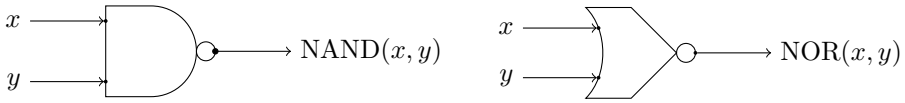
Exercice 3.1. Quelles sont les distributions de valeurs des variables $\{x_1, \ldots, x_n\}$ qui rendent les formules suivantes vraies :

1. $F = (x_1 \Rightarrow x_2) \wedge (x_2 \Rightarrow x_3) \wedge \cdots \wedge (x_{n-1} \Rightarrow x_n)$.
2. $G = F \wedge (x_n \Rightarrow x_1)$.
3. $H = \bigwedge_{\substack{1 \leq i,j \leq n \\ i \neq j}} (x_i \Rightarrow \neg x_j)$.

Exercice 3.2. Les fonctions NAND et NOR sont définies comme suit :

$$\text{NAND}(x, y) := \neg(x \wedge y), \quad \text{NOR}(x, y) = \neg(x \vee y).$$

1. Trouver une forme DNF pour NAND et une forme DNF pour NOR.
2. Trouver une forme CNF pour NAND et une forme CNF pour NOR.
3. Trouver une représentation polynomiale pour NAND et NOR.
4. Montrer que la fonction AND, OR et la négation peuvent s'obtenir comme combinaisons des fonctions NAND et NOR.
5. Les diagrammes logiques pour les fonctions NAND et NOR sont donnés ci-dessous :



   Dessiner les diagrammes des fonctions AND, OR et négation à l'aide de ces blocs.
6. Dessiner un diagramme logique de la fonction XOR en utilisant ces blocs.

Exercice 3.3. [Transformée de Moebius] Soit f une fonction de m variables. La forme polynomiale de f peut toujours s'écrire

$$f(X_1, \ldots, X_n) = \bigoplus_{u \in \{0,1\}^n} f_u X_1^{u_1} \cdots X_n^{u_n}$$

ou $f_u \in \{0, 1\}$ et par définition $X_i^1 = X_i$ et $X_i^0 = 1$. Pour $x = (x_1, \ldots, x_n)$ et $u = (u_1, \ldots, u_n)$ dans $\{0, 1\}^n$ on note $x \subseteq u$ ssi $x_i \Rightarrow u_i$ pour tout i. Le but de l'exercice est de montrer la relation suivante entre le vecteur des valeurs de f et sa représentation polynomiale :

$$f(x) = \bigoplus_{u \subseteq x} f_u \quad \text{et} \quad f_u = \bigoplus_{x \subseteq u} f(x)$$

1. Soient $u \in \{0, 1\}^n$ et la fonction monôme $m_u(X_1, \ldots, X_n) = X_1^{u_1} \cdots X_n^{u_n}$. Montrer que $m_u(x) = 1$ ssi $u \subseteq x$. En déduire la première partie du résultat.
2. On appelle transformée de Moebius l'application

$$\mathcal{M} : f = \bigoplus_{u \in \{0,1\}^n} f_u X^u \mapsto g = \bigoplus_{x \in \{0,1\}^n} f(x) X^x$$

   Montrer la seconde partie en montrant que la transformé de Moebius est involutive, c'est-à-dire en montrant que $\mathcal{M} \circ \mathcal{M}$ est l'identité.

Exercice 3.4. Trouver toutes les relations sur $\{a, b\} \times \{c, d\}$ qui ne sont pas des fonctions. Trouver toutes les relations sur $\{a, b\} \times \{c, d\}$ qui ne sont pas des applications.

Exercice 3.5. Soit X un ensemble non-vide et $R \subseteq (P(X) - \emptyset) \times (P(X) - \emptyset)$ la relation définie par $(A, B) \in R$ ssi $A \cap B \neq \emptyset$.

(a) R est-elle réflexive ? c'est-à-dire, $(A, A) \in R$ pour $A \in P(X) - \emptyset$?

(b) R est-elle symétrique ? c'est-à-dire, $(A, B) \in R$ implique $(B, A) \in R$?

