M2 Informatique
Année 2019-2020

Examen de Méthodes formelles et Vérification probabiliste

Éléments de corrections

Corrigé partiel et non-officiel,
à lire d'un œil critique

Exercice 1 :

Rappels de cours

Les éléments d'un **alphabet $2^{\{a,b\}}$** sont les sous-ensembles de l'ensemble de **propositions atomiques** {a, b}.
C'est-à-dire : ∅, {a}, {b} et {a,b}
Dans la suite, on a appellera ces éléments des **étiquettes.**
(le terme d'étiquette n'est peut-être pas le plus approprié, mais on ne les appellera pas des « lettres » pour éviter la confusion avec les propositions atomiques)

Exemple d'un mot de longueur 6 (6 étiquettes) sur cet alphabet : {a,b} {a,b} {a} ∅ {b} {a}

Remarque : Les étiquettes sont bien des sous-ensembles, donc évidemment :

- On ne peut pas prendre 2 fois la même proposition atomique dans une étiquette (pas de {a,a})
- L'ordre des propositions atomiques ne compte pas (écrire {a,b} ou {b,a} revient au même).

Attention : L'étiquette {a} n'est pas « incluse » dans l'étiquette {a,b}. On peut transposer ces étiquettes en logique propositionnelle pour s'en convaincre :
$\{a\} = a \land \neg b$
$\{a,b\} = a \land b$

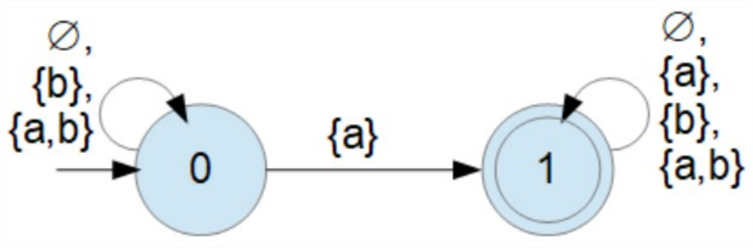
Rappels de cours

Un **automate de Büchi** fonctionne à peu près comme un automate fini, mais il lit des mots de longueurs infinies.
Les états entourés sont appelés **états répétés** (au lieu de état finaux ou terminaux comme dans les automates finis).
Un mot est reconnu par l'automate s'il passe une infinité de fois par l'état répété.

Voici quelques exemples sur l'alphabet défini précédemment :

Exemple 1 :

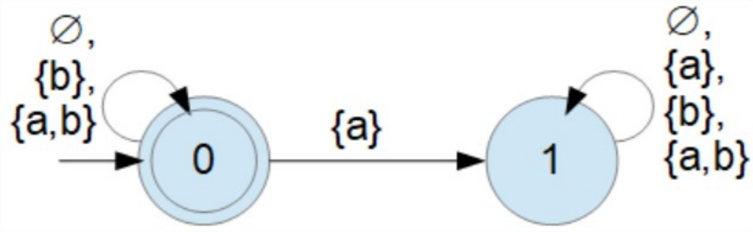
Cet automate reconnaît tous les mots qui contiennent **au moins une fois l'étiquette {a}**.
(les numéros sur les états sont évidemment arbitraires et optionnels)



Dès qu'on a trouvé un {a} : on va dans l'état répété (1) et on y reste.
Donc trouver un {a} conduit à une infinité de passages dans l'état répété.

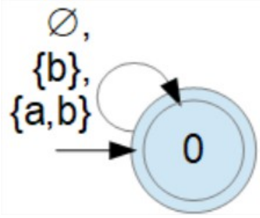
Exemple 2 :

Cet automate reconnaît tous les mots qui ne contiennent **jamais l'étiquette {a}**.



Dès qu'on a trouvé un {a}, on va dans l'état « poubelle » (c'est-à-dire non répété et dont on ne peut pas sortir) et on y reste.
Donc il faut ne jamais trouver de {a} pour rester infiniment dans l'état répété.

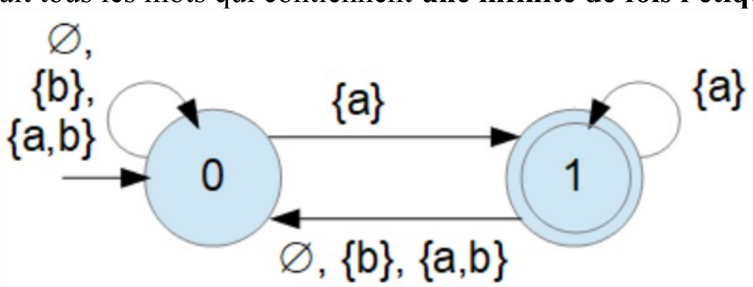
Variante :
On peut aussi ne pas écrire les états « poubelles » ni les transitions qui y conduisent.



