Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Carthage
Ecole Nationale d'Ingénieurs de Carthage

وزارة التعليم العالي و البحث العلمي
جامعة قرطاج
المدرسة الوطنية للمهندسين بقرطاج

Nom :…….. **Prénom :**…… **CIN :**…… **Salle :**……

Correction Examen Final: Spécification formelle

Enseignantes	**:** E. Menif & M. Fourati	**Date**	**: 27**/01/2021	**Nbre. de pages**	**: 9**
Filière / Classe	**:** 3ème Ing. Inf. SI	**Calculatrices/documents**	**:** non autorisés	**Durée**	**:** 1h30

Vérification formelle : (10 points)

Exercice 1 : (Traduction en CTL et LTL: 1 point)

Exprimez, lorsque c'est possible, les propriétés suivantes en CTL et LTL. Lorsque la traduction n'est pas possible, dites qu'elle n'est pas exprimable.

1. Il est possible d'atteindre un état où p_1 est vrai et p_2 est vrai dans le prochain état.
   LTL **F**$(p_1 \wedge \mathbf{X}p_2)$ **0.25 pt**
   CTL : Non exprimable **0.25 pt**

2. Les propriétés p_1 et p_2 sont infiniment souvent vraies.
   LTL : **GF**$p_1 \wedge$ **GF**p_2 **0.25 pt**
   CTL : **AGAF**$p_1 \wedge$ **AGAF**p_2 **0.25 pt**

Exercice 2 Model Checking LTL et Automate de Büchi (5.25 points) :

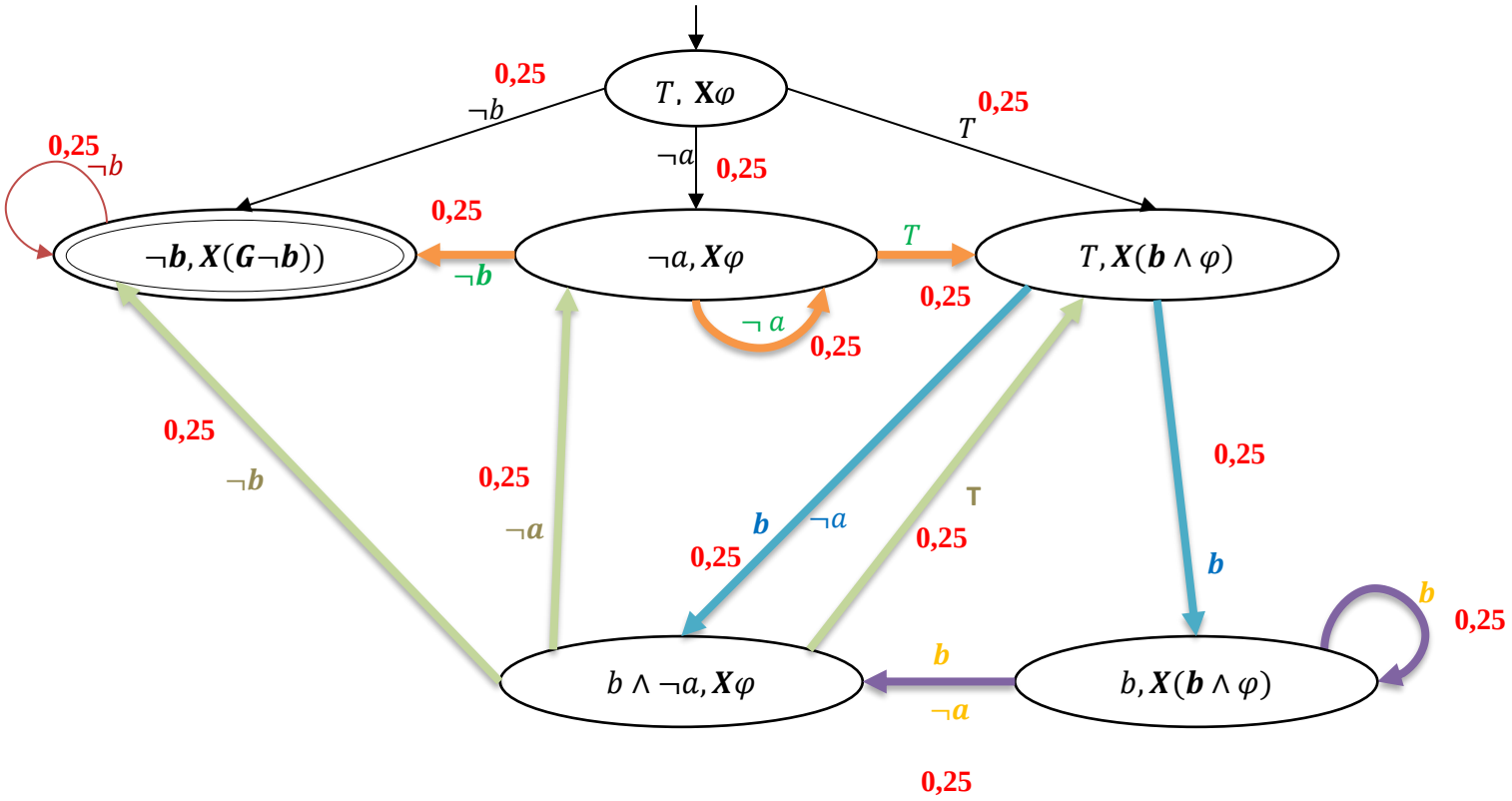
1. Transformez la propriété de chemin $\varphi = (a \Rightarrow \mathbf{X}b)\boldsymbol{U}(\boldsymbol{G}\neg\boldsymbol{b})$ en automates de Büchi minimal.
   Rappelons qu'on dispose des règles d'expansions : $\varphi\mathbf{U}\psi=\psi\vee(\varphi\wedge\mathbf{X}(\varphi\mathbf{U}\psi))$, $\mathbf{G}\varphi=\varphi\wedge\mathbf{X}(\mathbf{G}\varphi)$, $\mathbf{F}\varphi=\varphi\vee\mathbf{X}(\mathbf{F}\varphi)$. **1.25 point**

