

Ensemble des lois algébriques pour le langage 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

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

Projection et sélection

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

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 :

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

Projection et déchiffrement d'un attribut projeté ou non

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

Projection et déchiffrement d'un attribut non projeté

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

Projection et jointure

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

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

Projection et agrégation

$$\text{group}_\delta \circ \pi_{\delta'} \equiv \pi_{\delta'} \circ \text{group}_\delta \quad \text{si } \delta \subset \delta' \quad (7)$$

Projection et réduction d'un attribut projeté ou non

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

Projection et réduction d'un attribut non projeté

$$\text{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \quad \text{si } \alpha \notin \delta \cup \{id\} \quad (9)$$

Lois de sélection

Sélection et sélection

$$\sigma_{p_1} \circ \dots \circ \sigma_{p_n} \equiv \sigma_{p_1 \wedge \dots \wedge p_n} \quad (10)$$

Sélection et défragmentation

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

$$\sigma_p \circ \text{defrag} \equiv \text{defrag} \circ (\sigma_p, id) \quad \text{si } \text{dom}(p) \subset \delta_1 \quad (11)$$

$$\sigma_p \circ \text{defrag} \equiv \text{defrag} \circ (id, \sigma_p) \quad \text{si } \text{dom}(p) \subset \delta_2 \quad (12)$$

Sélection et déchiffrement non sélectif

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

Sélection et déchiffrement d'un attribut sélectif

$$\sigma_p \circ \text{decrypt}_{\alpha,c} = \text{decrypt}_{\alpha,c} \circ \sigma_{c \Rightarrow p} \quad \text{si } p \text{ est compatible avec } c \quad (14)$$

Sélection et jointure

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

$$\sigma_p \circ \bowtie = \bowtie \circ (\sigma_p, id) \quad \text{si } \text{dom}(p) \subset \delta_1 \quad (15)$$

$$\sigma_p \circ \bowtie = \bowtie \circ (id, \sigma_p) \quad \text{si } \text{dom}(p) \subset \delta_2 \quad (16)$$

Sélection et agrégation

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

Sélection et réduction

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

Lois de fragmentation

Fragmentation et défragmentation

$$\text{defrag} \circ \text{frag}_\delta = \text{id} \quad (19)$$

Fragmentation et chiffrement

$$\text{frag}_\delta \circ \text{crypt}_{\alpha,c} \equiv (\text{crypt}_{\alpha,c}, \text{id}) \circ \text{frag}_\delta \quad \text{si } \alpha \in \delta \quad (20)$$

$$\text{frag}_\delta \circ \text{crypt}_{\alpha,c} \equiv (\text{id}, \text{crypt}_{\alpha,c}) \circ \text{frag}_\delta \quad \text{si } \alpha \notin \delta \quad (21)$$

Fragmentation et déchiffrement

$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,c} \equiv (\text{decrypt}_{\alpha,c}, \text{id}) \circ \text{frag}_\delta \quad \text{si } \alpha \in \delta \quad (22)$$

$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,c} \equiv (\text{id}, \text{decrypt}_{\alpha,c}) \circ \text{frag}_\delta \quad \text{si } \alpha \notin \delta \quad (23)$$

Lois de défragmentation

Défragmentation et chiffrement

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

$$\text{defrag} \circ (\text{crypt}_{\alpha,c}, \text{id}) \equiv \text{crypt}_{\alpha,c} \circ \text{defrag} \quad \text{si } \alpha \in \delta_1 \quad (24)$$

$$\text{defrag} \circ (\text{id}, \text{crypt}_{\alpha,c}) \equiv \text{crypt}_{\alpha,c} \circ \text{defrag} \quad \text{si } \alpha \in \delta_2 \quad (25)$$

Défragmentation et déchiffrement

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

$$\text{decrypt}_{\alpha,c} \circ \text{defrag} \equiv \text{defrag} \circ (\text{decrypt}_{\alpha,c}, \text{id}) \quad \text{si } \alpha \in \delta_1 \quad (26)$$

$$\text{decrypt}_{\alpha,c} \circ \text{defrag} \equiv \text{defrag} \circ (\text{id}, \text{decrypt}_{\alpha,c}) \quad \text{si } \alpha \in \delta_2 \quad (27)$$