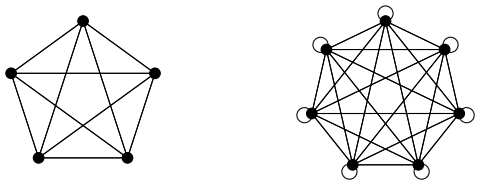
(c) R est-elle transitive ? c'est-à-dire, $(A, B), (B, C) \in R$ implique $(A, C) \in R$?

Exercice 3.6. Soit R une relation transitive sur $\mathbb{Z}$ pour laquelle on sait que $\forall a, b \in \mathbb{Z}$ si $|a-b| = 2$ alors $(a, b) \in R$. R est-elle nécessairement une relation d'équivalence ? Même question si $|a - b| \in \{3, 4\}$ implique $(a, b) \in R$.

Exercice 3.7. Pour une relation R sur l'ensemble X, on définit la relation R^n par récurrence sur n avec $R^1 = R$ et $R^{n+1} = R \circ R^n$. Répondre aux questions suivantes :

1. Montrer que si X est fini, il existe $s, r \in \mathbb{N}$ tels que $s < r$ et $R^s = R^r$.
2. Trouver une relation R sur un ensemble fini X tel que $R^{n+1} \neq R^n$ pour tout $n \in \mathbb{N}$.
3. Trouver une relation R sur un ensemble infini X tel que toutes les R^n pour $n \in \mathbb{N}$ sont distinctes.
4. Montrer qu'une relation R est transitive ssi $R^n \subseteq R$ pour tout $n \geq 1$.

Exercice 3.8. On dit qu'une arête d'un graphe qui relie un sommet à lui-même est une boucle. Une n-clique est un graphe avec n sommets tel que tous les couples de sommets soient connectés. Une n-clique à boucles est une n-clique dont chaque sommet possède une boucle. Par exemple, le dessin ci-dessous montre une 5-clique et une 7-clique à boucles.



Une clique est une n-clique pour un certain n. Soit R une relation d'équivalence sur un certain ensemble X. Montrer que le graphe de R est une union de cliques à boucles.

Exercices complémentaires

Exercice 3.9. Donner une CNF, une DNF et une forme polynomiale de $(x_1 \Leftrightarrow (x_2 \Leftrightarrow x_3))$.

Exercice 3.10. Dessiner un diagramme logique de la fonction $f(x, y) = (x \Rightarrow y)$ en utilisant les portes AND et XOR.

Exercice 3.11. Un coffre fort est muni de cinq serrures et ne peut être ouvert que lorsque les cinq serrures sont simultanément en position ouverte. Cinq personnes : Alice, Bernard, Christine, Dominique et Emile reçoivent chacun des clefs, correspondant à certaines de ces serrures. Donner une répartition possible des clefs telle que le coffre puisse être ouvert si et seulement si l'on se trouve dans l'une des situations suivantes :

- Présence de Alice et Bernard.
- Présence de Alice, Christine et Dominique.
- Présence de Bernard, Dominique et Emile.

Exercice 3.12. Soit K un corps et n un entier positif. On définit la relation C sur $K^{n\times n}$ de la manière suivante :

$$A \sim_C B \iff \exists T \in K^{n\times n} : TAT^{-1} = B.$$

Montrer que $\sim_C$ est une relation d'équivalence. Elle est appelée la relation de conjugaison. Si $A \sim_C B$, alors A et B sont des matrices conjuguées.

Exercice 3.13. Montrer que si R_1 et R_2 sont des relations d'équivalence sur un ensemble X, alors il en est de même pour $R_1 \cap R_2$. De plus, montrer que ce n'est en général pas le cas pour $R_1 \cup R_2$.

Correction.

Exercice 3.1. 1. La formule est vraie pour les distributions de valeurs suivantes

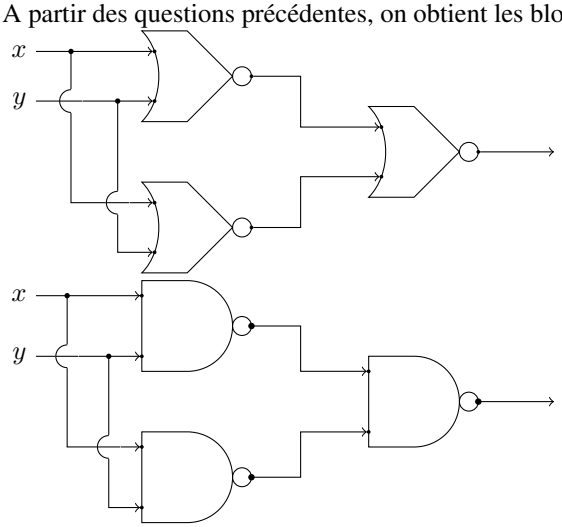
$$\begin{array}{l}(0,0,0,\ldots,0)\\ \ldots\\ (0,\ldots,0,1,\ldots,1)\\ \ldots\\ (1,\ldots,1)\end{array}.$$

En effet, dès lors que pour un certain rang i, x_i vaut 1, tous les x_j pour $j > i$ valent 1 aussi.

