CORRECTION SERIE 2

Cours : Vérification formelle
Filière/Classe : 3ème ING

Exercice 1 :

Ecrire les formules suivantes en utilisant uniquement les opérateurs basiques, soient **$\wedge$, $\neg$, EX, EG, EU** :

1. **AG**(**AF** p $\Rightarrow$**AF** q)
2. **AF**(p$\vee$ **AG** q)

Correction :

1. AG(AF p $\Rightarrow$ AF q) = $\neg$EF $\neg$(AF p $\Rightarrow$ AF q) = $\neg$EF $\neg$($\neg$AF p $\vee$ AF q) = $\neg$EF(AF p $\wedge$ $\neg$AF q) =$\neg$EF($\neg$EG$\neg$p $\wedge$ EG$\neg$q) =$\neg$E true U($\neg$EG$\neg$p $\wedge$ EG$\neg$q) =

2. AF(p $\vee$ AG q) = $\neg$EG$\neg$ (p $\vee$ AG q)= $\neg$EG($\neg$p $\wedge$ $\neg$AG q)= $\neg$EG($\neg$p $\wedge$ EF$\neg$q)= $\neg$(EG($\neg$p $\wedge$ E true U $\neg$q))

Exercice 2 :

Dire si les équivalences suivantes sont valides. Pour une réponse positive justifier votre réponse et pour une réponse négative donner un contre-exemple.

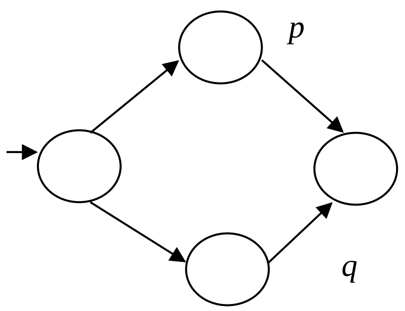
1. **EF**($p\vee q$)=**EF** p $\vee$ **EF** q
2. **EF**($p\wedge q$)=**EF** p $\wedge$ **EF** q

Correction :

1. **EF**($p\vee q$) = **EF** p $\vee$ **EF** q :
   Vrai et voici la preuve :

   Supposons que K $\vDash$ **EF**($p\vee q$), alors il existe une exécution s_0s_1 … tel qu'il existe i $\geq$0 avec $s_i \vDash p\vee q$, ceci veut dire que soit $s_i \vDash p$ ou $s_i \vDash q$ ou les deux. Donc il existe une exécution t_0t_1 … tel que $t_i \vDash p$ ou il existe une exécution t_0t_1 … tel que $t_i \vDash q$, donc K $\vDash$ **EF** p $\vee$ **EF** q.

2. **EF**($p\wedge q$)=**EF** p $\wedge$ **EF** q
   Faux. Voici un contre exemple où nous avons K $\vDash$**EF**p et K $\vDash$**EF**q mais K $\nvDash$**EF** $p\wedge q$:



Exercice 3 :

Dire pour chacune des propositions suivantes si elle est vraie ou fausse :

1. *Fp* est-il vrai si *p* vrai tout de suite dans l'état courant ?
2. *Gp* est-il vrai si *p* faux dans l'état courant et vrai partout ailleurs ?
3. *pUq* est-il vrai si *p* faux et *q* vrai dans l'état courant ?
4. *pUq* est-il vrai si *q* est toujours faux, et *p* toujours vrai ?

Correction :

1. **F***p* est-il vrai si *p* vrai tout de suite dans l'état courant ?

   $\sigma, i \vDash Fp \; ssi \; \exists j | i \leq j \leq |\sigma| \; et \; \sigma, j \vDash p$

   Vrai. Comme *p* est vrai à l'état courant donc vous n'avez qu'à prendre i=j.

2. **G***p* est-il vrai si *p* faux dans l'état courant et vrai partout ailleurs ?

   $\sigma, i \vDash Gp \; ssi \; \forall j | i \leq j \leq |\sigma| \; on \; a \; \sigma, j \vDash p$

   Faux. Nous avons p est vrai à l'état courant mais faux dans tous les autres états, donc $\exists j | i \leq j \leq |\sigma| \; et \; \sigma, \nvDash p$, vous pouvez prendre n'importe quel $j > 0$.

3. *p***U***q* est-il vrai si *p* faux et *q* vrai dans l'état courant ?