Mais dans la suite on écrira tous les états et toutes les transitions : faire des automates complets évite parfois certaines erreurs.

Exemple 3 :

Cet automate reconnaît tous les mots qui contiennent **une infinité de fois l'étiquette {a}**.



On passe par l'état répété autant de fois qu'on trouve {a}.
Donc il faut trouver une infinité de {a} pour passer une infinité de fois par l'état répété.

Question 1

Méthode

La principale difficulté de cette question consiste à comprendre la formule qui décrit le langage.
$\{w \in (2^{PA})^\omega \mid \forall i \in \mathbb{N}. \exists j \in \mathbb{N}. j \geq i \text{ et } w(j) = \{p,q\}\}$

Prenons la formule morceau par morceau :

- $\{w \in (2^{PA})^\omega \mid \forall i \in \mathbb{N}. \exists j \in \mathbb{N}. j \geq i \text{ et } w(j) = \{p,q\}\}$

Nous cherchons les mots w de longueurs infinies (ω) composés d'étiquettes qui sont des sous-ensembles des propositions atomiques (2^{PA}).
Il existe donc les 8 étiquettes suivantes : ∅, {p}, {q}, {r}, {p,q}, {p,r}, {q,r}, {p,q,r}.
Et les mots du langage sont une succession infinie de ces étiquettes : $e_0 e_1 e_2 e_3 \dots$
(pour illustrer, je note « e » les étiquettes dont on ne connaît pas la forme et j'écris en indice leur position dans le mot w)

- $\{w \in (2^{PA})^\omega \mid \forall i \in \mathbb{N}. \exists j \in \mathbb{N}. j \geq i \text{ et } w(j) = \{p,q\}\}$

Pour tout entier i, il existe un j plus grand...
En terme de position dans le mot infini w, ça donne ça : $e_0 e_1 e_2 e_3 \dots e_i \dots e_j \dots$

- $\{w \in (2^{PA})^\omega \mid \forall i \in \mathbb{N}. \exists j \in \mathbb{N}. j \geq i \text{ et } w(j) = \{p,q\}\}$

Et l'étiquette à la place j est $\{p,q\}$.
$w = e_0 e_1 e_2 e_3 \dots e_i \dots \{p,q\}_j \dots$

Donc en résumé, où qu'on se trouve dans le mot, il reste forcément au moins une étiquettes {p,q} plus loin dans le mot.
Si on était sur un mot fini, cela reviendrait à dire « la dernière étiquette du mot est {p,q} ».
Mais ici, on est sur un mot infini, donc pas de dernière étiquette.
Sur un mot infini, cela revient à dire « **il y a une infinité d'étiquettes {p,q}** ».

Pour se convaincre qu'il y a une infinité d'étiquettes {p,q}
(passez ce long paragraphe si vous êtes déjà convaincus)

On peut imaginer qu'on part d'une étiquette à une place i quelconque.
Disons qu'on part de i=73.
$e_0 e_1 e_2 e_3 \dots e_{73} \dots$

La formule nous dit qu'on doit trouver, quelque part plus loin dans le mot une étiquette {p,q}.
Disons qu'on la trouve par exemple à la place 94.
$e_0 e_1 e_2 e_3 \dots e_{73} \dots \{p,q\}_{94} \dots$

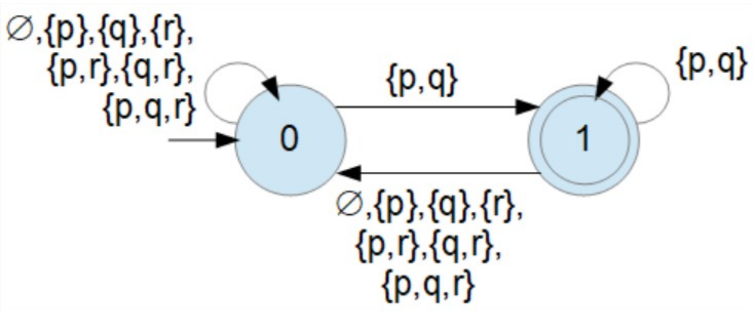
Regardons à présent l'étiquette suivante : la 95 (ou n'importe quelle étiquette après 94).
$e_0 e_1 e_2 e_3 \dots e_{73} \dots \{p,q\}_{94}\ e_{95} \dots$

Cette étiquette doit également respecter la règle d'avoir une étiquette {p,q} plus loin dans le mot (la règle est vraie « pour tout i », donc elle doit être vraie pour 95).
Disons qu'on la trouve par exemple la place 210.
$e_0 e_1 e_2 e_3 \dots e_{73} \dots \{p,q\}_{94}\ e_{95} \dots \{p,q\}_{210}$

