

LIF11 - TD2

Correction

Exercice 1:

Pour chacune des fonctions f_1 et f_2 , donner une formule qui la réalise. On pourra éventuellement pour cela suivre la méthode suggérée à travers la démonstration du fait que $\{\top, \perp, \neg, \wedge, \Rightarrow, \vee\}$ est fonctionnellement complet.

x	y	z	$f_1(x, y, z)$	$f_2(x, y, z)$
1	1	1	1	0
1	1	0	1	0
1	0	1	0	0
1	0	0	1	1
0	1	1	0	0
0	1	0	0	1
0	0	1	1	0
0	0	0	0	0

Correction: On décompose f_1 en deux fonctions à 2 arguments $f_1^1(y, z) = f_1(V, y, z)$ et $f_1^2(y, z) = f_1(F, y, z)$. On recommence l'opération avec f_1^1 décomposée en f_1^{11} et f_1^{12} et f_1^1 décomposée en f_1^{21} et f_1^{22} . On en donne également une version simplifiée obtenue en utilisant à chaque étape des équivalences remarquables. On procède de la même manière pour f_2

Fonction	Formule	Formule simplifiée
f_1^{11}	$(p_z \Rightarrow \top) \wedge (\neg p_z \Rightarrow \top)$	\top
f_1^{12}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_1^{21}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \perp)$	\perp
f_1^{22}	$(p_z \Rightarrow \top) \wedge (\neg p_z \Rightarrow \perp)$	p_z
f_1^1	$(p_y \Rightarrow \top) \wedge (\neg p_y \Rightarrow \neg p_z)$	$p_z \Rightarrow p_y$
f_1^2	$(p_y \Rightarrow \perp) \wedge (\neg p_y \Rightarrow p_z)$	$\neg(p_z \Rightarrow p_y)$
f_1	$(p_x \Rightarrow (p_z \Rightarrow p_y)) \wedge (\neg p_x \Rightarrow \neg(p_z \Rightarrow p_y))$	$p_x \Leftrightarrow (p_z \Rightarrow p_y)$
f_2^{11}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \perp)$	\perp
f_2^{12}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_2^{21}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_2^{22}	$(p_z \Rightarrow \perp) \wedge (\neg p_z \Rightarrow \perp)$	\perp
f_2^1	$(p_y \Rightarrow \perp) \wedge (\neg p_y \Rightarrow \neg p_z)$	$\neg p_y \wedge \neg p_z$
f_2^2	$(p_y \Rightarrow \neg p_z) \wedge (\neg p_y \Rightarrow \perp)$	$p_y \wedge \neg p_z$
f_2	$(p_x \Rightarrow (\neg p_y \wedge \neg p_z)) \wedge (\neg p_x \Rightarrow (p_y \wedge \neg p_z))$	$\neg p_x \wedge \neg(p_x \Leftrightarrow p_y)$

Exercice 2: Additionneur binaire

Un additionneur binaire est un circuit électronique permettant de réaliser des additions sur des entiers positifs écrits en base 2. Un additionneur additionnant des nombres codés sur n bits possède $2 \times n$ entrées et $n + 1$ sorties (en effet, en binaire $10 + 10 = 100$).

On souhaite vérifier un additionneur binaire en contrôlant ses sorties en fonction de ses entrées. L'additionneur est représenté par $n + 1$ formules A_1, \dots, A_{n+1} ayant $2n$ variables représentant les entrées du circuit et telle que la valeur de vérité de A_k correspond à la valeur de la $k^{ième}$ sortie.

1. Donner la table de vérité de deux fonctions pour l'addition de 3 bits:

- la première calcule la somme des 3 bits sans retenue (i.e. $1 + 1 + 1 \mapsto 1$);
- la seconde calcule la retenue de cette somme.

Correction:

p	q	r	somme	retenue
1	1	1	1	1
1	1	0	0	1
1	0	1	0	1
1	0	0	1	0
0	1	1	0	1
0	1	0	1	0
0	0	1	1	0
0	0	0	0	0

2. Donner deux formules réalisant ces fonctions.

Correction:

- somme: $S = p \Leftrightarrow (q \Leftrightarrow r)$
- retenue: $R = (p \Rightarrow (q \vee r)) \wedge (\neg p \Rightarrow (q \wedge r))$

3. En déduire les formules spécifiant les sorties d'un additionneur 2 bits. On considère que les entiers sont représentés avec le bit de poids faible ayant le plus petit indice, que le premier entier est représenté par p_1, p_2 et que le second est représenté par q_1, q_2 .

