Démonstrations des lois algébriques utilisées en C2QL

Santiago Bautista

Juin 2017

Pour tout chiffrement `c`, on appellera `c'` le chiffrement qui agit sur une liste en appliquant `c` à chacun des éléments de la liste. Lorsqu'une défragmentation est effectuée, on supposera que le schéma relationnel du fragment de gauche s'appelle δ' .

Lois de projection

Projection et projection

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

Projection et sélection

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

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 :

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

Projection et déchiffrement d'un attribut projeté ou non

$$\pi_\delta \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \pi_\delta \tag{4}$$

Projection et déchiffrement d'un attribut non projeté

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

Projection et jointure

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

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

Projection et agrégation

$$\mathrm{group}_\delta \circ \pi_{\delta'} \equiv \pi_{\delta'} \circ \mathrm{group}_\delta \qquad \text{si } \delta \subset \delta' \tag{7}$$

Projection et réduction d'un attribut projeté ou non

$$\mathrm{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \circ \mathrm{fold}_{\alpha,f,z} \tag{8}$$

Projection et réduction d'un attribut non projeté

$$\mathrm{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \qquad \text{si } \alpha \notin \delta \cup \{id\} \tag{9}$$

Lois de sélection

Sélection et sélection

$$\sigma_{p_1} \circ \cdots \circ \sigma_{p_n} \equiv \sigma_{p_1 \wedge \cdots \wedge p_n} \tag{10}$$

Sélection et défragmentation

En appelant δ_1 le schéma relationnel du premier argument, et δ_2 le schéma relationnel du deuxième arguemnt,

$$\sigma_p \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\sigma_p, \mathrm{id}) \qquad \text{si } dom(p) \subset \delta_1 \tag{11}$$
$$\sigma_p \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{id}, \sigma_p) \qquad \text{si } dom(p) \subset \delta_2 \tag{12}$$

Sélection et déchiffrement non sélectif

$$\sigma_p \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} = \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \sigma_p \qquad \text{si } \alpha \notin \mathrm{dom}(p) \tag{13}$$

Sélection et déchiffrement d'un attribut sélectif

$$\sigma_p \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} = \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \sigma_{\mathtt{c} \Rightarrow p} \qquad \text{si } p \text{ est compatible avec } \mathtt{c} \tag{14}$$

Sélection et jointure

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\sigma_p \circ \bowtie = \bowtie \circ (\sigma_p, \mathrm{id}) \qquad \text{si } \mathrm{dom}(p) \subset \delta_1 \tag{15}$$
$$\sigma_p \circ \bowtie = \bowtie \circ (\mathrm{id}, \sigma_p) \qquad \text{si } \mathrm{dom}(p) \subset \delta_2 \tag{16}$$

Sélection et agrégation

$$\text{group}_\delta \circ \sigma_p \equiv \sigma_p \circ \text{group}_\delta \qquad \text{si } \text{dom}(p) \subset \delta \tag{17}$$

Sélection et réduction

$$\sigma_p \circ \text{fold}_{\alpha,f,z} = \text{fold}_{\alpha,f,z} \circ \sigma_p \qquad \text{si } \alpha \notin \text{dom}(p) \tag{18}$$

Lois de fragmentation

Fragmentation et défragmentation

$$\text{defrag} \circ \text{frag}_\delta = \text{id} \tag{19}$$

Fragmentation et chiffrement

$$\text{frag}_\delta \circ \text{crypt}_{\alpha,\mathsf{c}} \equiv (\text{crypt}_{\alpha,\mathsf{c}}, \text{id}) \circ \text{frag}_\delta \qquad \text{si } \alpha \in \delta \tag{20}$$
$$\text{frag}_\delta \circ \text{crypt}_{\alpha,\mathsf{c}} \equiv (\text{id}, \text{crypt}_{\alpha,\mathsf{c}}) \circ \text{frag}_\delta \qquad \text{si } \alpha \notin \delta \tag{21}$$

