iversité de Manouba

Nationale des Sciences
de l'Informatique

Section : ..... A. U : ..... / .....

Module : .....

Classe : .....

Session : .....

Total
s feuilles
les remises

Signature
des Surveillants

Nom : ..... Prénom : .....

N° C.I.N. :

N° d'inscription

Signature
de l'étudiant

: ..... Salle n° : ..... Place n° : .....

Note

Examen de : .....

Appréciations du correcteur

GL II

Total
feuilles
es remises

Model Checking :

Déf

- technique de vérification formelle
  - ↳ permet de vérifier les propriétés comportementales désirées d'un syst
  - ↳ vérification basé sur un modèle adéquat du syst
  - ↳ A travers une inspection systématique de tous les états du modèle.
  - ↳ Complètement automatique
- Méthode qui applique les mathématiques pour la modélisation et l'analyse du syst.
  - ↳ Etablir que le syst est Correct avec rigueur mathématique

syst ↓ modèle syst de transition. | satisfait ↓ = | spécification ↓ . la formule . la propriété.

fe17018c420040ea

NE RIEN ECRIRE ICI

terdit de signer la copie à la fin de la composition.

Importance :

✓ fortement recommandée comme technique de vérification pour le dév. de logiciels pour safety_critical syst. selon → NASA ; E.S.A ; FAA

✓ Certains erreurs fatales ds l'histoire de l'informatique ont pu être évitées si ces techniques sont utilisées.

Logique temporelle :

Besoins : ✓ traiter l'aspect dynamique du syst. (Comportement dans le temps).

✓ Exprimer des situations au moment de l'exécution.

✓ Décrire le séquencement d'évt observés le long de l'exécution.

➡ Logique temporelle

↳ Extension de la logique des prédicats avec les opérateurs qui permettent d'exprimer le comportement des syst au fil du temps.

⚠ Logique des prédicats + temps.

Logique temporelle ⟶ Spécifier des prop. sous forme de formules temporelles:

Logique temporelle linéaire propositionnelle (Linear time PLTL):
vue linéaire du temps.
↳ A chaque instant, on peut ∃ un seul instant successeur (future déterminé).

Logique temporelle arborescente (branching time CTL)
arbre d'exécution du syst.
future ambigüe.

Notion du temps:
Sens abstrait: Spécifier l'ordre des évts. (pas l'instant exacte de l'event).
↳ Durée de transition n'est pas spécifié.

- M: Syst. de transitions (implémentation représentée par un modèle sémantique).
- φ: formule temporelle (prop. temporelle).

Modèle checking: . est $M \models^{?} \varphi$
. M est-il un modèle pour la formule logique φ?

NE RIEN ECRIRE ICI

est interdit de signer la copie à la fin de la composition.

Types de propriétés temporelles :

- Accessibilité : Une certaine situation peut être atteinte.
- Invariance : tous les états du syst satisfait une bonne propriété.
- Sûreté : Quelque chose de mauvais n'arrive jamais.
- Vivacité : Quelque chose de bon finit par arriver.
- Equité : Quelque chose de bon se répète infiniment.
- Equivalence Comportementale : est-ce que 2 syst sont équivalents ?

PLTL :

→ les opérateurs temporels X, G, F et U permettant de représenter des enchaînements d'état :

- ✓ Xp (neXt p) : l'état suivant vérifie p.
- ✓ Gp (Global p) : tous les états suivants vérifient p.
- ✓ Fp (Future p) : inévitablement (fatalement) un état dans le futur vérifie p.
- ✓ p1 U p2 (Until) : tous les états suivants vérifient p1 jusqu'à un état vérifiant p2

ersité de Manouba
ationale des Sciences
e l'Informatique

Section : ..... A. U : ..... / .....

Module : .....

Classe : .....

Session : .....

Signature des Surveillants

Nom : ..... Prénom : .....

N° C.I.N. :

N° d'inscription

Signature de l'étudiant

..... Salle n° : ..... Place n° : .....