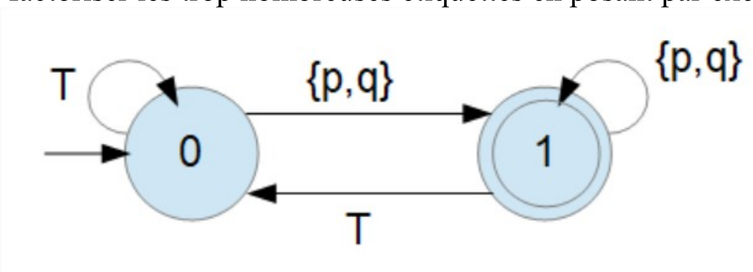
Mais alors il doit y avoir encore une étiquette {p,q} plus loin dans le mot, pour que l'étiquette 211 respecte la règle.
Et ainsi de suite...

En bref, chaque fois qu'on trouve une étiquette {p,q}, on en trouve forcément une autre plus loin dans le mot infini.
Il y a donc une infinité d'étiquette {p,q}.

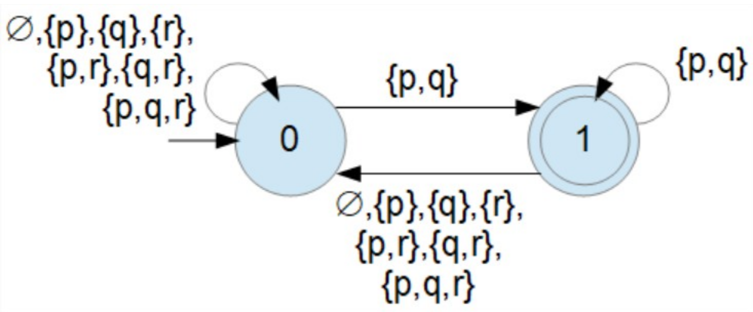
Or, on sait construire un automate de Büchi qui reconnaît les mots contenant une infinité de {p,q} (cf. l'exemple n°3 des rappels de cours ci-dessus) : seules les transitions {p,q} envoient dans l'état répété et les autres envoient dans l'état non répété.



On pouvait peut-être factoriser les trop nombreuses étiquettes en posant par exemple $T = 2^{PA} \setminus \{p,q\}$



Réponse



Question 2

Méthode

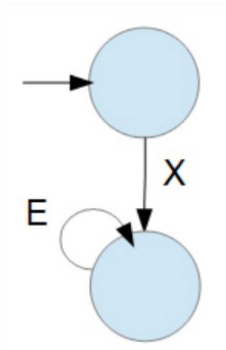
Cette fois, la contrainte est donnée par une formule LTL : $(Gp) \wedge (qUr)$
Traduction :

1) Toutes les étiquettes contiennent p
2) Un jour une étiquettes contiendra un r, et jusque-là elles devront contenir q (« q until r »)

Notons $E = 2^{AP} = \varnothing, \{p\}, \{q\}, \{r\}, \{p,q\}, \{p,r\}, \{q,r\}, \{p,q,r\}$
Notons X les étiquettes sans p : $X = \varnothing, \{q\}, \{r\}, \{q, r\}$
Notons Y les étiquettes avec p : $Y = \{p\}, \{p,q\}, \{p, r\}, \{p, q, r\}$

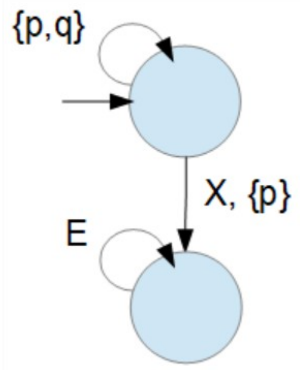
D'après la règle (1), tout mot où on trouve une étiquette sans p est éliminé.
Donc tous les états de cet automate devront porter une transition X directement vers un état « poubelle ».

Les premiers états auront donc cette forme :

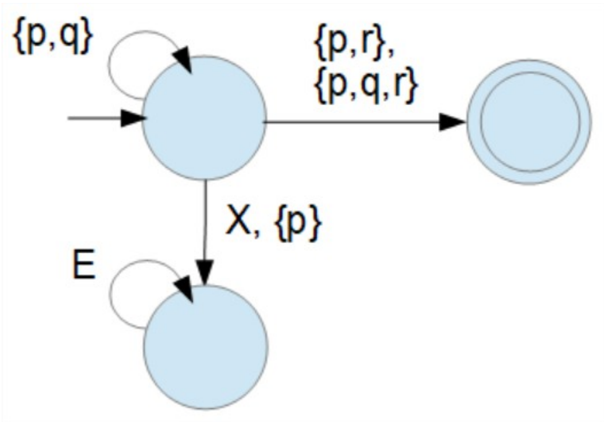


D'après la règle (2), si on trouve une étiquette sans q avant le premier r, le mot est aussi éliminé.
Il faut donc ajouter l'étiquette {p} à celles qui vont dans la poubelle tant qu'on a pas lu de r.