Fragmentation et déchiffrement

$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,\mathsf{c}} \equiv (\text{decrypt}_{\alpha,\mathsf{c}}, \text{id}) \circ \text{frag}_\delta \qquad \text{si } \alpha \in \delta \tag{22}$$
$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,\mathsf{c}} \equiv (\text{id}, \text{decrypt}_{\alpha,\mathsf{c}}) \circ \text{frag}_\delta \qquad \text{si } \alpha \notin \delta \tag{23}$$

Lois de défragmentation

Défragmentation et chiffrement

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{defrag} \circ (\text{crypt}_{\alpha,\mathsf{c}}, \text{id}) \equiv \text{crypt}_{\alpha,\mathsf{c}} \circ \text{defrag} \qquad \text{si } \alpha \in \delta_1 \tag{24}$$
$$\text{defrag} \circ (\text{id}, \text{crypt}_{\alpha,\mathsf{c}}) \equiv \text{crypt}_{\alpha,\mathsf{c}} \circ \text{defrag} \qquad \text{si } \alpha \in \delta_2 \tag{25}$$

Défragmentation et déchiffrement

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{decrypt}_{\alpha,\mathsf{c}} \circ \text{defrag} \equiv \text{defrag} \circ (\text{decrypt}_{\alpha,\mathsf{c}}, \text{id}) \qquad \text{si } \alpha \in \delta_1 \tag{26}$$
$$\text{decrypt}_{\alpha,\mathsf{c}} \circ \text{defrag} \equiv \text{defrag} \circ (\text{id}, \text{decrypt}_{\alpha,\mathsf{c}}) \qquad \text{si } \alpha \in \delta_2 \tag{27}$$

Défragmentation et jointure

On appelle, $\delta_1, \delta_2, \delta_3, \ldots$ les schémas relationnels respectifs du premier, deuxième et troisième argument.

$$\bowtie \circ(\text{defrag}, \text{id}) \equiv \text{defrag} \circ(\text{id}, \bowtie) \qquad \text{si } \delta_1 \cap (\delta_2 \cup \delta_3) = \emptyset \tag{28}$$
$$\bowtie \circ(\text{id}, \text{defrag}) \equiv \text{defrag} \circ(\bowtie, \text{id}) \qquad \text{si } \delta_3 \cap (\delta_1 \cup \delta_2) = \emptyset \tag{29}$$

Défragmentation et agrégation

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{group}_\delta \circ \text{defrag} \equiv \text{defrag} \circ(\text{send} \circ \text{group}_\delta, \text{receiveAndGroup}) \qquad \text{Si } \delta \subset \delta_1 \tag{30}$$
$$\text{group}_\delta \circ \text{defrag} \equiv \text{defrag} \circ(\text{receiveAndGroup}, \text{send} \circ \text{group}_\delta) \qquad \text{Si } \delta \subset \delta_2 \tag{31}$$

Défragmentation et réduction

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{fold}_{\alpha,f,z} \circ \text{defrag} = \text{defrag} \circ(\text{fold}_{\alpha,f,z}, \text{id}) \qquad \text{si } \alpha \in \delta_1 \tag{32}$$
$$\text{fold}_{\alpha,f,z} \circ \text{defrag} = \text{defrag} \circ(\text{id}, \text{fold}_{\alpha,f,z}) \qquad \text{si } \alpha \in \delta_2 \tag{33}$$

Lois de chiffrement

Chiffrement et chiffrement

$$\text{crypt}_{\alpha,\texttt{c}} \circ \text{crypt}_{\beta,\texttt{s}} \equiv \text{crypt}_{\beta,\texttt{s}} \circ \text{crypt}_{\alpha,\texttt{c}} \qquad \text{si } \alpha \neq \beta \tag{34}$$

Chiffrement et déchiffrement

$$\text{id} \equiv \text{decrypt}_{\alpha,\texttt{c}} \circ \text{crypt}_{\alpha,\texttt{c}} \tag{35}$$

Lois de déchiffrement

Déchiffrement et déchiffrement

$$\text{decrypt}_{\alpha,\texttt{c}} \circ \text{decrypt}_{\beta,\texttt{s}} \equiv \text{decrypt}_{\beta,\texttt{s}} \circ \text{decrypt}_{\alpha,\texttt{c}} \qquad \text{si } \alpha \neq \beta \tag{36}$$