   $\sigma, i \vDash p\mathbf{U}q \; ssi \; \exists j | i \leq j \leq |\sigma| : \; \sigma, j \vDash q \; et \; \forall k | i \leq k < j \; on \; a \; \sigma, k \vDash p$

   Vrai. Puisque *q* est vrai à l'état courant, donc on peut prendre j=i et on aura $\sigma, j \vDash q$ et ceci vérifie aussi $\forall k | i \leq k < j = i \; on \; a \; \sigma, k \vDash p$ puisque le domaine est vide ($i \leq k < i$).

4. *p***U***q* est-il vrai si *q* est toujours faux, et *p* toujours vrai ?

   $\sigma, i \vDash p\mathbf{U}q \; ssi \; \exists j | i \leq j \leq |\sigma| : \; \sigma, j \vDash q \; et \; \forall k | i \leq k < j \; on \; a \; \sigma, k \vDash p$

   Faux. Puisque $\nexists j | i \leq j \leq |\sigma| : \; \sigma, j \vDash q$.

Exercice 4 :

Exprimer les propriétés suivantes en CTL :

1. Tous les états satisfont p.
2. On peut atteindre *p* par un chemin où *q* est toujours vrai.
3. Quel que soit l'état, on finit par aller à un état où *p* vrai.
4. Quel que soit l'état, on peut aller à un état où *p* vrai.
5. Absence de deadlock.

Correction :

1. Tous les états satisfont p.
   $\mathbf{AG}p$

2. On peut atteindre p par un chemin où q est toujours vrai.
   $q\mathbf{EU}p$.
   On peut aussi penser à la formule CTL* $\mathbf{E}(\mathbf{F}p\wedge\mathbf{G}q)$, il est à noter que $q\mathbf{EU}p$ signifie qu'il existe un chemin dans lequel p est *vrai* et ce jusqu'à ce que q soit *vrai*, alors que $\mathbf{E}(\mathbf{F}p\wedge\mathbf{G}q)$ signifie qu'il existe un chemin, dans lequel q est toujours *vrai*, et p est atteignable.

3. Quel que soit l'état, on finit par aller à un état où p vrai.
   $\mathbf{AGAF}p$: on finit nécessairement par atteindre p à partir de tout état. Il est à noter que $\mathbf{AF}p$ ne veut pas dire la même chose, qui exprime le fait que p est atteignable à partir de l'état initial et ce dans toutes les exécutions.

4. Quel que soit l'état, on peut aller à un état où p vrai.
   $\mathbf{AGEF}p$

5. Absence de deadlock.
   $\mathbf{AGEX}$*vrai* : chaque état a un successeur

Exercice 5 :

Exprimer en LTL les propriétés suivantes :

1. Il est possible d'atteindre un état à partir duquel p_1 sera toujours fausse.
2. Si p_1 est infiniment souvent vrai, alors p_2 reste toujours faux.
3. p_1 doit être fausse et ce jusqu'à ce que p_2 devienne vraie, mais si cette dernière ne devienne pas vraie, p_1 doit rester fausse.

Correction :

1. Il est possible d'atteindre un état à partir duquel p_1 sera toujours fausse.
   $\mathbf{FG}\neg p_1$. (Dans toutes les exécutions)
2. Si p_1 est infiniment souvent vrai, alors p_2 reste toujours faux.
   $\mathbf{GF}p_1 \Rightarrow \mathbf{G}\neg p_2$.
3. p_1 doit être fausse et ce jusqu'à ce que p_2 devienne vraie, mais si cette dernière ne devienne pas vraie, p_1 doit rester fausse.
   $\neg p_1\mathbf{GW}p_2$ ($p\mathbf{GW}q \equiv (p\mathbf{U}q) \vee \mathbf{G}p$)

Exercice 6 :

On va voir que certains connecteurs sont redondants.

1. Exprimer $\mathbf{G}p$ avec les connecteurs : $\neg$, $\mathbf{F}$ et p.
2. Exprimer $\mathbf{F}p$ grâce au connecteur $\mathbf{U}$.
3. Peut-on exprimer $\mathbf{X}$ en fonction des autres connecteurs ?
4. Peut-on exprimer $\mathbf{U}$ en fonction des autres connecteurs ?