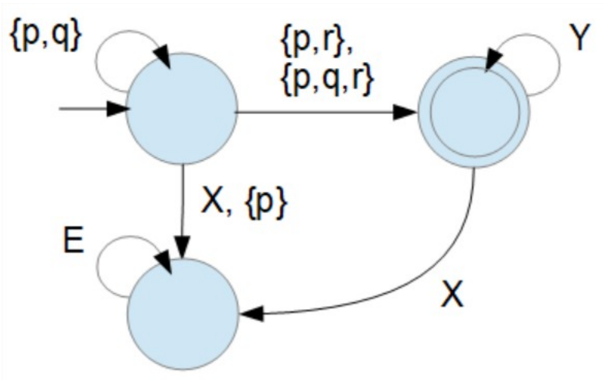
Tant qu'on ne n'a pas trouvé de r, on reste dans l'état de départ non-répété (avec {p,q}, la seule transition sans r qui ne soit pas déjà dirigée vers la « poubelle »).



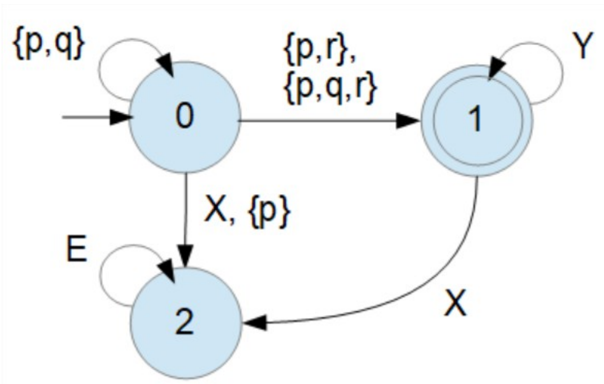
Mais lorsqu'on a trouvé un r, on peut accéder à l'état répété.



Et lorsqu'on a atteint l'état répété, on peut y rester tant qu'on lit des étiquettes contenant un p. Sinon, on est envoyé vers l'état « poubelle » comme expliqué plus haut.



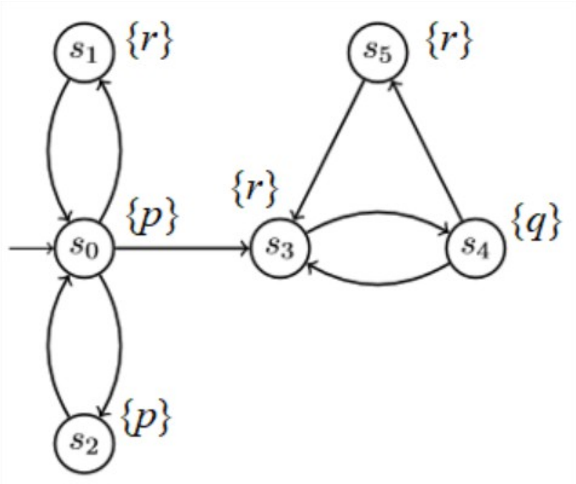
Réponse



E = 2^{AP} = ∅, {p}, {q}, {r}, {p,q}, {p,r}, {q,r}, {p,q,r}
X = les étiquettes sans p : X = ∅, {q}, {r}, {q, r}
Y = les étiquettes avec p : Y = {p}, {p,q}, {p, r}, {p, q, r}

Exercice 2 :

Réécrivons le système avec les étiquettes sur les états.



Question 1 : p **U** r

Traduction de la formule :
On aura r un jour, et jusque là on a toujours p.

Réponse
Faux
Il est possible de ne jamais avoir r si on boucle en S_0-S_2- S_0-S_2- S_0-S_2- …

Question 2 : $(\mathbf{G}p) \vee (\mathbf{F}r)$

Traduction de la formule :
On a soit toujours p, soit un jour r.

Réponse
Vrai
Soit on reste toujours bloqué en S_0 et S_2, et alors on a toujours p.
Soit on arrive à quitter ces états, ce qui amène forcément à passer par S_1 ou S_3, et alors on a r.

Question 3 : $(\mathbf{GF}q) \Rightarrow (\mathbf{GF}r)$

Traduction de la formule :
Si on a une infinité de q, alors on a une infinité de r aussi.