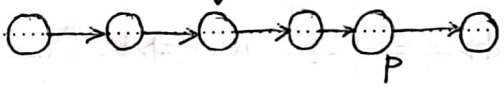
Note

Examen de : .....

Appréciations du correcteur

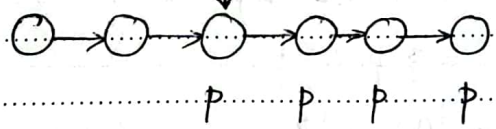
1. nécessairement p : $\Diamond p \equiv Fp$

instant courant



toujours p : $\Box p \equiv Gp$

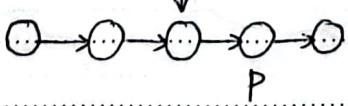
instant courant



A partir de l'instant courant. (p vérifié ds l'instant courant).

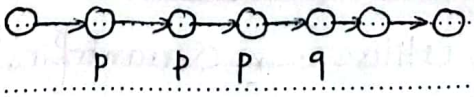
l'instant suivant, p vrai : $\bigcirc p \equiv Xp$:

instant courant



p jusqu'à q : p U q :

instant courant



⚠ Si l'instant courant vérifie q, p U q retourne vrai.

↝ les propositions atomiques sont des formules PLTL.

↝ Si p et q sont PLTL alors $p \wedge q$, $\neg p$, $p \mathcal{U} q$, $\bigcirc p$ sont PLTL.

opérateurs dérivés:

*) $p \vee q = \neg(\neg p \wedge \neg q)$

*) $p \Rightarrow q = \neg p \vee q$

*) $p \Leftrightarrow q = p \Rightarrow q \wedge q \Rightarrow p$

*) true $= \neg p \vee p$

*) false $= \neg$ true

$= \neg(\neg p \vee p)$

→ false $= p \wedge \neg p$

*) $\Diamond p =$ true $\mathcal{U} p$

*) $\Box p = \neg \Diamond \neg p$

CTL:

↳ temps arborescent: Chaque instant peut avoir plusieurs successeurs.

↳ on Utilise: *) Quantificateurs d'état (opér. temporelles)

• $\Diamond$, $\Box$, $\bigcirc$, $\mathcal{U}$ (m de PLTL)

*) Quantificateurs de chemins:

NE RIEN ECRIRE ICI

...rdit de signer la copie à la fin de la composition.

→ pour tout chemin : A (All) ≡ ∀

↳ tous les futurs chemins vérifient la prop

→ il existe un chemin future : E (EXIST) ≡ ∃

↳ il existe un futur chemin qui vérifie la prop.

Syntaxe : • toute proposition atomique est CTL

• f, g sont CTL ⟹ ¬f, f∧g, AXF, EXF, A(f U g), E(f U g) sont CTL.

*) $A \Diamond g = A(\text{true} \cup g)$

*) $E \Diamond g = E(\text{true} \cup g)$

*) $A \circ g = \neg E \circ \neg g$

*) $E \circ g = \neg A \circ \neg g$

*) $A \Box g = \neg E \Diamond \neg g = \neg E(\text{true} \cup \neg g)$

*) $E \Box g = \neg A(\text{true} \cup \neg g)$

ركز ! [illegible] ماتنساش !!!!

⚠ Soit la formule ★ (f où :

les chem [illegible] : ★ ∈ {A, E}

LTL [illegible] chemin : (∈ {◇, □, ○, U}

⚠ Dans CTL, chaque opérateur temporel doit être sous la portée d'un qualificateur de chemin.

càd : . AG EX : Correct

. AG X : Incorrect
?

PLTL VS CTL

. PLTL est linéaire.
↳ temps basé sur les chemins.
↳ formule PLTL = formule de chemins (séquence d'état).

. CTL : Arborescent
↳ Notion de A et E
↳ Dans PLTL, le All est implicite (Déjà 1 seul chemin) mais some (E) ne peut pas être exprimé.

