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 $\{\top, \bot, \neg, \wedge, \Rightarrow, \vee\}$ 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}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_1^{21}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \bot)$	$\bot$
f_1^{21}	$(p_z \Rightarrow \top) \wedge (\neg p_z \Rightarrow \bot)$	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	$(p_y \Rightarrow \bot) \wedge (\neg p_y \Rightarrow p_z)$	$\neg(p_z \Rightarrow p_y)$
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}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \bot)$	$\bot$
f_2^{12}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_2^{21}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \top)$	$\neg p_z$
f_2^{21}	$(p_z \Rightarrow \bot) \wedge (\neg p_z \Rightarrow \bot)$	$\bot$
f_2^1	$(p_y \Rightarrow \bot) \wedge (\neg p_y \Rightarrow \neg p_z)$	$\neg p_y \wedge \neg p_z$
f_2^2	$(p_y \Rightarrow \neg p_z) \wedge (\neg p_y \Rightarrow \bot)$	$p_y \wedge \neg p_z$
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 entier positifs écrit 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 $A_1, \ldots, A_{n+1}$ ayant $2n$ variables représentant les entrées du circuit et telle que valeur de vérité de A_k correpond à la valeur de la k^{ieme} 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 entier 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 replaçant r par $\perp$).
   - On pose $R_1 = p_1 \wedge q_1$ (obtenue à partir de la formule pour la retenue en replaçant 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 $A_1, \ldots, A_{n+1}$ 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
$p \Rightarrow q \land r$	$u \Rightarrow (s \lor t) \land s$
$p \lor q \Rightarrow r$	$u \lor t \Rightarrow u \land (u \lor t)$
$p \Rightarrow p \land q$	$\bot \lor u \Rightarrow (\bot \lor u) \land s$
$p \lor q \Rightarrow p \land (r \lor q)$	

Correction:

	$u \Rightarrow (s \lor t) \land s$	$u \lor t \Rightarrow u \land (u \lor t)$	$\bot \lor u \Rightarrow (\bot \lor u) \land s$
$p \Rightarrow q \land r$	$[{}^{u}/_{p}, {}^{s\lor t}/_{q}, {}^{s}/_{r}]$	$[{}^{u\lor t}/_{p}, {}^{u}/_{q}, {}^{u\lor t}/_{r}]$	$[{}^{\bot\lor u}/_{p}, {}^{\bot\lor u}/_{q}, {}^{s}/_{r}]$
$p \lor q \Rightarrow r$	non: u pour $p \lor q$	$[{}^{u}/_{p}, {}^{t}/_{q}, {}^{u\land(u\lor t)}/_{r}]$	$[{}^{\bot}/_{p}, {}^{u}/_{q}, {}^{(\bot\lor u)\land s}/_{r}]$
$p \Rightarrow p \land q$	non: u vs $s \lor t$ pour p	non: $u \lor t$ vs u pour p	$[{}^{\bot\lor u}/_{p}, {}^{s}/_{q}]$
$p \lor q \Rightarrow p \land (r \lor q)$	non: u pour $p \lor q$	$[{}^{u}/_{p}, {}^{t}/_{q}, {}^{u}/_{r}]$	non:$\bot$ vs $\bot \lor u$ pour p

Exercice 4:

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

- $(p \Rightarrow q) \land p \vdash q$
- $\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
- $p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$
- $\vdash p \lor (q \land r) \Rightarrow (p \lor q) \land (p \lor r)$

Correction:

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

$$\dfrac{\dfrac{\dfrac{}{p \vdash q, p}(Ax) \qquad \dfrac{}{p, q \vdash q}(Ax)}{p \Rightarrow q, p \vdash q}(\Rightarrow_G)}{(p \Rightarrow q) \land p \vdash q}(\land_G)$$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash q, p}(Ax)}{\vdash p \Rightarrow q, p}(\Rightarrow_D) \qquad \dfrac{}{p \vdash p}(Ax)}{(p \Rightarrow q) \Rightarrow p \vdash p}(\Rightarrow_G)}{\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p}(\Rightarrow_D)$$

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

$$\dfrac{\dfrac{\dfrac{}{p, q \Rightarrow r \vdash r, p}(Ax) \qquad \dfrac{\dfrac{}{p, q \vdash r, q}(Ax) \qquad \dfrac{}{p, q, r \vdash r}(Ax)}{p, q, q \Rightarrow r \vdash r}(\Rightarrow_G)}{p, p \Rightarrow q, q \Rightarrow r \vdash r}(\Rightarrow_G)}{p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r}(\Rightarrow_D)$$

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

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash p, q}(Ax)}{p \vdash p \vee q}(\vee_D) \quad \dfrac{\dfrac{}{p \vdash p, r}(Ax)}{p \vdash p \vee r}(\vee_D)}{p \vdash (p \vee q) \wedge (p \vee r)}(\wedge_D) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{q, r \vdash p, q}(Ax)}{q, r \vdash p \vee q}(\vee_D) \quad \dfrac{\dfrac{}{q, r \vdash p, r}(Ax)}{q, r \vdash p \vee r}(\vee_D)}{q, r \vdash (p \vee q) \wedge (p \vee r)}(\wedge_D)}{q \wedge r \vdash (p \vee q) \wedge (p \vee r)}(\wedge_G)}{p \vee (q \wedge r) \vdash (p \vee q) \wedge (p \vee r)}(\vee_G)}{\vdash p \vee (q \wedge r) \Rightarrow (p \vee q) \wedge (p \vee r)}(\Rightarrow_D)
$$

Exercice 5:

Montrer que la règle $(\vee_D)$ du système $\mathcal{G}$ et la règle $(\Rightarrow_G)$ du système $\mathcal{LK}$ sont correctes.
Correction: On pose $\Gamma = \{\{A_1, \ldots, A_n\}\}$ et $\Delta = \{\{B_1, \ldots, B_k\}\}$. 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 $\mathcal{G}$

$$(\vee_G) \quad \dfrac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \qquad\qquad (\vee_D) \quad \dfrac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

$$(\wedge_G) \quad \dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad\qquad (\wedge_D) \quad \dfrac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}$$

$$(\Rightarrow_G) \quad \dfrac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta} \qquad\qquad (\Rightarrow_D) \quad \dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}$$

$$(\neg_G) \quad \dfrac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta} \qquad\qquad (\neg_D) \quad \dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A}$$

$$(Axiome) \quad \dfrac{}{\Gamma, A \vdash \Delta, A}$$