensemble de noms d'attributs et p un prédicat sur les lignes tel que $\mathrm{dom}(p) \subset \delta$.
Soit r une relation. On pose $r_1 = (\pi_\delta \circ \sigma_p)(r)$ et $r_2 = (\sigma_p \circ \pi_\delta)(r)$

Schéma relationnel

Une sélection ne modifiant jamais le schéma relationnel d'une relation, la schéma relation de r_1 et de r_2 est $\mathrm{sch}(r) \cap \delta$.

Première inclusion

Soit l une ligne de r_1.
Il existe une ligne l' de $\sigma_p(r_1)$ telle que $l = l'|_{(\mathrm{sch}(r) \cap \delta) \cup \{id\}}$.
Puisque l et l' coïncident sur δ et que $\mathrm{dom}(p) \subset \delta$, on a $p(l) = p(l') = true$.
Or, par définition de π_δ, $l' \in \pi_\delta(r)$, donc $l' \in \sigma_p(\pi_\delta(r)) = r_2$.
Ainsi, $r_1 \subset r_2$.

Deuxième inclusion

De même, si l est un élément de r_2,alors $p(l) = true$ et $l \in \pi_\delta(r)$ donc il existe une ligne l' dans r telle que $l = l'|_{(\mathrm{sch}(r) \cap \delta) \cup \{id\}}$. l et l' coïncidant sur δ qui contient le domaine de p, l' vérifie le prédicat p donc $l' \in \sigma_p(r)$.
On en déduit par définition de π_δ que $l \in r_1$.
Ainsi, $r_2 \subset r_1$.

Projection et défragmentation (verticale)

En appelant δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument, on a :

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

Soit δ un ensemble de noms d'attributs. Soient r_1 et r_2 deux relations unifiables.
On pose $res_1 = (\pi_\delta \circ \mathrm{defrag})(r_1, r_2)$ et $res_2 = \mathrm{defrag} \circ (\pi_\delta, \pi_\delta)(r_1, r_2)$.

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 $\mathrm{defrag}(r_1, r_2)$ 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 defrag(r_1, r_2) est $\delta_1 \cup \delta_2$, donc celui de 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 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 res_1.

Il existe l_0 une ligne de 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 res_2.

Or,

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

Donc : $l \in res_2$.

Deuxième inclusion

Soit l une ligne de 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 $_2$ 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 defrag(r_1, r_2) donc $l = (l_1.l_2)|_{\delta \cup \{id\}}$ appartient à res_1

Projection et déchiffrement d'un attribut projeté ou non

$$\pi_\delta \circ \text{decrypt}_{\alpha,\mathsf{c}} \equiv \text{decrypt}_{\alpha,\mathsf{c}} \circ \pi_\delta \tag{4}$$

Soit δ un ensemble de noms d'attributs et α un attribut (appartenant à δ ou pas). Soit r une relation. On pose $r_1 = (\pi_\delta \circ \text{decrypt}_{\alpha,\mathsf{c}})(r)$ et $r_2 = (\text{decrypt}_{\alpha,\mathsf{c}} \circ \pi_\delta)(r)$.

Schémas relationnels

Le déchiffrement ne changeant pas le schéma relationnel d'une relation,le schéma relationnel de r_1 et r_2 est sch$(r) \cap \delta$.

Première inclusion

Soit l une ligne de r_1.

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

Puisque l_0 appartient à r, $l_0|_{\delta\cup\{id\}}$ appartient à $\pi_\delta(r)$ et donc $\mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$ appartient à r_2.

Montrons que $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}} = \mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$. 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 :

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

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

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

Ainsi, $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}} = \mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$ donc l appartient à r_2.

Deuxième inclusion

Soit l une ligne de r_2.

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

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

Vu que l_0 appartient à r, $\mathtt{c}^{-1}(l_0)_\alpha$ appartient à $\text{decrypt}_{\alpha,\mathtt{c}}(r)$ et $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}}$ appartient à r_1.

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

On en déduit que l appartient à r_1.

Projection et déchiffrement d'un attribut non projeté

$$\pi_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}} \equiv \pi_\delta \qquad\qquad \text{si } \alpha \notin \delta \tag{5}$$

Soit δ un ensemble de noms d'attributs et α un attribut n'appartenant pas à δ. Soit r une relation. On pose $r_1 = (\pi_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}})(r)$ et $r_2 = (\text{decrypt}_{\alpha,\mathtt{c}} \circ \pi_\delta)(r)$.

Schémas relationnels

Le déchiffrement ne changeant pas le schéma relationnel d'une relation,le schéma relationnel de r_1 et r_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 $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}} = \mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$.

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

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

d'où l'égalité voulue.

À partir de là, si l est une ligne de r_1, elle s'écrit $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}}$ avec $l_0 \in r$ et $\mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$ appartient à r_2 donc l appartient à r_2.

Inversement, si l est une ligne de r_2, elle s'écrit $\mathtt{c}^{-1}(l_0|_{\delta\cup\{id\}})_\alpha$ avec $l_0 \in r$ et $\mathtt{c}^{-1}(l_0)_\alpha|_{\delta\cup\{id\}}$ appartient à r_1 donc l appartient à r_1.