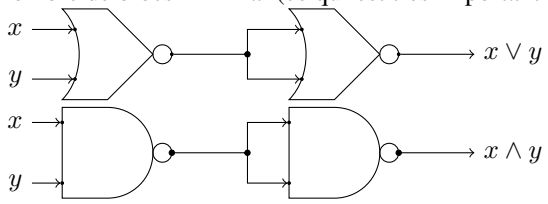
2. La formule est vraie pour $(0,\ldots,0)$ et $(1,\ldots,1)$ car dès lors que l'un des x_i vaut un, tous les autres valent un.
3. La formule est vraie pour les valeurs $(0,\ldots,0)$ et $(0,\ldots,0,1,0,\ldots,0)$. En effet, si pour un certain i, $x_i = 1$, alors pour tout $j \neq i$, $x_j = 0$.

Exercice 3.2. 1. $\text{NAND}(x,y) = (\neg x) \vee (\neg y)$, $\text{NOR}(x,y) = (\neg x \wedge \neg y)$ (c'est bien une disjonction de clauses conjonctives, même s'il n'y a qu'une seule clause conjonctive dans la disjonction).

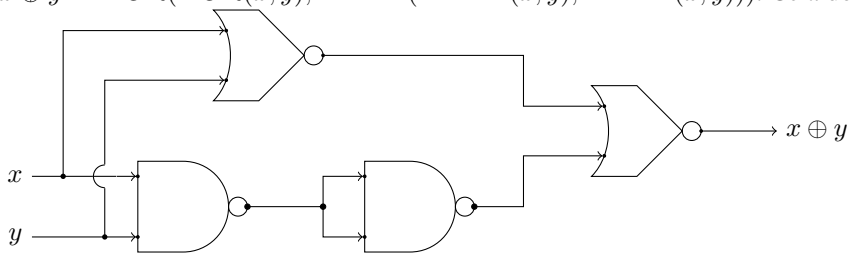
2. $\text{NAND}(x,y) = (\neg x \vee \neg y)$, $\text{NOR}(x,y) = \neg x \wedge \neg y$.
3. $\text{NAND} = 1 \oplus xy$. $\text{NOR}(x,y) = 1 \oplus x \oplus y \oplus xy$.
4. $\neg x = \text{NAND}(x,x) = \text{NOR}(x,x)$. $x \vee y = \text{NOR}(\text{NOR}(x,y), \text{NOR}(x,y))$, $x \wedge y = \text{NAND}(\text{NAND}(x,y), \text{NAND}(x,y))$.
5. A partir des questions précédentes, on obtient les blocs suivants.



Toutefois ces solutions ne sont pas optimales ! On peut faire mieux : les solutions suivantes présentent un nombre de blocs minimal (ce qui est très important lorsqu'on construit des circuits électriques réels).



6. $x \oplus y = NOR(NOR(x,y), NAND(NAND(x,y), NAND(x,y)))$. Cela donne le diagramme suivant.



Exercice 3.3. 1. Supposons que $u \subseteq x$. Alors pour tout i, soit $u_i = 0$ et alors $x_i^{u_i} = 1$ quelque soit la valeur de x_i, soit $u_i = 1$ et alors par hypothèse, comme $u_i \Rightarrow x_i$, $x_i = 1$, donc $x_i^{u_i} = 1$. Ainsi $m_u(x) = x_1^{u_1} \cdots x_n^{u_n} = 1$. Supposons que $u \not\subseteq x$, alors il existe un indice i tel que $u_i = 1$ et $x_i = 0$, mais alors $x_i^{u_i} = 0$ et $m_u(x) = 0$.
A présent, comme $f(x) = \bigoplus_{u\in\{0,1\}^n} f_u m_u(x)$, les seuls termes éventuellement non-nuls sont $f(x) = \bigoplus_{u\subseteq x} f_u$ lorsque le monôme s'évalue à 1.