Réponse
Vrai
On ne peut trouver q que dans S_4.
Pour aller dans S_4 il faut avoir été en S_3 au tour précédent.
Or S_3 porte la lettre r.
Donc pour chaque q trouvé, on a trouvé au moins un r.
Donc si on trouve une infinité de q, on trouve aussi une infinité de r.

Exercice 3

Pour chaque question il y avait pleins de réponses possibles : plusieurs formules logiquement équivalentes et parfois plusieurs façons d'interpréter la phrase.

Question 1

Les portes de deux étages différents ne sont jamais ouvertes en même temps.

Donc, sur P0, P1 et P2, au moins 2 doivent être Faux.
Il y a plein de façons possibles de l'écrire, en voici 4 :

> « Si on prend 2 portes, il est faux que les 2 sont ouvertes »
> $G(\neg(P0 \wedge P1) \wedge \neg(P0 \wedge P2) \wedge \neg(P1 \wedge P2))$
>
> « Si on prend 2 portes, au moins l'une est fermée »
> $G((\neg P0 \vee \neg P1) \wedge (\neg P0 \vee \neg P2) \wedge (\neg P1 \vee \neg P2))$
>
> « Soit la porte 0 est ouverte et les autres sont fermées,
> soit la porte 1 est ouverte et les autres sont fermées,
> soit la porte 2 est ouverte et les autres sont fermées,
> soit les 3 portes sont fermées »
> $G((P0 \wedge \neg P1 \wedge \neg P2) \wedge (\neg P0 \wedge P1 \wedge \neg P2) \wedge (\neg P0 \wedge \neg P1 \wedge P2) \wedge (\neg P0 \wedge \neg P1 \wedge \neg P2))$
>
> « Si une porte est ouverte, alors les 2 autres sont fermées »
> $G((P0 \Rightarrow (\neg P1 \wedge \neg P2)) \wedge (P1 \Rightarrow (\neg P0 \wedge \neg P2)) \wedge (P2 \Rightarrow (\neg P0 \wedge \neg P1)))$

Question 2

A tout moment, si les portes d'un étage sont ouvertes, l'ascenseur se trouve à cet étage.

> En forme factorisée :
> $G(\forall i. \wedge Pi \Rightarrow Ai)$
>
> En forme développée :
> $G((P0 \Rightarrow A0) \wedge (P1 \Rightarrow A1) \wedge (P2 \Rightarrow A2))$

Question 3

A tout moment, si un bouton est appuyé, dans l'état suivant le voyant correspondant est allumé sauf si l'ascenseur est à l'étage correspondant au bouton appuyé.

La phrase est ambiguë, plusieurs interprétations possibles (pas équivalentes), en voici 2 :

> « Si le bouton i est appuyé et que l'ascenseur n'est pas à l'étage i, alors allumer le voyant i à l'étape suivante.
> Si le bouton i est appuyé et que l'ascenseur est déjà à l'étage i, on n'impose rien au voyant i (il fait ce qu'il veut) »
>
> En forme factorisée :
> $G(\forall i. \wedge (Bi \Rightarrow (XVi \vee Ai)))$
>
> En forme développée :
> $G((B0 \Rightarrow (XV0 \vee A0)) \wedge (B1 \Rightarrow (XV1 \vee A1)) \wedge (B1 \Rightarrow (XV1 \vee A1)))$

« Si le bouton i est appuyé et que l'ascenseur n'est pas à l'étage i, alors allumer le voyant i à l'étape suivante.
Si le bouton i est appuyé et que l'ascenseur est déjà à l'étage i, on impose au voyant i d'être éteint à l'étape suivante.»

En forme factorisée :
$G(\forall i.\wedge ((Bi \wedge \neg Ai) \Rightarrow XVi \;\wedge\; (Bi \wedge Ai) \Rightarrow X\neg Vi))$

En forme développée :
$G($
$((B0 \wedge \neg A0) \Rightarrow XV0 \wedge (B0 \wedge A0) \Rightarrow X\neg V0) \wedge$
$((B1 \wedge \neg A1) \Rightarrow XV1 \wedge (B1 \wedge A1) \Rightarrow X\neg V1) \wedge$
$((B2 \wedge \neg A2) \Rightarrow XV2 \wedge (B2 \wedge A2) \Rightarrow X\neg V2))$

Question 4

A tout moment, si un voyant correspondant à un étage est allumé, il reste allumé jusqu'à ce que l'ascenseur finisse par arriver à l'étage correspondant (et il finira par y arriver).

Encore une fois, plusieurs interprétations possible de la phrase.
Par exemple, est-ce que le voyant est obligé de s'éteindre lorsqu'on arrive ?