Défragmentation et jointure

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

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

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

Défragmentation et agrégation

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

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

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

Défragmentation et réduction

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

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

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

Lois de chiffrement

Chiffrement et chiffrement

$$\text{crypt}_{\alpha, c} \circ \text{crypt}_{\beta, s} \equiv \text{crypt}_{\beta, s} \circ \text{crypt}_{\alpha, c} \quad \text{si } \alpha \neq \beta \quad (34)$$

Chiffrement et déchiffrement

$$\text{id} \equiv \text{decrypt}_{\alpha, c} \circ \text{crypt}_{\alpha, c} \quad (35)$$

Lois de déchiffrement

Déchiffrement et déchiffrement

$$\text{decrypt}_{\alpha, c} \circ \text{decrypt}_{\beta, s} \equiv \text{decrypt}_{\beta, s} \circ \text{decrypt}_{\alpha, c} \quad \text{si } \alpha \neq \beta \quad (36)$$

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 $\alpha \notin \delta_1 \cap \delta_2$ »,

$$\text{decrypt}_{\alpha, c} \circ \bowtie \equiv \bowtie \circ (\text{decrypt}_{\alpha, c}, \text{id}) \quad \text{si } \alpha \in \delta_1 \text{ et } (P) \quad (37)$$

$$\text{decrypt}_{\alpha, c} \circ \bowtie \equiv \bowtie \circ (\text{id}, \text{decrypt}_{\alpha, c}) \quad \text{si } \alpha \in \delta_2 \text{ et } (P) \quad (38)$$

Déchiffrement et agrégation

$$\text{group}_\delta \circ \text{decrypt}_{\alpha, \mathbf{c}} \equiv \text{decrypt}_{\alpha, \mathbf{c}} \circ \text{group}_\delta \quad \text{Si } \alpha \notin \delta \quad (39)$$

$$\text{group}_\delta \circ \text{decrypt}_{\alpha, \mathbf{c}} \equiv \text{decrypt}_{\alpha, \mathbf{c}} \circ \text{group}_\delta \quad \text{Si } \alpha \in \delta \text{ et } \mathbf{c} \text{ est compatible avec l'égalité} \quad (40)$$

Déchiffrement et réduction

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

$$\text{fold}_{\alpha, f, z} \circ \text{decrypt}_{\beta, \mathbf{c}} = \text{decrypt}_{\beta, \mathbf{c}} \circ \text{fold}_{\alpha, f, z} \quad \text{si } \alpha \neq \beta \quad (41)$$

$$\text{fold}_{\alpha, f, z} \circ \text{decrypt}_{\alpha, \mathbf{c}} = \text{decrypt}_{\alpha, \mathbf{c}} \circ \text{fold}_{\alpha, \mathbf{c} \Rightarrow f, \mathbf{c} \Rightarrow z} \quad \text{si } \mathbf{c} \text{ est compatible avec } f \quad (42)$$

Lois de jointure

Jointure et jointure

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

Jointure et agrégation

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

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

Jointure et réduction

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

$$\text{fold}_{\alpha, f, z} \circ \bowtie = \bowtie \circ (\text{fold}_{\alpha, f, z}, \text{id}) \quad \text{si } \alpha \in \delta_1 \setminus \delta_2 \quad (45)$$

$$\text{fold}_{\alpha, f, z} \circ \bowtie = \bowtie \circ (\text{id}, \text{fold}_{\alpha, f, z}) \quad \text{si } \alpha \in \delta_2 \setminus \delta_1 \quad (46)$$

$$\text{fold}_{\alpha, f, z} \circ \bowtie = \bowtie \circ (\text{fold}_{\alpha, f, z}, \text{fold}_{\alpha, f, z}) \quad \text{si } \text{red}_{\alpha, f, z, \bullet} \text{ est injective} \quad (47)$$

Lois d'agrégation

Agrégation et agrégation

$$\text{group} \text{ ne commute pas avec lui-même} \quad (48)$$

Agrégation et réduction

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

Lois de réduction

Réduction et réduction

$$\text{fold}_{\alpha,f,z} \circ \text{fold}_{\beta,g,z'} = \text{fold}_{\beta,g,z'} \circ \text{fold}_{\alpha,f,z} \quad \text{si } \alpha \neq \beta \quad (50)$$