Correction :

1. Exprimer **G**p avec les connecteurs : ¬, F et p.
   $\mathbf{G}p \equiv \neg\mathbf{F}\neg p$

2. Exprimer **F**p grâce au connecteur U.
   $\mathbf{F}p \equiv true\mathbf{U}p$

3. Peut-on exprimer **X** en fonction des autres connecteurs ?

   Non. **X** est le seul opérateur qui impose fortement quand va avoir l'observation (prochain coup), ce qui ne peut être fait par les autres opérateurs.

4. Peut-on exprimer **U** en fonction des autres connecteurs ?
   Non. L'opérateur **U** est binaires, alors que **X**, **F** et **G** sont unaires.

Exercice 7 :

1. Nous allons définir quelques connecteurs utiles en donnant la sémantique formelle (⊨)
   a. $p\boldsymbol{W}q$ (weak until) : signifie que p est vrai jusqu'à ce que q soit vrai, mais q n'est pas forcément vrai à un moment. Dans ce cas, p reste vrai tout le long du chemin.
   b. $\boldsymbol{GF}p$ *ou* $\boldsymbol{F}^{\infty}p$ (infiniment souvent) : p est infiniment vrai au long de l'exécution.
   c. $\boldsymbol{FG}p$ *ou* $\boldsymbol{G}^{\infty}p$ (presque toujours) : àpartir d'un moment donné, p est toujours vrai.
   d. $p\boldsymbol{R}q$ (release) : q est vraie jusqu'à (et inclus) le premier état où p est vraie, et p n'est pas forcément vraie un jour.

Correction :

1.
   a. $p\mathbf{W}q$ (weak until) : signifie que p est vrai jusqu'à ce que q soit vrai, mais q n'est pas forcément vrai à un moment. Dans ce cas, p reste vrai tout le long du chemin.

$$\sigma, i \vDash p\mathbf{W}q \; ssi \; (\forall j | i \leq j \leq |\sigma| : \; \sigma, j \vDash p)$$
$$\vee \; (\exists t | i \leq t \leq |\sigma| : \; \sigma, t \vDash q \; et \; \forall k | i \leq k < t : k \vDash p)$$

   Comme $p\mathbf{GW}q \equiv (\mathbf{G}p \;\vee (p\mathbf{U}q))$, la première partie de la disjonction exprime la sémantique de $\mathbf{G}p$ et la deuxième définit la sémantique de $p\mathbf{U}q$.

   b. $\mathbf{GF}p$ *ou* $\mathbf{F}^{\infty}p$ (infiniment souvent) : p est infiniment vrai au long de l'exécution.

$$\sigma, i \vDash \mathbf{GF}p \; ssi \; (\forall j | i \leq j \leq |\sigma| : (\exists k \mid j \leq k \leq |\sigma| : \sigma, k \vDash p))$$

   c. $\mathbf{FG}p$ *ou* $\mathbf{G}^{\infty}p$ (presque toujours) : àpartir d'un moment donné, p est toujours vrai.

$$\sigma, i \vDash \mathbf{FG}p \; ssi \; (\exists j | i \leq j \leq |\sigma| : (\forall k \mid j \leq k \leq |\sigma| : \sigma, k \vDash p))$$

   d. $p\mathbf{R}q$ (release) : q est vraie jusqu'à (et inclus) le premier état où p est vraie, et p n'est pas forcément vraie un jour.

$$\sigma, i \vDash p\mathbf{R}q \ ssi \ (\forall j \ | i \leq j \leq |\sigma| : \sigma, j \vDash q) \ \lor [(\exists k | i \leq k \leq |\sigma| : \sigma, k \vDash p \land q \ et \ \forall t : i \leq t \leq k : \sigma, t \vDash q)]$$

En effet, $p\mathbf{R}q \equiv \mathbf{G}q \lor (q\mathbf{U}(p \land q))$.

Exercice 8 :