   $\varphi = (a \Rightarrow \mathbf{X}b)\mathbf{U}(\boldsymbol{G}\neg\boldsymbol{b}) = (\neg a \vee \mathbf{X}b)\mathbf{U}(\boldsymbol{G}\neg\boldsymbol{b}) = (\boldsymbol{G}\neg\boldsymbol{b}) \vee ((\neg a \vee \mathbf{X}b) \wedge \mathbf{X}\varphi))$
   $= (\boldsymbol{G}\neg\boldsymbol{b}) \vee (\neg a \wedge \mathbf{X}\varphi) \vee (\mathbf{X}b \wedge \mathbf{X}\varphi) = (\neg\boldsymbol{b} \wedge \mathbf{X}(\boldsymbol{G}\neg\boldsymbol{b})) \vee (\neg a \wedge \mathbf{X}\varphi) \vee (\mathbf{X}b \wedge \mathbf{X}\varphi)$ **0.5 pt**

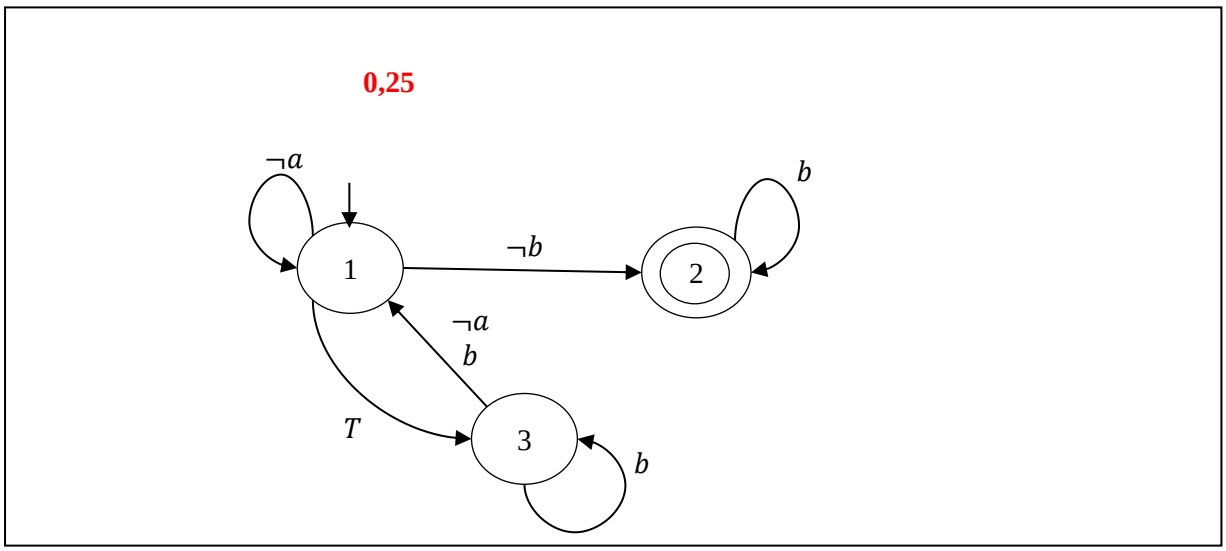
   $(\boldsymbol{G}\neg\boldsymbol{b}) = \neg\boldsymbol{b} \wedge \mathbf{X}(\boldsymbol{G}\neg\boldsymbol{b})$ **0.25 pt**

   $b \wedge \varphi = b \wedge \Big((\neg\boldsymbol{b} \wedge \mathbf{X}(\boldsymbol{G}\neg\boldsymbol{b})) \vee (\neg a \wedge \mathbf{X}\varphi) \vee (\mathbf{X}b \wedge \mathbf{X}\varphi)\Big) = \Big((b \wedge \neg\boldsymbol{b} \wedge \mathbf{X}(\boldsymbol{G}\neg\boldsymbol{b})) \vee$
   $(b \wedge \neg a \wedge \mathbf{X}\varphi) \vee (b \wedge \mathbf{X}b \wedge \mathbf{X}\varphi)\Big) = (b \wedge \neg a \wedge \mathbf{X}\varphi) \vee (b \wedge \mathbf{X}b \wedge \mathbf{X}\varphi)$ **0.5 pt**

Automate : **3.5+0.25 pour l'état final**



Automate minimal :



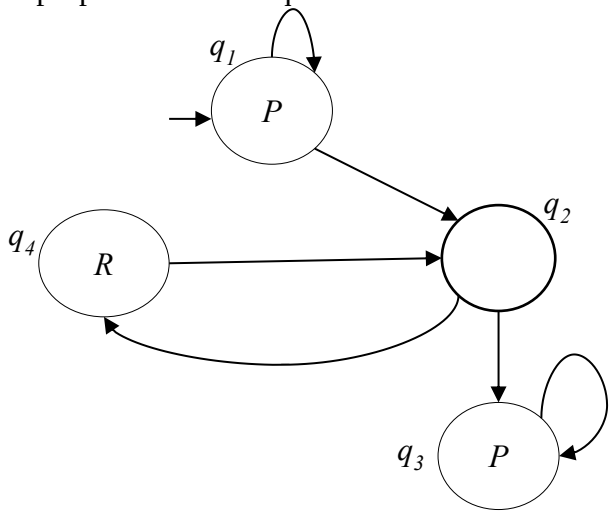
Exercice 4 : (Model-Checking CTL 4,5 points)

1. Normalisez la formule φ=**AF**(**AG**p) (l'écrire en terme de AU, EU, EX, $\wedge$,$\neg$ et T). Rappelons que **AX**ϕ = $\neg$**EX**$\neg\phi$, **AF**ϕ = T**AU**ϕ, **AG**ϕ = $\neg$**EF**$\neg\phi$, **EF**ϕ = T**EU**ϕ, **EG**ϕ = $\neg$**AF**$\neg\phi$.