. syntaxe CTL (formule d'état)
. $\phi := True \mid a \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \exists\varphi \mid A\varphi$

où : . a : prop. atomique.
. ϕ, ϕ_1, ϕ_2 : formule d'état
. φ : formule de chemin (LTL)

ersité de Manouba
ationale des Sciences
e l'Informatique

Section : .... A. U : .... /...................

Module : ....

Classe : ....

Session : ....

Signature des Surveillants

tal
uilles
remises

Nom : .... Prénom : ....

N° C.I.N. :

N° d'inscription

Signature de l'étudiant

.... Salle n° : .... Place n° : ....

Note

Examen de : ....

Appréciations du correcteur

otal
euilles
s remises

syntaxe C.T.L (formule de chemins)

F. de chemin ← $\varphi ::= O\,\phi \mid \phi_1 \; U \; \phi_2$

→ F. d'état.

⚠ بالك تغلط في هاذم ال :

× ∃ Formule d'état

× A Formule d'etat

× O Formule de chemin

Expression des prop temporelles :

× Sûreté : quelque chose de mauvais n'arrivera jamais.

Soit ϕ qui exprime la sûreté.

P.L.T.L : $G\,\phi$ → $G\,\neg\,(acc\_A \wedge acc\_B)$

exp : pas d'accès multiple à une section critique.

C.T.L : $AG\,\phi$ → $AG\,\neg\,(acc\_A \wedge Acc\_B)$

fe17701&c42004Osu

NE RIEN ECRIRE ICI

st interdit de signer la copie à la fin de la composition.

*) Fatalité : sous certaines cdt qque chose de bien finira par avoir lieu au moins 1 fois à partir d'un certain état.

PLTL : $G(p \rightarrow Fq) \equiv G(\text{dde acc} \rightarrow F \text{ accès})$

exp: Si A demande l'accès alors fatalement il l'aura.

CTL : $AG(p \rightarrow AFq) \equiv AG(\text{dde\_acc} \rightarrow AF \text{ accès})$

*) Atteignabilité : certaine situation peut être atteinte.

PLTL : Non exprimé

CTL : AGEF ϕ

*) Absence du blocage : il ne peut jamais se trouver dans une situation où il est impossible de progresser

. PLTL : non exprimable

. AGEX true :

*) Equité : sous certaines cdt, qque chose de bien aura lieu

PLTL : GFϕ

CTL : AGAFϕ

Structure de Krippke :

↳ Automate où les propositions qui étiquettent les états des automates jouent un rôle fondamental pour une logique basé sur les états (ex CTL).

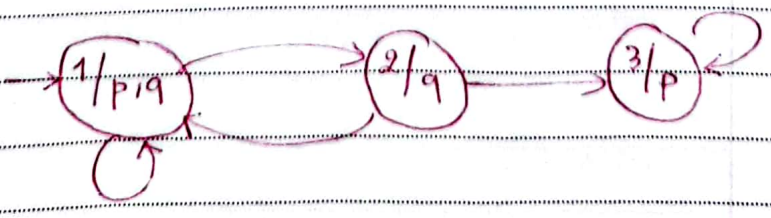
↳ les actions qui étiquètent les transitions sont moins importants.

↳ On associe à chaque noeud un {} fini de variables propositionnelles.

Soit $A = \{Q, T, q_0, l\}$ une Str. de Kripke :

- Q : ensemble d'états
- $T \subseteq Q \times Q$: {} de transitions
- q_0 : état initial
- l : étiquetage qui à chaque état $q \in Q$ associe l'{} $l(q)$ des prop. vérifiés par q

exp :



$Q = \{1, 2, 3\}$; $T = \{(1,1), (1,2), (2,1), (2,3), (3,3)\}$

$q_0 = 1$; $l(q_1) = \{p, q\}$; $l(q_2) = \{q, \neg p\}$, $l(q_3) = \{p, \neg q\}$.

NE RIEN ECRIRE ICI

erdit de signer la copie à la fin de la composition.

⚠ . $A \models \phi$: Modèle de Kripke satisfait ϕ

. on écrit $\sigma, i \models \phi$

c'est-à-dire : à l'instant i (l'état i) de l'exécution σ la formule ϕ est vérifié.