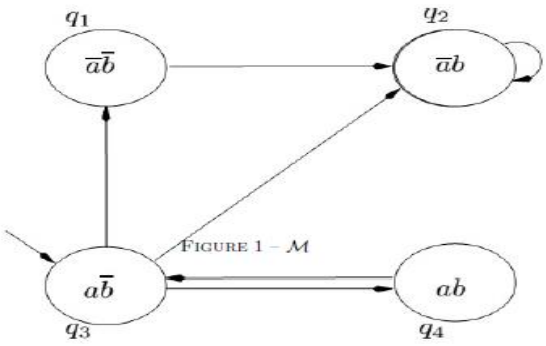


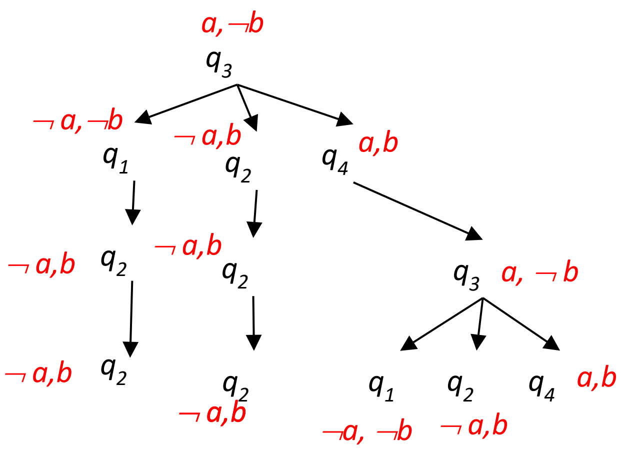
FIGURE 1 – $\mathcal{M}$

Soit le modèle M donné par la figure 1

1. Représentez l'arbre d'exécution de M (dépliage) à partir de l'état initial, on donnera les 4 premiers niveaux.
2. Donnez les exécutions de cet automate.
3. Pour chacune de ces formules dites si la formules est satisfaite et trouvez un chemin à partir de $q3$ qui satisfait la formule, et un chemin qui ne la satisfait pas, quand c'est possible :
   a. Ga.
   b. aUb.
   c. $aUX(a \land \neg b)$.
   d. $X\neg b \land G(\neg a \lor \neg b)$
   e. $X(a \land b) \land F(\neg a \land \neg b)$

Correction :

1. Représentez l'arbre d'exécution de M (dépliage) à partir de l'état initial, on donnera les 4 premiers niveaux.



2. Donnez les exécutions de cet automate.
   $\sigma_1 = q_3 q_1 q_2 q_2 q_2 \dots$
   $\sigma_2 = q_3 q_2 q_2 q_2 \dots$
   $\sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots$
   $\sigma_4 = q_3 q_4 q_3 q_4 q_3 q_4 \dots$
   $\sigma_5 = q_3 q_4 q_3 q_4 q_3 q_1 q_2 q_2 q_2 \dots$
   $\sigma_6 = q_3 q_4 q_3 q_4 q_3 q_2 q_2 q_2 \dots$

3. Pour chacune de ces formules trouvez un chemin à partir de $q3$ qui satisfait chacune des formules, sinon donnez un chemin qui ne la satisfait pas :
   a. $\mathbf{G}a$.
      $M \nvDash \mathbf{G}a$
      $M, \sigma_1 = q_3 q_1 q_2 q_2 q_2 \dots \nvDash \mathbf{G}a$
      $M, \sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots \vDash \mathbf{G}a$

   b. $M \nvDash a\mathbf{U}b$.
      $M, \sigma_1 = q_3 q_1 q_2 q_2 q_2 \dots \nvDash a\mathbf{U}b$
      $M, \sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots \vDash a\mathbf{U}b$

   c. $M \nvDash a\mathbf{UX}(a \wedge \neg b)$.
      $M, \sigma_1 = q_3 q_1 q_2 q_2 q_2 \dots \nvDash a\mathbf{UX}(a \wedge \neg b)$
      $M, \sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots \vDash a\mathbf{UX}(a \wedge \neg b)$

   d. $M \nvDash \mathbf{X}\neg b \ \wedge \mathbf{G}(\neg a \vee \neg b)$.
      $M, \sigma_2 = q_3 q_2 q_2 q_2 \dots \nvDash \mathbf{X}\neg b \ \wedge \mathbf{G}(\neg a \vee \neg b)$
      $M, \sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots \vDash \mathbf{X}\neg b \ \wedge \mathbf{G}(\neg a \vee \neg b)$

   e. $M \nvDash \mathbf{X}(a \wedge b) \wedge \mathbf{F}(\neg a \wedge \neg b)$.
      $M, \sigma_1 = q_3 q_1 q_2 q_2 q_2 \dots \nvDash \mathbf{X}(a \wedge b) \wedge \mathbf{F}(\neg a \wedge \neg b)$
      $M, \sigma_3 = q_3 q_4 q_3 q_4 q_3 q_4 \dots \nvDash \mathbf{X}(a \wedge b) \wedge \mathbf{F}(\neg a \wedge \neg b)$
      Aucune exécution ne satisfait le modèle.