

Mathématiques pour l'informatique. L1 Informatique UE-12.

Contrôle Terminal - Session 2 (correction) - Juin 2025

Problème. Un système informatique gère un ensemble d'utilisateurs et leur accès aux ressources de ce système. Chaque utilisateur a un identifiant unique et dispose de certaines clefs qui lui permettent d'accéder à certaines ressources du système.

On introduit les prédicats suivants :

- $A(x)$: «l'utilisateur d'identifiant x est authentifié» ;
- $U(x, k)$: «l'utilisateur d'identifiant x dispose de la clef k » ;
- $V(k, r)$: «la clef k donne accès à la ressource r ».

On note X l'ensemble des identifiants, K l'ensemble des clefs et Y l'ensemble des ressources.

(1) Formalisez les propositions suivantes :

- (1) «l'utilisateur x est authentifié et a accès à la ressource r ».
- (2) «une seule clef permet d'accéder à la ressource r ».
- (3) «au moins deux utilisateurs disposent de la même clef».
- (4) «il n'existe aucune clef permettant d'accéder à la ressource r ».
- (5) «tout utilisateur authentifié peut accéder à une ressource au moins».

On pose $X := \{x_1, \dots, x_4\}$, $K := \{k_1, k_2, k_3\}$ et $Y := \{r_1, \dots, r_6\}$ et les interprétations suivantes des prédicats $U(x, k)$ et $V(k, r)$:

U	k_1	k_2	k_3
x_1	V	F	V
x_2	F	F	V
x_3	V	V	F
x_4	F	V	F

V	r_1	r_2	r_3	r_4	r_5	r_6
k_1	V	F	F	V	F	F
k_2	F	F	V	F	F	V
k_3	F	F	F	V	F	F

(2) Définissez le prédicat $C(x, r)$ sur $X \times Y$ «l'utilisateur x peut accéder à la ressource r » à l'aide des prédicats U et V .

(3) Soit $c := (X, G, Y)$ la correspondance dont le graphe G est défini par la relation binaire C . Exprimez formellement G .

(4) Soit $u = (X, G_u, K)$ et $v = (K, G_v, Y)$ les correspondances définies par les relations binaires U et V . Dessinez leur diagramme sagittal. Calculez $u^{-1}(\{k_2, k_3\})$ et $v(\{k_1, k_2\})$.

(5) Comment définir la correspondance c à partir des correspondances u et v ? Justifiez.

(6) La correspondance c est-elle fonctionnelle ? La restriction de c à $\{x_2\}$ est-elle fonctionnelle ? Le cas échéant, indiquez si c'est une application et dans ce cas, si elle est injective, surjective ? Justifiez.

(7) Quelles sont les propriétés satisfaites par la relation binaire définie sur X par $x \mathcal{R} y$ si et seulement si x et y ont accès à une même ressource $r \in Y$? Justifiez.

Réponse. (1) Explicitons la formalisation de la proposition «l'utilisateur x est authentifié et a accès à la ressource r ». Faut-il quantifier x et r dans ce contexte ? *Non*, car x et r ne sont pas ici des variables au sens logique, mais désignent respectivement un utilisateur particulier baptisé x et une ressource particulière baptisée r . Si l'on conserve la même lettre que dans les prédicats $A(x)$, $U(x, k)$ et $V(k, r)$, c'est précisément pour permettre l'association immédiate avec les définitions de ces prédicats.

À noter : le fait que l'on utilise des lettres comme x et r ne suffit pas à en faire des variables logiques. C'est l'usage dans le contexte (en particulier la présence ou non de quantificateurs) qui détermine si une lettre représente une variable libre, liée, ou une constante (instanciation).

Voici des expressions possibles :

- (1) $A(x) \wedge (\exists k \in K (U(x, k) \wedge V(k, r)))$
L'utilisateur est authentifié et il existe une clef qu'il possède et qui lui permet d'accéder à la ressource r .
- (2) $\exists! k \in K V(k, r)$
On rappelle que le quantificateur $\exists!$ signifie «il existe un unique» ; cela exprime que **une seule clef** donne accès à r .
- (3) $\exists (x_1, x_2) \in X^2 \exists k \in K ((x_1 \neq x_2) \wedge U(x_1, k) \wedge U(x_2, k))$
On demande qu'il existe **au moins deux utilisateurs distincts** partageant une même clef.
- (4) $\forall k \in K \neg V(k, r)$ logiquement équivalent à $\neg(\exists k \in K V(k, r))$.
Autrement dit, **aucune clef** ne donne accès à r .

- (5) $\forall x \in X (A(x) \Rightarrow (\exists k \in K \exists r \in Y (U(x, k) \wedge V(k, r))))$
 Tout utilisateur, s'il est authentifié, a accès à **au moins** une ressource, via **au moins** une clef.