Si on suppose que le voyant n'est pas obligé de s'éteindre.
En forme factorisée :
$\forall i.\wedge (Vi \Rightarrow (Vi \;U\; Ai))$
En forme développée :
$G((V0 \Rightarrow (V0 \;U\; A0)) \wedge (V1 \Rightarrow (V1 \;U\; A1)) \wedge (V2 \Rightarrow (V2 \;U\; A2)))$

Si on suppose que le voyant est obligé de s'éteindre.
En forme factorisée :
$\forall i.\wedge (Vi \Rightarrow (Vi \;U\; (Ai \wedge \neg Vi)))$
En forme développée :
$G((V0 \Rightarrow (V0 \;U\; (A0 \wedge \neg V0))) \wedge (V1 \Rightarrow (V1 \;U\; (A1 \wedge \neg V1))) \wedge (V2 \Rightarrow (V2 \;U\; (A2 \wedge \neg V2))))$

Question 5

Si un utilisateur appuie infiniment souvent sur le bouton d'un étage, l'ascenseur sera infiniment souvent à cet étage.

Encore plusieurs interprétations possibles.
Par exemple, est-ce « être infiniment souvent à un étage » sous-entend qu'on a quitté cet étage entre 2 passages ? Ou est-ce qu'on peut simplement être resté à cet étage tout le temps ?
Prenons le second sens, bien plus simple à écrire en LTL.

En forme factorisée :
$\forall i.\wedge ((GF\; Bi) \Rightarrow GF\; Ai))$

En forme développée :
$((GF\; B0) \Rightarrow GF\; A0)) \wedge ((GF\; B1) \Rightarrow GF\; A1)) \wedge ((GF\; B2) \Rightarrow GF\; A2))$

Exercice 4

Question 1

Pr($S_0 \models FB_1$) = 1

Traduction de la formule : En partant de S_0 on a 100% de chances de passer un jour en S_9.

Faux
Depuis S_0, on a 20% de chance d'aller dans S_3, et alors on n'ira jamais en S_9 car il n'existe aucun chemin de S_3 vers S_9.
Depuis S_0, on a aussi 50% de chance d'aller dans S_1, et alors on n'ira jamais non plus en S_9 pour la même raison.
Et ils existe encore d'autres chemins partant de S_0 qui ne vont pas en S_9.
Donc, de façon triviale *Pr*($S_0 \models FB_1$) < 0,3

Question 2

Pr($S_0 \models FB_2$) = 1

Traduction de la formule : En partant de S_0 on a 100% de chances de passer un jour en S_4.

Faux
Car il existe un chemin non nul de S_0 vers S_9 et qu'une fois en S_9 on est bloqué, on ne peut plus aller en S_4.
On peut même calculer la probabilité du chemin le plus direct de S_0 à S_9 :
f(0,6) * f(6,7) * f(7, 8) * f(8, 9)
= 0.3 * 0.5 * 0.5 * 0.5 = 0.0375
Donc il y a au moins 3.75% de chances, en partant de S_0, d'aller se bloquer en S_9 sans passer par S_4.
Et ils existe encore d'autres chemins partant de S_0 qui ne vont pas en S_4.
Donc *Pr*($S_0 \models FB_2$) < 0,9625

Question 3

Pr($S_1 \models GFB_2$) = 1

Traduction de la formule : En partant de S_1 on a 100% de chances de passer une infinité de fois en S_4.

Vrai
Depuis S_1, on est sûr d'aller dans S_2.
A partir de S_2, on est bloqué dans le groupe de 4 états S_2, S_3, S_4 et S_5.
Dans ce groupe d'états, il est impossible de rester hors de S_4 plus de 3 tours consécutifs.
Donc on passe forcément une infinité de fois par S_4.
Donc *Pr*($S_1 \models GFB_2$) = 1 *cqfd*

Exercice 5

Méthode

On cherche la probabilité, pour chaque état S_i , d'atteindre un jour l'état S_7 .
C'est-à-dire Xi = *Pr*(S_i |= FS_7)

Commençons par les cas évidents :

X7 = 1
Car si on part de S_7 on est sûr d'arriver un jour dans S_7

X5 = 0
Car il n'existe aucun chemin ni de S_5 à S_7

X6 = 0
Car il n'existe aucun chemin ni de S_6 à S_7

Les autres chemins ne sont pas triviaux.
On pourrait croire que X4 = 0.5 en voyant la transition de S_4 à S_7 mais il existe d'autres chemins de S_4 à S_7 (par exemple en passant par S_2 puis S_3 et à nouveau par S_4). Donc X4>0.5.

Pour résoudre les 5 cas non-triviaux, il faut poser un système d'équations.