2. Notons $g = \mathcal{M}(f)$. On a $g = \bigoplus_{x\in\{0,1\}^n} f(x)X^x$, soit encore d'après 1.

$$g = \bigoplus_{x\in\{0,1\}^n} \underbrace{\left[\bigoplus_{u\subseteq x} f_u\right]}_{=:g_x} X^x.$$

Notons encore $h = \mathcal{M}(g) = \bigoplus_{x\in\{0,1\}^n} g(x)X^x$ soit encore, toujours d'après la question 1.,

$$h = \bigoplus_{x\in\{0,1\}^n} \underbrace{\left[\bigoplus_{u\subseteq x} g_u\right]}_{=:h_x} X^x.$$

Il nous faut montrer que $h = f$, c'est-à-dire que $f_x = h_x$ pour tout $x \in \{0,1\}^n$. Or pour tout $x \in \{0,1\}^n$, on a

$$\begin{aligned} h_x &= \textstyle\bigoplus_{u\subseteq x} g_u \\ &= \textstyle\bigoplus_{u\subseteq x} \bigoplus_{v\subseteq u} f_v \\ &= \textstyle\bigoplus_{v\subseteq x} \bigoplus_{u \text{ tq. } v\subseteq u\subseteq x} f_v \\ &= \textstyle\bigoplus_{v\subseteq x} f_v \cdot \left(\bigoplus_{v\subseteq u\subseteq x} 1\right) \end{aligned}$$

Or la somme $\bigoplus_{v\subseteq u\subseteq x} 1$ vaut zéro, sauf si $v = x$. Dans ce cas, il n'y a qu'un terme, correspondant à $u = v = x$. Sinon, il y a deux cas possibles. Si $v \not\subseteq x$, l'ensemble à parcourir est vide. Si $v \subseteq x$ et $v \neq x$, soit $J \subset [1, n]$ l'ensemble des indices tels que $v_i \neq x_i$; u peut prendre exactement les valeurs $u_i = 0$ ou 1 si $i \in J$ et $u_i = x_i = v_i$ sinon ce qui fait $2^{|J|}$ possibilités. Donc $\bigoplus_{v\subseteq u\subseteq x} 1 = 2^{|J|} = 0 \mod 2$. Finalement on obtient $h_x = f_x$ comme attendu.

Exercice 3.4. Soit $A := \{a, b\}$ et $C := \{c, d\}$. Dans ce cas, une relation $R \subseteq A \times C$ n'est pas une fonction s'il existe $x \in A$ tel que $|\{y \in C \mid (x, y) \in R\}| > 1$. On trouve :

$$\begin{aligned} &\{(a,c),(a,d)\},\{(a,c),(a,d),(b,c)\},\{(a,c),(a,d),(b,d)\},\{(a,c),(b,c),(b,d)\},\\ &\quad\{(b,c),(b,d),(a,d)\},\{(a,c),(a,d),(b,c),(b,d)\},\{(b,c),(b,d)\}. \end{aligned}$$

Ainsi il y a 7 relations qui ne sont pas des fonctions.

Une relation R n'est pas une application si R n'est pas une fonction ou si la relation n'est pas totale, c'est-à-dire qu'il existe $x \in A$ tel que pour tout $y \in C$, $(x, y) \notin R$. Cela ajoute donc les cas suivants

$$\emptyset, \{(a, c)\}, \{(a, d)\}, \{(b, c)\}, \{(b, d)\}.$$

et porte à 11 le nombre de relations qui ne sont pas des applications.

Exercice 3.5. (a) La relation n'est pas réflexive si $A \in P(X)$. Par exemple, si $A = \emptyset$, alors $(\emptyset, \emptyset) \notin R$. Mais si $A \in P(X) - \emptyset$, alors $A \cap A = A \neq \emptyset$, si bien que $(A, A) \in R$.

(b) C'est clairement le cas puisque $A \cap B = B \cap A$, si bien que ces ensembles sont tous les deux vide ou non simultanément.

(c) La relation n'est pas transitive. Supposons que $B = A \sqcup C$, où $A, C \neq \emptyset$ et $A \cap C = \emptyset$. Alors $(A, B) \in R$ et $(B, C) \in R$ mais $(A, C) \notin R$.