Correction

$\mathbf{AF}(\mathbf{AG}p) = T\mathbf{AU}(\neg\mathbf{EF}\neg p) = T\mathbf{AU}(\neg T\mathbf{EU}\neg p)$ **(0,25 point)**

2. Soit la structure de Kripke K suivant, P et R sont des propositions atomiques :



A l'aide de l'algorithme de marquage vu en cours (*et présenté ci-bas*), vérifiez la validité de la formule φ pour chaque état du modèle. Détaillez les itérations (précisez les valeurs de *L,nb* (degré de chaque état) et *déjà vu* pour toutes les variables q_i ainsi que les valeurs des sous formules φ_i pour chaque état). Toutes les itérations doivent être détaillées. Ensuite, remplissez la table ci-dessous (par les valeurs de vérité adéquates) pour chaque sous formule de φ. Le tableau ne sera pas noté si l'itération correspondante n'est pas explicitée.

$\phi = T\mathbf{AU}(\neg T\mathbf{EU}\neg p)$

$\phi_1 = T\mathbf{EU}\neg p$

Marquage de T et $\neg p$ et initialisation de ϕ_1 à faux.

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$faux$	$faux$	$faux$	$faux$
$\phi_2 = \neg\phi_1$				
$\phi = T\mathbf{AU}\phi_2$				

Initialisation de *déjà vu (dv)*.

	q_1	q_2	q_3	q_4
dv	$faux$	$faux$	$faux$	$faux$

Initialisation de L=∅.
L={q_2, q_4} (q_2.¬*p*=*vrai et* q_4.¬*p*=*vrai*) ***0.25 pt***

1) *Traitement de* q_2, *L*={q_4}
   $q_2.\phi_1$:=*vrai* ***0.25 pt***
   a. $q_1 \rightarrow q_2$ ***0.25 pt***
      q_1.*dv=faux, donc* q_1.*dv*:=*vrai avec* q_1.*T=vrai donc L=L*∪{q_1}={q_1, q_4}

   b. $q_4 \rightarrow q_2$ ***0.25 pt***
      q_4.*dv=faux, donc* q_4.*dv*:=*vrai avec* q_4.*T=vrai donc L=L*∪{q_4}={q_1, q_4}

      Mise à jour de *dv* et de ϕ_1.

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$faux$	$vrai$	$faux$	$faux$
dv	$vrai$	$faux$	$faux$	$vrai$

2) *Traitement de* q_1, *L*= {q_4}
   $q_1.\phi_1$:=*vrai* ***0.25 pt***
   a. $q_1 \rightarrow q_1$ ***0.25 pt***
      q_1.*dv=vrai, rien à faire*

      Mise à jour de *dv* et de ϕ_1.

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$vrai$	$vrai$	$faux$	$faux$
dv	$vrai$	$faux$	$faux$	$vrai$

3) *Traitement de* q_4, *L*={ }
   $q_4.\phi_1$:=*vrai* ***0.25 pt***
   a. $q_2 \rightarrow q_4$ ***0.25 pt***
      q_2.*dv=faux, donc* q_2.*dv*:=*vrai avec* s_2.*T=vrai donc L=L*∪{q_2}={q_2}

      Mise à jour de *dv* et de ϕ_1.