X0 = 0.5X1 + 0.5X3
Car S4 possède une transition 0.5 vers S7 et 0.5 vers S2
Et ainsi de suite pour les 4 autres :

X1 = 0.8X0 + 0.2X5
X2 = 0.7X0 + 0.3X3
X3 = 0.6X4 + 0.4X5
X4 = 0.5X7 + 0.5X2

On remplace les X5, X6 et X7 par leurs valeurs connues :
X0 = 0.5X1 + 0.5X3
X1 = 0.8X0
X2 = 0.7X0 + 0.3X3
X3 = 0.6X4
X4 = 0.5X2 + 0.5

Et on résout le système d'équations.
Note : On le résout ici le système à la main, mais il était sans doute autorisé de confier le traitement à un logiciel de calcul.

X0 = 0.5*(0.8X0) + 0.5X3
X0 = 0.4X0 + 0.5X3
0.6X0 = 0.5X3
X0 = 0.5X3/0.6
X0 = (5/6)X3

$X2 = 0.7X0 + 0.3X3$
$X2 = 0.7(5/6)X3 + 0.3X3$
$X2 = (7/12)X3 + (3/10)X3$
$X2 = (70+36/120)X3$
$X2 = (106/120)X3$
$X2 = (53/60)X3$

$X4 = 0.5X2 + 0.5$
$X4 = 0.5(53/60)X3 + 0.5$
$X4 = (53/120)X3 + 0.5$

$X3 = 0.6((53/120)X3 + 0.5)$
$X3 = ((53*6)/(120*10))X3 + 0.3$
$X3 = (53/200)X3 + 0.3$
$(147/200)X3 = 0.3$
$X3 = 0.3 * (200/147)$
$X3 = (3/10) * (200/147)$
$X3 = 600/1470$
$X3 = 60/147$
$\mathbf{X3 = 20/49}$

$X4 = (53/120)X3 + 0.5$
$X4 = (53/120)*(20/49) + 0.5$
$X4 = (1060/5880) + 0.5$
$X4 = (53/294) + (1/2)$
$X4 = 106/588 + 294/588$
$\mathbf{X4 = 100/147}$

$X2 = (53/60)X3$
$X2 = (53/60)*(20/49)$
$X2 = 1060/2940$
$\mathbf{X2 = 53/147}$

$X0 = (5/6)X3$
$X0 = (5/6)*(20/49)$
$X0 = 100/294$
$\mathbf{X0 = 50/147}$

$X1 = 0.8X0$
$X1 = (8/10)*(50/147)$
$X1 = 400/1470$
$\mathbf{X1 = 40/147}$

Astuce : Pour vérifier le résultat en fin de calcul, reprendre de système d'équations de départ, et remplacer les variables par les valeurs trouvées.

Si certaines égalités sont fausses, c'est qu'il y a une erreur de calcul quelque part.

Réponse

$\mathbf{X0 = 50/147}$
$\mathbf{X1 = 40/147}$
$\mathbf{X2 = 53/147}$
$\mathbf{X3 = 20/49}$
$\mathbf{X4 = 100/147}$
$\mathbf{X5 = 0}$
$\mathbf{X6 = 0}$
$\mathbf{X7 = 1}$