Déchiffrement et jointure

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

En appelant (P) la propriété « Soit `c` est injectif, soit $\alpha \notin \delta_1 \cap \delta_2$ »,

$$\text{decrypt}_{\alpha,\texttt{c}} \circ \bowtie \equiv \bowtie \circ(\text{decrypt}_{\alpha,\texttt{c}}, \text{id}) \qquad \text{si } \alpha \in \delta_1 \text{ et } (P) \tag{37}$$
$$\text{decrypt}_{\alpha,\texttt{c}} \circ \bowtie \equiv \bowtie \circ(\text{id}, \text{decrypt}_{\alpha,\texttt{c}}) \qquad \text{si } \alpha \in \delta_2 \text{ et } (P) \tag{38}$$

Déchiffrement et agrégation

$$\text{group}_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}} \equiv \text{decrypt}_{\alpha,\mathtt{c}'} \circ \text{group}_\delta \qquad \text{Si } \alpha \notin \delta \tag{39}$$
$$\text{group}_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}} \equiv \text{decrypt}_{\alpha,\mathtt{c}} \circ \text{group}_\delta \qquad \text{Si } \alpha \in \delta \text{ et } \mathtt{c} \text{ est compatible avec l'égalité} \tag{40}$$

Déchiffrement et réduction

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{fold}_{\alpha,f,z} \circ \text{decrypt}_{\beta,\mathtt{c}} = \text{decrypt}_{\beta,\mathtt{c}} \circ \text{fold}_{\alpha,f,z} \qquad \text{si } \alpha \neq \beta \tag{41}$$
$$\text{fold}_{\alpha,f,z} \circ \text{decrypt}_{\alpha,\mathtt{c}} = \text{decrypt}_{\alpha,\mathtt{c}} \circ \text{fold}_{\alpha,\mathtt{c}\Rightarrow f,\mathtt{c}\Rightarrow z} \qquad \text{si } \mathtt{c} \text{ est compatible avec } f \tag{42}$$

Lois de jointure

Jointure et jointure

$$\bowtie \circ(\bowtie, \text{id}) \equiv \bowtie \circ(\text{id}, \bowtie) \tag{43}$$

Jointure et agrégation

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{group}_\delta \circ \bowtie \equiv \bowtie \circ(\text{group}_\delta, \text{group}_\delta) \qquad \text{si } \delta = \delta_1 \cap \delta_2 \tag{44}$$

Jointure et réduction

Soit δ_1 le schéma relationnel du premier argument et δ_2 le schéma relationnel du deuxième argument.

$$\text{fold}_{\alpha,f,z} \circ \bowtie = \bowtie \circ(\text{fold}_{\alpha,f,z}, \text{id}) \qquad \text{si } \alpha \in \delta_1 \setminus \delta_2 \tag{45}$$
$$\text{fold}_{\alpha,f,z} \circ \bowtie = \bowtie \circ(\text{id}, \text{fold}_{\alpha,f,z}) \qquad \text{si } \alpha \in \delta_2 \setminus \delta_1 \tag{46}$$
$$\text{fold}_{\alpha,f,z} \circ \bowtie = \bowtie \circ(\text{fold}_{\alpha,f,z}, \text{fold}_{\alpha,f,z}) \qquad \text{si red}_{\alpha,f,z,\bullet} \text{ est injective} \tag{47}$$

Lois d'agrégation

Agrégation et agrégation

$$\textit{group} \text{ ne commute pas avec lui-même} \tag{48}$$

Agrégation et réduction

$$\text{fold}_{\alpha,f,z} \circ \text{group}_\delta = \text{group}_\delta \circ \text{fold}_{\alpha,f,z} \qquad \text{si red}_{\alpha,f,z,\bullet} \text{ est injective et } \alpha \in \delta \tag{49}$$

Lois de réduction

Réduction et réduction

$$\mathrm{fold}_{\alpha,f,z} \circ \mathrm{fold}_{\beta,g,z'} = \mathrm{fold}_{\beta,g,z'} \circ \mathrm{fold}_{\alpha,f,z} \qquad \text{si } \alpha \neq \beta \tag{50}$$