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$vrai$	$vrai$	$faux$	$vrai$
dv	$vrai$	$vrai$	$faux$	$vrai$

4) *Traitement de* q_2, $L=\{\ \}$ ***0.25 pt***
$q_2.\phi_1 := vrai$

a. $q_1 \rightarrow q_2$
$q_1.dv = vrai$, *donc rien à faire*

b. $q_4 \rightarrow q_2$
$q_4.dv = vrai$, *donc rien à faire*

Mise à jour de *dv* et de ϕ_1 : *rien à faire*

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$vrai$	$vrai$	$faux$	$vrai$
dv	$vrai$	$vrai$	$faux$	$vrai$

$\underline{\phi = T\mathbf{AU}(\neg T\mathbf{EU}\neg p)}$

Calcul de $\phi_2 = \neg\phi_1$, initialisation de ϕ à faux et calcul de *nb*.

	q_1	q_2	q_3	q_4
T	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$vrai$	$vrai$	$faux$	$vrai$
$\phi_2 = \neg\phi_1$ ***0.25 pt***	$faux$	$faux$	$vrai$	$faux$
$\phi = T\mathbf{AU}\phi_2$	$faux$	$faux$	$faux$	$faux$
nb ***0.25 pt***	2	2	1	1

Initialisation de L=∅.

$L=\{q_3\}$ $(q_3.\phi_2 = vrai)$ ***0.25 pt***

1) *Traitement de* q_3, $L=\{\ \}$
$q_3.\phi := vrai$ ***0.25 pt***

a. $q_2 \rightarrow q_3$ ***0.25 pt***
$q_2.nb := q_2.nb - 1 = 1 \neq 0$, *rien à faire*

b. $q_3 \rightarrow q_3$ ***0.25 pt***
$q_3.nb := q_3.nb - 1 = 0$, *avec* $q_3.T = vrai$, *mais* $q_3.\phi = vrai$ *donc rien à faire*

	q_1	q_2	q_3	q_4
T ***0.25 pt***	$vrai$	$vrai$	$vrai$	$vrai$
p	$vrai$	$faux$	$vrai$	$faux$
$\neg p$ ***0.25 pt***	$faux$	$vrai$	$faux$	$vrai$
$\phi_1 = T\mathbf{EU}\neg p$	$vrai$	$vrai$	$faux$	$vrai$
$\phi_2 = \neg\phi_1$	$faux$	$faux$	$vrai$	$faux$
$\phi = T\mathbf{AU}\phi_2$	$faux$	$faux$	$vrai$	$faux$

```
Entrées : formule CTL ϕ, M= (Q,q0,E,T,Prop,l)
Cas 5 : ϕ= ψ1EUψ2
faire marquage(ψ1,M) ; marquage(ψ2,M) ;
pour tout q∈Q faire
        q.ϕ:=faux;
        q.dejavu:=faux;
fin pour tout
L:=∅
pour tout q∈Q faire
   si q.ψ2=vrai alors L:=L∪{q} fin si
fin pour tout
tant que L≠∅ faire
        prendre un q ∈ L;
        L:=L\{q};
        q.ϕ:=vrai;
        pour tout (q',q) ∈T faire
                si q'.dejavu=faux alors
                  q'.dejavu := vrai;
                  si q'.ψ1=vrai alors L:=L∪{q'}
                  finsi
                fin si
        fin pour tout
fin tant que
```

```
Entrées : formule CTL ϕ, M= (Q,q0,E,T,Prop,l)
Cas 6 : ϕ= ψ1AUψ2
faire marquage(ψ1,M) ; marquage(ψ2,M) ;
L:=∅
pour tout q∈Q faire
        q.nb:=degre(q) ; q.ϕ:=faux ;
        si q.ψ2=vrai alors L:=L∪{q} fin si
fin pour tout
tant que L≠∅ faire
        prendre un q ∈ L;
        L:=L\{q};
        q.ϕ:=vrai;
        pour tout (q',q) ∈Tfaire
                q'.nb:=q'.nb-1
                si (q'.nb=0) et (q'.ψ1=vrai) et
                   (q'. ϕ =faux)  alors  L:=L ∪{q'}
                 fin si
        fin pour tout
fin tant que
```