Correction:

- $B_1 = p_1 \Leftrightarrow \neg q_1$ (obtenue à partir de la formule pour la somme en remplaçant r par \perp).
- On pose $R_1 = p_1 \wedge q_1$ (obtenue à partir de la formule pour la retenue en remplaçant r par \perp). On a alors $B_2 = S[p_2/p, q_2/q, R_1/r] = p_2 \Leftrightarrow (q_2 \Leftrightarrow (p_1 \wedge q_1))$.
- $B_3 = R[p_2/p, q_2/q, R_1/r] = (p_2 \Rightarrow (q_2 \vee (p_1 \wedge q_1))) \wedge (\neg p_2 \Rightarrow (q_2 \wedge p_1 \wedge q_1))$.

4. Généraliser la construction précédente pour donner une manière de construire les formules de spécification des sorties d'un additionneur n bits.

Correction: On construit itérativement les formules B_k et R_k selon le schéma suivant:

- $B_1 = p_1 \Leftrightarrow \neg q_1$
- $R_1 = p_1 \wedge q_1$
- $B_k = S[p_k/p, q_k/q, R_{k-1}/r]$ pour $2 \leq k \leq n$
- $R_k = R[p_k/p, q_k/q, R_{k-1}/r]$ pour $2 \leq k \leq n + 1$
- $B_{n+1} = R_{n+1}$

5. Expliquer comment on peut utiliser ces formules avec les formules A_1, \dots, A_{n+1} afin de vérifier que l'additionneur est correct.

Correction: Il suffit de vérifier que $A_i \equiv B_i$ pour $1 \leq i \leq n + 1$.

Exercice 3:

Pour chacune des formules *motif*, dire quelles sont les formules *candidat* qui en sont des instances et avec quelle substitution. Lorsqu'une formule candidat n'est pas une instance d'une formule motif, indiquer l'endroit où il y a non-correspondance.

motifs	candidats
$p \Rightarrow q \wedge r$	$u \Rightarrow (s \vee t) \wedge s$
$p \vee q \Rightarrow r$	$u \vee t \Rightarrow u \wedge (u \vee t)$
$p \Rightarrow p \wedge q$	$\perp \vee u \Rightarrow (\perp \vee u) \wedge s$
$p \vee q \Rightarrow p \wedge (r \vee q)$	

Correction:

	$u \Rightarrow (s \vee t) \wedge s$	$u \vee t \Rightarrow u \wedge (u \vee t)$	$\perp \vee u \Rightarrow (\perp \vee u) \wedge s$
$p \Rightarrow q \wedge r$	$[u/p, s \vee t/q, s/r]$	$[u \vee t/p, u/q, u \vee t/r]$	$[\perp \vee u/p, \perp \vee u/q, s/r]$
$p \vee q \Rightarrow r$	non: u pour $p \vee q$	$[u/p, t/q, u \wedge (u \vee t)/r]$	$[\perp/p, u/q, (\perp \vee u) \wedge s/r]$
$p \Rightarrow p \wedge q$	non: u vs $s \vee t$ pour p	non: $u \vee t$ vs u pour p	$[\perp \vee u/p, s/q]$
$p \vee q \Rightarrow p \wedge (r \vee q)$	non: u pour $p \vee q$	$[u/p, t/q, u/r]$	non: \perp vs $\perp \vee u$ pour p

Exercice 4:

Démontrer que les séquents suivants sont corrects en utilisant le système \mathcal{G} :

- $(p \Rightarrow q) \wedge p \vdash q$
- $\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
- $p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$
- $\vdash p \vee (q \wedge r) \Rightarrow (p \vee q) \wedge (p \vee r)$

Correction:

- $(p \Rightarrow q) \wedge p \vdash q$

$$\frac{\frac{\overline{p \vdash q, p} (Ax)}{p \Rightarrow q, p \vdash q} (\Rightarrow_G) \quad \frac{\overline{p, q \vdash q} (Ax)}{p, q \vdash q} (\Rightarrow_G)}{p \Rightarrow q, p \vdash q} (\wedge_G)$$

- $\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

$$\frac{\frac{\overline{p \vdash q, p} (Ax)}{p \vdash q, p} (\Rightarrow_D) \quad \frac{\overline{p \vdash p} (Ax)}{p \vdash p} (\Rightarrow_G)}{p \Rightarrow q \Rightarrow p \vdash p} (\Rightarrow_D)}{\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p} (\Rightarrow_D)$$