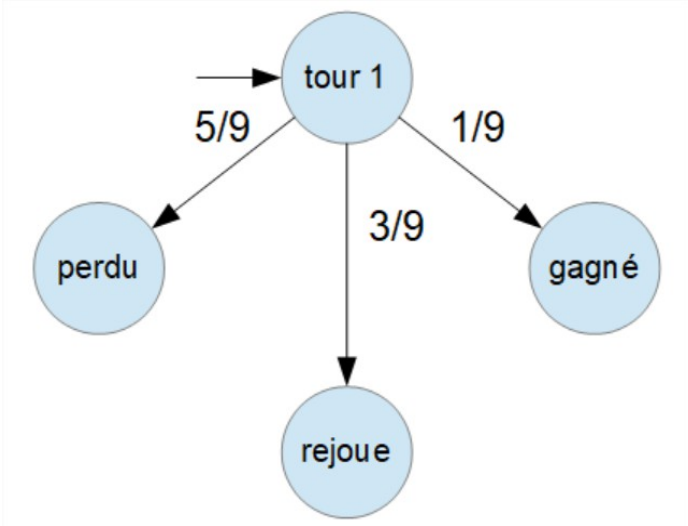
Exercice 6

Question 1

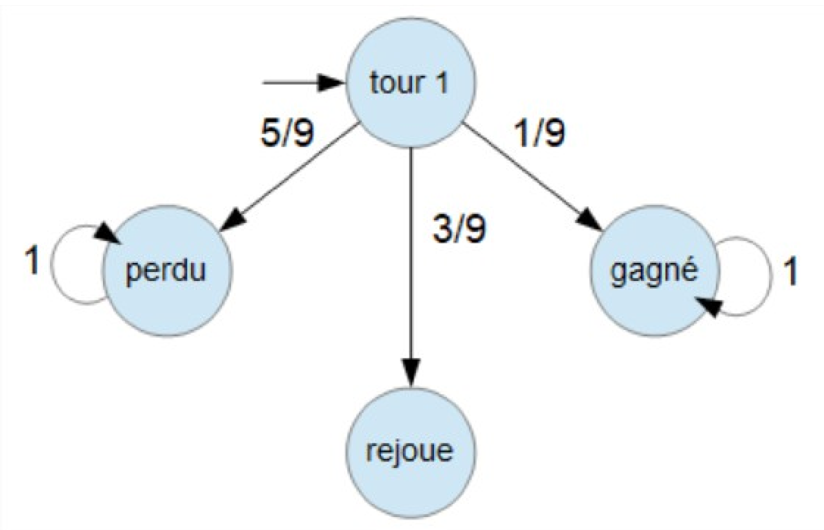
Méthode

Construisons la chaîne de Markov par étape.

Au 1er tour :
- 1/9 de gagner (123)
- 3/9 de rejouer (111, 222, 333)
- 5/9 de perdre (les autres tirages)

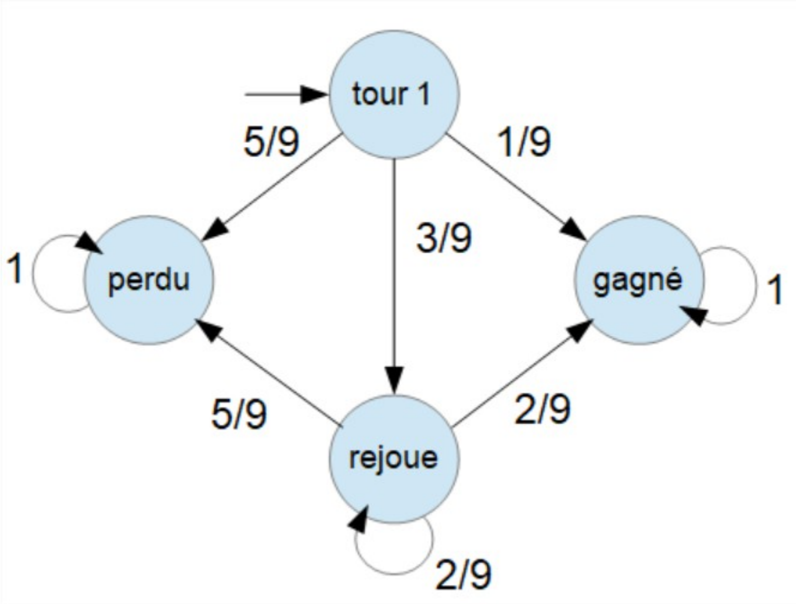


Si on a gagné ou perdu : on reste forcément dans gagné ou perdu (le jeu est terminé)



Si on rejoue, c'est qu'on a fait un triple au tour précédent, donc :
- 2/9 de gagner (123 ou le triple du tour précédent)
- 2/9 de rejouer (les deux autres triples possibles)
- 5/9 de perdre (les autres tirages)

Réponse



Question 2

Méthode

Résoudre le système d'équations comme à l'exercice 5 pour trouver la probabilité Xtour1.
$X_i = Pr(S_i \models \text{Fgagné})$

De façon triviale :
Xgagné = 1
Xperdu = 0

Pour les 2 autres états, moins triviaux, on pose le système d'équations :
Xtour1 = (1/9)Xgagné + (3/9)Xrejoue + (5/9)Xperdu
Xrejoue = (2/9)Xgagné + (2/9)Xrejoue + (5/9)Xperdu

En remplace les Xgagné et Xperdu par leurs valeurs connues :
Xtour1 = 1/9 + (3/9)Xrejoue
Xrejoue = 2/9 + (2/9)Xrejoue

Et on résout les équations :

Xrejoue = 2/9 + (2/9)Xrejoue
(7/9)Xrejoue = 2/9
7 * Xrejoue = 2
Xrejoue = 2/7

Xtour1 = 1/9 + (3/9)Xrejoue
Xtour1 = 1/9 + (1/3) * (2/7)
Xtour1 = 1/9 + 2/21
Xtour1 = (21+18)/(9*21)
Xtour1 = 39/189
Xtour1 = 13/63

Réponse
Si on choisit de jouer, on a 13 chances sur 63 de gagner un jour (soit environ 20,6%).

source : http://info.paris7.free.fr
Questions, commentaires, critiques, remarques, etc : phosphore85@gmail.com