Le but de ce document est de donner une définition formelle des fonctions dont est composé le langage C2QL.

Définitions générales

Soit $\mathcal{V}$ un ensemble, appelé ensemble des valeurs.

Définition 1 *Ici, pour simplifier, on appelle chaîne de caractères tout mot sur l'alphabet*

$$\Sigma = \{a, \ldots, z\} \cup \{A, \ldots, Z\} \cup \{0, \ldots, 9\}$$

Définition 2 *On appelle* nom d'attribut *toute chaîne de caractères.*

Définition 3 *On appelle* schéma relationnel *tout ensemble de noms d'attributs.*

Définition 4 *On appelle* relation *de schéma relationnel* Δ *un ensemble de fonctions de* $\Delta \cup \{id\}$ *dans* $\mathcal{V}$.

Chacune de ces fonctions (chacun des éléments de la relation) est appelé(e) ligne.

Pour chaque ligne l *de la relation et chaque* α *de* Δ, $l(\alpha)$ *est appelé* attribut *de* nom α *pour la ligne* l.

L'image de id est appelé identifiant de la ligne, *et il est, au sein de chaque relation, unique pour chaque ligne.*

Définition 5 *On appelle* S *l'ensemble des schémas relationnels possibles. Autrement dit, on pose* $\mathrm{S} = \mathcal{P}(\Sigma^*)$.

On appelle R *l'ensemble des relations possibles,*

et on introduit la fonction sch *de* R *dans* S *qui à une relation associe son schéma relationnel.*

Projections et sélections

Définition 6 *Pour tout ensemble* δ *de noms d'attributs, on appelle* projection sur les attributs δ *la fonction suivante :*

$$\begin{array}{rccc} \pi_\delta : & \mathrm{R} & \to & \mathrm{R} \\ & r & \mapsto & \{l|_{(\delta \cap \mathrm{sch}(r)) \cup \{id\}} / l \in r\} \end{array}$$

Définition 7 *On appelle* L *l'ensemble de toutes les lignes possibles.*

On appelle prédicat *toute fonction de* L *dans* $\{true, false\}$.

On appelle domaine *d'un prédicat* p *le plus petit ensemble* D *tel que :*

$$\forall (l, l') \in \mathrm{L}^2, (l|_D = l'|_D \Rightarrow p(l) = p(l'))$$

et on le note $\mathrm{dom}(p)$.

Définition 8 *On appelle* sélection de prédicat p, *pour tout prédicat* p, *la fonction :*

$$\begin{array}{rccc} \sigma_p : & \mathrm{R} & \to & \mathrm{R} \\ & r & \mapsto & r \cap p^{-1}(\{true\}) \end{array}$$

Jointure naturelle

Définition 9 *On dit que* deux relations r *et* r' *sont* joignables *si on a :*

$$\forall l \in r \quad \exists! l' \in r' \quad \forall \alpha \in \mathrm{sch}(r) \cap \mathrm{sch}(r'), \quad l(\alpha) = l'(\alpha)$$

Si r *et* r' *sont deux relations joignables et* l *est une ligne de* r*, on appelle* correspondant de l dans r' *la ligne* l' *de la propriété précédente (unique par définition). On note cette ligne* $\mathrm{cor}_{r,r'}(l)$.

On dit alors que l *et* l' *sont* deux lignes correspondantes.

Définition 10 *Si* l *et* l' *sont deux lignes correspondantes, on appelle* concaténation de l et de l'*, notée* $l.l'$ *la fonction de* $\mathrm{sch}(l) \cup \mathrm{sch}(l') \cup \{id\}$ *définie par :*

$$\begin{cases} l.l'(\alpha) = l(\alpha) & si\ \alpha \in \mathrm{sch}(r) \setminus \mathrm{sch}(r') \\ l.l'(\alpha) = l'(\alpha) & si\ \alpha \in \mathrm{sch}(r') \setminus \mathrm{sch}(r) \\ l.l'(\alpha) = l(\alpha) = l'(\alpha) & si\ \alpha \in \mathrm{sch}(r) \cap \mathrm{sch}(r') \\ l.l'(id) = l(id) \end{cases}$$

Définition 11 *Pour* r *et* r' *deux relations joignables, on appelle* jointure naturelle *de* r *et* r' *la table*

$$r \bowtie r' = \{l.\,\mathrm{cor}_{r,r'}(l) / l \in r\}$$

On utilisera aussi la notation préfixe. En effet, si on appelle Rj *l'ensemble des paires de relations unifiables, on vient de définir la fonction*

$$\begin{array}{rccc} \bowtie : & \mathrm{Rj} & \to & \mathrm{R} \\ & (r, r') & \mapsto & r \bowtie r' \end{array}$$

Fragmentation et défragmentation

La défragmentation est un cas particulier de jointure naturelle, le seul attribut en commun pour les deux tables est l'identifiant des lignes.