- $p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$

$$\frac{\frac{\overline{p, q \Rightarrow r \vdash r, p} (Ax)}{p, q \Rightarrow r \vdash r, p} (\Rightarrow_G) \quad \frac{\frac{\overline{p, q \vdash r, q} (Ax)}{p, q \vdash r, q} (\Rightarrow_G) \quad \frac{\overline{p, q, r \vdash r} (Ax)}{p, q, r \vdash r} (\Rightarrow_G)}{p, q, q \Rightarrow r \vdash r} (\Rightarrow_G)}{p, p \Rightarrow q, q \Rightarrow r \vdash r} (\Rightarrow_D)}{p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r} (\Rightarrow_D)$$

- $\vdash p \vee (q \wedge r) \Rightarrow (p \vee q) \wedge (p \vee r)$

$$\begin{array}{c}
\frac{\frac{\frac{\overline{p \vdash p, q} (Ax)}{p \vdash p \vee q} (\vee_D) \quad \frac{\overline{p \vdash p, r} (Ax)}{p \vdash p \vee r} (\vee_D)}{p \vdash (p \vee q) \wedge (p \vee r)} (\wedge_D) \quad \frac{\frac{\frac{\overline{q, r \vdash p, q} (Ax)}{q, r \vdash p \vee q} (\vee_D) \quad \frac{\overline{q, r \vdash p, r} (Ax)}{q, r \vdash p \vee r} (\vee_D)}{q, r \vdash (p \vee q) \wedge (p \vee r)} (\wedge_D)}{q \wedge r \vdash (p \vee q) \wedge (p \vee r)} (\wedge_G)}{\frac{p \vee (q \wedge r) \vdash (p \vee q) \wedge (p \vee r)}{\vdash p \vee (q \wedge r) \Rightarrow (p \vee q) \wedge (p \vee r)} (\Rightarrow_D)} (\vee_G)
\end{array}$$

Exercice 5:

Montrer que la règle (\vee_D) du système \mathcal{G} et la règle (\Rightarrow_G) du système \mathcal{G} sont correctes.

Correction: On pose $\Gamma = \{\{A_1, \dots, A_n\}\}$ et $\Delta = \{\{B_1, \dots, B_k\}\}$. Remarque: les cas présentés ne sont pas toujours mutuellement exclusifs, mais ce n'est pas grave.

(\vee_D) : Si $\Gamma \vdash \Delta, A, B$ est correct, alors $\models \bigwedge_{i=1}^n A_i \Rightarrow \bigvee_{i=1}^k B_i \vee A \vee B$. Alors $\models \bigwedge_{i=1}^n A_i \Rightarrow \bigvee_{i=1}^k B_i \vee (A \vee B)$ et donc $\Gamma \vdash \Delta, A, \vee B$ est correct.

(\Rightarrow_G) : Si $\Gamma \vdash A, \Delta$ est correct, alors $\models \bigwedge_{i=1}^n A_i \Rightarrow A \vee \bigvee_{i=1}^k B_i$. Si $\Gamma, B \vdash \Delta$ est correct, alors $\models \bigwedge_{i=1}^n A_i \wedge B \Rightarrow \bigvee_{i=1}^k B_i$. On pose $C = \bigwedge_{i=1}^n A_i \wedge (A \Rightarrow B) \Rightarrow \bigvee_{i=1}^k B_i$. Pour toute interprétation I :

- Soit $[\bigwedge_{i=1}^n A_i]_I = 0$, alors $[\bigwedge_{i=1}^n A_i \wedge (A \Rightarrow B)]_I = 0$ et $[C]_I = 1$.
- Soit $[\bigvee_{i=1}^k B_i]_I = 1$, alors $[C]_I = 1$.
- Soit $[A]_I = 1$ et $[B]_I = 0$. Alors $[A \Rightarrow B]_I = 0$, donc $[\bigwedge_{i=1}^n A_i \wedge (A \Rightarrow B)]_I = 0$, d'où $[C]_I = 1$.

Donc $\models \bigwedge_{i=1}^n A_i \wedge (A \Rightarrow B) \Rightarrow \bigvee_{i=1}^k B_i$, donc $\Gamma, A \Rightarrow B \vdash \Delta$ est correct.

Règles du système \mathcal{G}

$$\begin{array}{ll}
(\vee_G) \quad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} & (\vee_D) \quad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B} \\
(\wedge_G) \quad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} & (\wedge_D) \quad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \\
(\Rightarrow_G) \quad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta} & (\Rightarrow_D) \quad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta} \\
(\neg_G) \quad \frac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta} & (\neg_D) \quad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \\
(Axiome) \quad \overline{\Gamma, A \vdash \Delta, A} &
\end{array}$$