Exercice 3.6. Dans les deux cas, R est transitive par définition et l'on peut montrer facilement en utilisant la transitivité que R est aussi réflexive. En effet, donnons-nous un entier a, alors $(a, a + 2) \in R$ et $(a + 2, a) \in R$, donc par transitivité, $(a, a) \in R$. Le problème est donc de montrer la symétrie.

Dans le premier cas, on peut observer que tous les nombres de même parité $(a, a+2n)$ avec $n \in \mathbb{Z}$ sont en relation. Toutefois, ces conditions ne suffisent pas à imposer la symétrie. On peut en effet imaginer la relation $R = \{(2n, 2n'), (2n+1, 2n'+1), (2n, 2n'+1); n, n' \in \mathbb{Z}\}$ qui n'est pas symétrique.

Dans le second cas, les entiers dont la différence est divisible par 3 ou par 4 sont dans R, mais alors comme 3 et 4 sont premiers entre eux, tout couple d'entiers appartient à R. Donc R est trivialement une relation d'équivalence.

Exercice 3.7.

1. L'ensemble X est fini, il en va de même de $P(X \times X)$. Comme $R^n \in P(X \times X)$ pour tout entier n, il s'ensuit que la suite $R, R^2, R^3, \ldots$ ne peut être formée d'ensembles tous distincts (lemme des tiroirs). Ainsi il existe deux indices r et s ($r < s$) tels que $R^r = R^s$.
2. Soit $R = \{(1,2),(2,1)\} \subset \{1,2\} \times \{1,2\}$. Alors, $R^2 = R \circ R = \{(1,1),(2,2)\}$ et $R^3 = R \circ R^2 = R$. Plus généralement, $R^n = R^2$ si n est pair et $R^n = R$ si n est impair.
3. Soit R la relation « successeur direct », c'est-à-dire, $R = \{(a, a+1) \mid a \in \mathbb{Z}\}$, alors, $R^n = \{(a, a+n) \mid a \in \mathbb{Z}\}$. Les relations $(R^n)_{n\in\mathbb{N}}$ sont donc toutes distinctes.
4. D'après la définition 3.3, on sait que R est transitive ssi $R^2 \subseteq R$. Supposons que R soit transitive. Raisonnons par récurrence et supposons avoir démontré que $R^n \subseteq R$ pour un certain $n \geq 2$. Il s'ensuit que $R^{n+1} = R \circ R^n \subseteq R \circ R \subseteq R$, ce qui prouve notre assertion. Réciproquement, supposons que pour tout entier $n \geq 2$, $R^n \subseteq R$, alors pour $n = 2$ en particulier, nous avons $R^2 \subseteq R$ ce qui est la définition de la transitivité.

Exercice 3.8. Notons X_1, X_2, …, X_t les classes d'équivalence de X. On sait qu'elles forment une partition de X, c'est-à-dire que X est l'union disjointe des $(X_i)_{1\leq i\leq t}$. Il suffit de montrer les deux points suivants : il n'existe pas d'arrête entre deux sommets appartenants à des X_i distincts d'une part et le graphe de R restreint à chaque X_i forme une clique à boucle d'autre part.

Supposons qu'il existe deux indices i et j et deux éléments $x_i \in X_i$ et $x_j \in X_j$ tels que $(x_i, x_j) \in R$, alors, $x_i \sim_R x_j$. Donc x_i et x_j appartiennent à la même classe d'équivalence et $i = j$. Nous venons de démontrer la contraposée du premier point.

Soit à présent deux éléments x et x' éventuellement égaux d'une même classe X_i. Par définition, $x \sim_R x'$, donc $(x, x') \in R$. Donc le graphe restreint à X_i est bien une clique à boucle.

Exercices complémentaires

Exercice 3.9. La formule $x_1 \Leftrightarrow (x_2 \Leftrightarrow x_3)$ est vraie pour $(1,1,1)$, $(1,0,0)$, $(0,1,0)$ et $(0,0,1)$ ce qui donne la DNF suivante

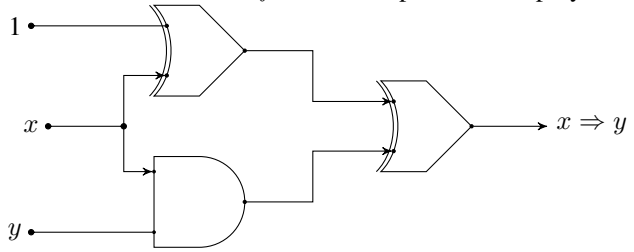
$$(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3).$$

La formule est fausse pour $(0,1,1)$, $(0,0,0)$, $(1,1,0)$ et $(1,0,1)$ ce qui donne la DNF suivante

$$(x_1 \vee \neg x_2 \vee \neg x_3) \wedge (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3).$$

La formule $a \Leftrightarrow b$ admet pour polynôme $a + b + 1$, donc $x_1 \Leftrightarrow (x_2 \Leftrightarrow x_3)$ admet $x_1 + x_2 + x_3$ comme polynôme.