(2) On souhaite définir le prédicat $C(x, r)$: «l'utilisateur x peut accéder à la ressource r ». On le définit naturellement comme :

$$C(x, r) := \exists k \in K (U(x, k) \wedge V(k, r))$$

(3) Le graphe G de la correspondance $c = (X, G, Y)$ est donné par :

$$G = \{(x, r) \in X \times Y \mid C(x, r)\}$$

On peut ici le calculer explicitement à partir des tables de vérité des prédicats :

- $x_1 \mapsto \{k_1, k_3\}$ or $k_1 \mapsto \{r_1, r_4\}$ et $k_3 \mapsto \{r_4\}$ donc

$$\{(x_1, r_1), (x_1, r_4)\} \subseteq G.$$

- $x_2 \mapsto \{k_3\}$ or $k_3 \mapsto \{r_4\}$ donc

$$\{(x_2, r_4)\} \subseteq G.$$

- $x_3 \mapsto \{k_1, k_2\}$ or $k_1 \mapsto \{r_1, r_4\}$ et $k_2 \mapsto \{r_3, r_6\}$ donc

$$\{(x_3, r_1), (x_3, r_3), (x_3, r_4), (x_3, r_6)\} \subseteq G.$$

- $x_4 \mapsto \{k_2\}$ or $k_2 \mapsto \{r_3, r_6\}$ donc

$$\{(x_4, r_3), (x_4, r_6)\} \subseteq G.$$

En collectant tous les couples, on obtient :

$$G = \{(x_1, r_1), (x_1, r_4), (x_2, r_4), (x_3, r_1), (x_3, r_3), (x_3, r_4), (x_3, r_6), (x_4, r_3), (x_4, r_6)\}$$

(4) On définit les deux correspondances u et v :

$$u := \{(x, k) \in X \times K \mid U(x, k)\} \quad \text{et} \quad v := \{(k, r) \in K \times Y \mid V(k, r)\}.$$

Leur diagramme sagittal est donné en figure 1. On a :

$$u^{-1}(\{k_2, k_3\}) = \{x_1, x_2, x_3, x_4\}$$

$$v(\{k_1, k_2\}) = \{r_1, r_3, r_4, r_6\}$$

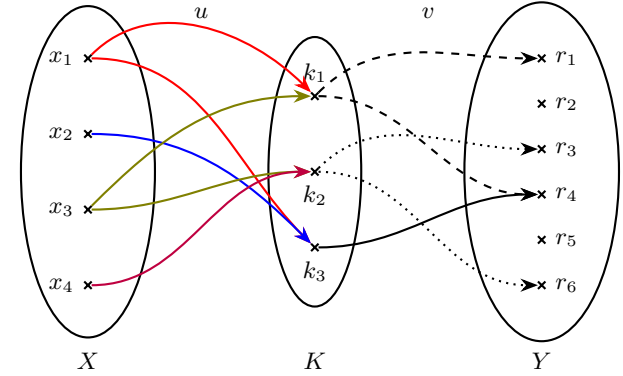


FIGURE 1. Diagrammes sagittaux des correspondances u et v .

(5) La correspondance c est la composée des correspondances u et v :

$$c = v \circ u$$

En effet, la correspondance u permet de déterminer l'ensemble des clefs $K_x := u(\{x\})$ disponibles pour un utilisateur x et la correspondance v l'ensemble des ressources $v(K_x)$ accessibles avec les clefs de K_x .

(6) D'après le graphe G , l'utilisateur x_1 a accès à 4 ressources, la correspondance c n'est donc pas fonctionnelle. Sa restriction $c|_{\{x_2\}}$ est une application puisque $c(\{x_2\}) = \{r_4\}$, elle est évidemment injective puisque l'ensemble de départ est réduit à un singleton, elle n'est pas surjective en revanche puisqu'aucune des ressources autres que r_4 ne sont accessibles.

(7) La relation se formalise ainsi :

$$x \mathcal{R} y \Leftrightarrow \exists r \in Y (C(x, r) \wedge C(y, r)). \quad (1)$$

Elle exprime que deux utilisateurs sont en relation s'ils peuvent accéder à une même ressource. Examinons ses propriétés. L'existence d'une ressource pour chaque individu est idempotence et la commutativité de la conjonction dans (1) entraînent immédiatement la réflexivité et la symétrie, seule la transitivité mérite un peu de réflexion.

- Elle est réflexive : Il suffit de remplacer y par x dans (1), d'appliquer l'idempotence de la conjonction et de s'assurer que tous les individus

ont accès à au moins une ressource, ce qui est le cas. Si un individu n'accédait à aucune ressource, la relation ne serait plus réflexive.

- Elle est symétrique : Par commutativité de la conjonction dans (1).
- Elle est transitive : La seule ressource partagée entre deux utilisateurs est la ressource r_4 pour x_1 et x_2 , il n'y a pas de troisième utilisateur qui permettrait d'invalider la propriété. En effet, on pourrait disposer de trois individus a , b et c tels que a et b partagent une même ressource r et b et c partagent une même ressource r' , sans pour autant que a et c partagent une même ressource (cf. figure 2).

Cette relation est donc une relation d'équivalence.

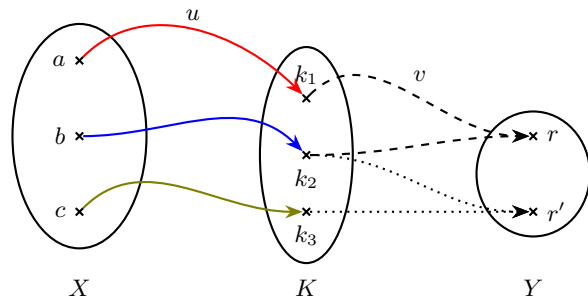


FIGURE 2. Illustration de la non-transitivité.