Définition 12 *Deux relations* r *et* r' *sont dites* unifiables *si :*

$$\begin{cases} \{l(id)/l \in r\} = \{l(id)/l \in r'\} \\ \mathrm{sch}(r) \cap \mathrm{sch}(r') = \emptyset \end{cases}$$

On remarquera que deux relations unifiables sont également joignables.

On note Ru *l'ensemble des paires de relations unifiables, qui est donc un sous-ensemble de* Rj*, qui lui même est un sous-ensemble de* R^2.

Définition 13 *Pour tout ensemble de noms d'attributs* δ *on appelle* fragmentation de fragment gauche δ *l'application suivante :*

$$\begin{array}{rccc} \mathrm{frag}_\delta & \mathrm{R} & \to & \mathrm{Ru} \\ & r & \mapsto & (\{l|_{(\mathrm{sch}(r)\cap\delta)\cup\{id\}} / l \in r\}, \{l_{(\mathrm{sch}(r)\setminus\delta)\cup\{id\}} / l \in r\}) \end{array}$$

Définition 14 *On appelle* défragmentation *la restriction de la jointure naturelle à* Ru.

$$\begin{array}{rccc} \mathrm{defrag} & \mathrm{Ru} & \to & \mathrm{R} \\ & (r, r') & \mapsto & r \bowtie r' \end{array}$$

Chiffrement et déchiffrement

Vu que pour l'instant on s'intéresse uniquement aux contenus des tables pour démontrer la correction sémantique des lois de composition, on ne parlera pas pour l'instant des éventuelles clefs de chiffrement et déchiffrement.

Définition 15 *On appelle* chiffrement *tout couple* $\mathtt{c}$ *de fonctions de* $\mathcal{V}$ *dans* $\mathcal{V}$ $(\mathrm{Enc}, \mathrm{Dec})$ *vérifiant* $\mathrm{Dec} \circ \mathrm{Enc} = \mathrm{id}$.

Pour toute valeur v *de* $\mathcal{V}$ *on note* $\mathtt{c}(v) = \mathrm{Enc}(v)$ *et* $\mathtt{c}^{-1}(v) = \mathrm{Dec}(v)$

Définition 16 *Pour une ligne* l *définie sur* Δ*, pour* α *un attribut, et pour* $\mathtt{c}$ *un chiffrement, on appelle* version de l chiffrée pour α avec le chiffrement $\mathtt{c}$ *la ligne notée* $\mathtt{c}(l)_\alpha$ *définie par :*

$$\begin{cases} \forall \beta \in \Delta \setminus \{\alpha\} & \mathtt{c}(l)_\alpha(\beta) = l(\beta) \\ & \mathtt{c}(l)_\alpha(\alpha) = \mathtt{c}(l(\alpha)) \quad \textit{si } \alpha \in \Delta \end{cases}$$

De même, on définit la version de l déchiffrée pour α avec le chiffrement $\mathtt{c}$*, notée* $\mathtt{c}^{-1}(l)_\alpha$*, par :*

$$\begin{cases} \forall \beta \in \Delta \setminus \{\alpha\} & \mathtt{c}^{-1}(l)_\alpha(\beta) = l(\beta) \\ & \mathtt{c}^{-1}(l)_\alpha(\alpha) = \mathtt{c}^{-1}(l(\alpha)) \quad \textit{si } \alpha \in \Delta \end{cases}$$

Définition 17 *Pour* α *un nom d'attribut et* $\mathtt{c}$ *un chiffrement, on appelle* fonction de chiffrement de α par $\mathtt{c}$ *la fonction*

$$\begin{array}{rccc} \mathrm{crypt}_{\alpha,\mathtt{c}} : & \mathrm{R} & \to & \mathrm{R} \\ & r & \mapsto & \{\mathtt{c}(l)_\alpha / l \in r\} \end{array}$$

De même, on appelle fonction de déchiffrement de α par $\mathtt{c}$ *la fonction*

$$\begin{array}{rccc} \mathrm{decrypt}_{\alpha,\mathtt{c}} : & \mathrm{R} & \to & \mathrm{R} \\ & r & \mapsto & \{\mathtt{c}^{-1}(l)_\alpha / l \in r\} \end{array}$$

Agrégation

Définition 18 *Pour* δ *un ensemble de noms d'attributs, et une relation* r*,* on note r_δ *la relation*

$$\{l|_\delta / l \in r\}$$

Notons que r_δ *étant un ensemble, il n'a pas de doublons.*