Exercice 3.10. La fonction f admet la représentation polynomiale $1 \oplus x \oplus xy$ ce qui fournit le diagramme :



Exercice 3.11. Nous procédons par analyse–synthèse :

Analyse du problème. Supposons qu'il existe une solution. Introduisons une variable booléenne (a, b, etc.) pour chaque personnage. Cette variable vaut 1 si la personne est présente, 0 sinon. D'après l'énoncé, le coffre s'ouvre si et seulement si la formule

$$\phi = (a \wedge b) \vee (a \wedge c \wedge d) \wedge (b \wedge d \wedge e).$$

est satisfaite.

Notons aussi s_i pour $1 \leq i \leq 5$ la variable booléenne indiquant que la clef n$^{\text{o}}$ i est présente. Le coffre s'ouvre si et seulement si la formule

$$s_1 \wedge \cdots \wedge s_5$$

est satisfaite. Si la clef s_i a été donnée aux personnes $x_1, \ldots, x_k$ avec $x_j \in \{a, b, \ldots, e\}$, on a de plus la relation $s_i = x_1 \vee \cdots \vee x_k$.

Synthèse. La analyse conduit donc à la question suivante : peut-on décomposer ϕ en une conjonction de 5 clauses disjonctives dont les littéraux sont tous positifs ? Or on peut calculer que

$$\phi = \underbrace{(a \vee b)}_{s_1} \wedge \underbrace{(a \vee d)}_{s_2} \wedge \underbrace{(a \vee e)}_{s_3} \wedge \underbrace{(b \vee c)}_{s_4} \wedge \underbrace{(b \vee d)}_{s_5}.$$

Il s'agit d'une CNF de ϕ. Ainsi une solution consiste en la distribution suivante. Alice reçoit les clefs des serrures s_1, s_2 et s_3 ; B. reçoit s_1, s_4 et s_5 ; C. reçoit s_4 ; D. reçoit s_2 et s_5 ; E. reçoit s_3.

Exercice 3.12.

1. Réfléxivité : on a $A \sim_C A : A = IAI^{-1}$ où I est la matrice identité.
2. Symétrie : Supposons que $A \sim_C B$, disons $TAT^{-1} = B$. Alors $T^{-1}BT = A$, donc $B \sim_C A$.
3. Transitivité : Supposons que $A \sim_C B$, disons $TAT^{-1} = B$, et $B \sim_C D$, disons $LBL^{-1} = D$. Alors $LTAT^{-1}L^{-1} = (LT)A(LT)^{-1} = D$, donc $A \sim_C D$.

Exercice 3.13. On considère $x, y, z \in X$.

1. Réflexivité de $R_1 \cap R_2$. On a $(x, x) \in R_1$ et $(x, x) \in R_2$ puisque R_1 comme R_2 sont des relations d'équivalence. Donc $(x, x) \in R_1 \cap R_2$.
2. Symétrie : si $(x, y) \in R_1 \cap R_2$, alors $(x, y) \in R_i$ pour $i = 1, 2$, donc par symétrie de la relation R_i, on a aussi $(y, x) \in R_i$ pour $i = 1, 2$. Mézalor, $(y, x) \in R_1 \cap R_2$.
3. Transitivité : si (x, y), $(y, z) \in R_1 \cap R_2$, alors (x, y), $(y, z) \in R_i$ pour $i = 1, 2$. Comme R_i est transitif, $(x, z) \in R_i$ pour $i = 1, 2$. Donc $(x, z) \in R_1 \cap R_2$.

Posons $R_1 = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$ et $R_2 = \{(2, 2), (3, 3), (2, 3), (3, 2)\}$. Alors R_1 et R_2 sont des relations d'équivalence. On a $(1, 2), (2, 3) \in R_1 \cup R_2$, mais $(1, 3) \notin R_1 \cup R_2$.