Relations

Notation	**Sens**	**Définition**
dom R	Domaine	$\{x{:}X \mid (\exists y{:}Y \bullet (x,y) \in R)\}$
ran R	Codomaine	$\{y{:}Y \mid (\exists x{:}X \bullet (x,y) \in R)\}$
id R	Identité	$\{x{:}X \bullet x \mapsto x\}$
$R^{\sim}$	Inverse	$\{y{:}Y, x{:}X \mid (x,y) \in R\}$
$R \fatsemi R'$	Composition	$\{x{:}X, z{:}Z \mid (\exists y{:}Y \bullet (x,y) \in R \land (y,z) \in R')\}$
R^k	Composition récurrente	
$R(\!\mid S \mid\!)$	Image relationnelle	$\{y{:}Y \mid (\exists x{:}S \bullet (x,y) \in R)\}$
$S \lhd R$	Restriction du domaine	$\{x{:}X, y{:}Y \mid x \in S \land (x,y) \in R\}$
$R \rhd S'$	Restriction du codomaine	$\{x{:}X, y{:}Y \mid y \in S' \land (x,y) \in R\}$
$S \lhd\!\!\!- R$	Soustraction de domaine	$(X \setminus S) \lhd R$
$R \rhd\!\!\!- S'$	Soustraction de codomaine	$R \rhd (Y \setminus S')$
$R \oplus R'$	Surcharge	$\{x{:}X, y{:}Y \mid (x,y) \in R' \lor (x \notin \mathrm{dom}\ R' \land (x,y) \in R)\}$

Séquence

Notation	**Sens**	**Définition**
$\#s$	Cardinal	
$s \frown t$	concaténation	$\triangleq s \cup \{n{:}\ \mathrm{dom}\ t \bullet n + \#s \mapsto t(n)\}$
rev s	Inversion	$(\lambda n : \mathrm{dom}\ s \bullet s(\#s - n + 1))$
head s	Premier élément	$\forall s{:}\mathrm{seq}_1 X \bullet \mathrm{head}\ s = s(1)$
tail s	Liste sans le premier élément	$\forall s{:}\mathrm{seq}_1 X \bullet \mathrm{tail}\ s = (\lambda n : 1..\#s-1 \bullet s(n+1))$
last s	Dernier élément	$\forall s{:}\mathrm{seq}_1 X \bullet \mathrm{last}\ s = s(\#s)$
front s	Liste sans le dernier élément	$\forall s{:}\mathrm{seq}_1 X \bullet \mathrm{front}\ s = (1..(\#s-1)) \lhd s$
squash f	Construit une séquence à partir d'une fonction	$(\mathbb{N} \twoheadrightarrow X) \rightarrow \mathrm{seq}\ X$
$s \upharpoonright A$	Filtre une séquence en ne considérant que les éléments de A	squash $(s \rhd A)$
$s \upharpoonleft A$	Extrait une sous-séquence formée d'éléments avec des indices de A	squash $(A \lhd s)$

Quelques opérations utiles

$S \setminus T$	Différence	$S, T : \mathbb{P}X \quad \triangleq \{x : X \mid x \in S \land x \notin T\}$
$\bigcup SS$	Union distribuée	$SS : \mathbb{P}(\mathbb{P}X) \quad \triangleq \{x : X \mid \exists S : SS \bullet x \in S\}$
$\bigcap SS$	Intersection distribuée	$SS : \mathbb{P}(\mathbb{P}X) \quad \triangleq \{x : X \mid \forall S : SS \bullet x \in S\}$
min S	Minimum	$S : \mathbb{F}\mathbb{N} \mid S \neq \emptyset \quad \min S \in S \land (\forall x \in S \bullet x \geq \min S)$
max S	Maximum	$S : \mathbb{F}\mathbb{N} \mid S \neq \emptyset \quad \max S \in S \land (\forall x \in S \bullet x \leq \max S)$
succ: $\mathbb{N} \rightarrow \mathbb{N}$	Fonction successeur	$\triangleq \forall n{:}\mathbb{N} \bullet succ(n) = n+1$