Chapitre I

Espaces d'accueil

Introduction

Un état d'accueil d'un système est un état qu'il est toujours possible d'atteindre, quelle que soit l'évolution de ce système. Ce concept a été introduit par Keller[36] pour les systèmes de transitions, et il a proposé le concept de norme (inspiré de Floyd) comme outil de preuve. Une norme est une fonction à valeurs entières définie sur les états, qui vaut zéro sur l'état d'accueil et qu'il est toujours possible de faire décroître.

Dans BRAMS[11], on trouve la transposition de cette notion aux réseaux de Petri, et des exemples de normes qui sont des combinaisons linéaires des marquages des places.

La notion d'espace d'accueil est une généralisation de celle d'état d'accueil due à Memmi[42,43]: au lieu de pouvoir toujours atteindre un état fixé, on peut toujours atteindre un état appartenant à un ensemble fixé (c-à-d, un état vérifiant une certaine propriété). La vérification d'espace d'accueil joue un rôle essentiel dans l'analyse des réseaux de Petri car il s'agit de montrer qu'on peut toujours atteindre une certaine propriété: cette notion est utile dans la preuve de propriétés temporelles des systèmes.

Memmi avait donné une autre méthode de preuve que la norme: preuve par raffinements successifs qui consiste en des réductions successives d'un espace contenant tous les marquages accessibles pour arriver à l'espace donné. Dans sa thèse, Johnen[35] a étudié la décidabilité et la vérification automatique des espaces d'accueil (utilisant des techniques de réécriture), et a proposé un algorithme qui est une formalisation et une automatisation de cette méthode. Cet algorithme prend en entrée l'espace global G (contenant tous les marquages accessibles) défini par des équations linéaires des marquages (égalités et inégalités) et l'espace E

supposé être espace d'accueil: puis il vérifie par raffinements successifs que E est accessible à partir de G.

Nous visons à munir les espaces d'accueil de méthodes de preuve compositionnelles. Nous proposons un nouveau concept de norme qui réunit ces deux méthodes: nous conservons la notion de norme qui est une fonction sur les marquages, mais en plus, ces normes peuvent représenter le passage d'un ensemble d'états à un autre et donc un pas de la preuve par raffinements successifs: une norme qui prouve l'existence de l'espace d'accueil est la composition de ces normes.

Ainsi ces normes sont munies d'opérateurs de composition qui permettent de les construire par raffinements successifs, et en plus, de construire la norme d'une composition de réseaux en composant leurs normes (dans certaines conditions).

Dans la première section, la définition d'un espace d'accueil est rappelée, et nous donnons une caractérisation de cette propriété en termes d'ordre bien fondé.

Dans la deuxième section, nous définissons un nouveau concept de norme, avec un cas particulier: les normes linéaires. Ces normes sont des applications de l'ensemble des marquages d'un réseau vers N^k, associées à des relations d'accessibilité.

La troisième section présente les opérations de composition de normes. La première est l'ordonnancement de normes, qui correspond à la preuve d'espace d'accueil par réductions successives d'un espace global. La deuxième opération est la somme de norme, qui permet de montrer que l'intersection de deux espaces d'accueil en est un, si une certaine condition "d'indépendance" est vérifiée.

La quatrième section est consacrée à la vérification hiérarchique des normes. Nous définissons la preuve d'une norme et la composition de ces preuves. Une méthode de réutilisation de preuve dans la vérification de normes est illustrée par des exemples au moyen de ces notions.

Nous définissons aussi une notion d'espace d'accueil plus précise: un A-espace d'accueil est un espace d'accueil accessible sans franchir des transitions dans A. Ceci peut s'exprimer par une propriété des preuves d'une norme associée à cet espace.

I-1 Ordre bien fondé sur les états

Les espaces d'accueil sont un des concepts de base pour l'expression et la preuve des propriétés temporelles des réseaux de Petri. Souvent la preuve de l'absence de blocage consiste à montrer qu'il existe un espace d'accueil E tel que pour tout marquage de E, il existe une séquence franchissable.

D'autre part, les espaces d'accueil sont utilisables dans la preuve de certaines relations synchroniques. Si on veut prouver que les occurrences de deux transitions a et b forment un langage de parenthèses dont le niveau d'imbrication est borné par n, il suffit d'ajouter une place p entre a et b, de montrer que p est implicite et bornée par n, puis que $E = \{M; M(p) = 0\}$ est un espace d'accueil.

Nous rappelons d'abord la définition d'un espace d'accueil, puis nous donnons une caractérisation de cette propriété en fonction de l'existence d'un ordre bien fondé sur les états accessibles.

Définition I-1 (Espace d'accueil) *Soit $\Sigma = (P, T; W; M_0)$ un système P/T. Un ensemble de marquages $H \subseteq \mathbf{N}^P$ est un* espace d'accueil *de Σ ssi*

$$\forall M \in R(\Sigma), \exists \sigma \in T^*, \exists M' \in H, M \xrightarrow{\sigma} M' \in H$$

Si $\{M\}$ est un espace d'accueil alors M est appelé état d'accueil.

La preuve de la propriété d'espace d'accueil, que ce soit au moyen d'une norme ou par raffinements successifs d'espaces, repose sur la notion d'ordre bien fondé. Un ordre sur un ensemble E est bien fondé s'il n'existe pas dans E de suite infinie strictement décroissante.

Définition I-2 (Ordre bien fondé) *Un ordre $\leq$ sur un ensemble E est dit bien fondé, s'il n'existe pas $(a_i)_{i \in \mathbf{N}} \in E^{\mathbf{N}}$ tel que $a_0 > a_1 > \cdots a_i > a_{i+1} > \cdots$*

Théorème I-1 *H est un espace d'accueil de Σ si, et seulement si, il existe un ordre (partiel) bien fondé $\leq$ sur $R(\Sigma)$, tel que $H \cap R(\Sigma)$ contienne l'ensemble des éléments minimaux de $R(\Sigma)$, et si $M \in R(\Sigma)$ n'est pas minimal, alors il existe $\sigma \in T^*$, $M \xrightarrow{\sigma} M'$ et $M' < M$.*

Preuve

-) Si H est un espace d'accueil, on définit $<$ par $M < Q$ ssi $M \in H$, $Q \notin H$ et $\exists \sigma \in T^*, Q \xrightarrow{\sigma} M$.

-) La réciproque est prouvée au moyen du principe de l'induction nœthérienne, qui s'énonce ainsi: si E est un ensemble muni d'un ordre bien fondé $\leq$, et si $A \subseteq E$ alors

$$\forall x \, [(\forall y < x, y \in A) \Rightarrow x \in A] \Rightarrow A = E$$

On suppose donc qu'il existe un ordre bien fondé $\leq$ sur $R(\Sigma)$ vérifiant les hypothèses énoncées dans le théorème. On considère

$$A = \{M \in R(\Sigma); \exists \sigma, M \xrightarrow{\sigma} M' \in H\}$$

Pour $M \in R(\Sigma)$, on note

$$B(M) = \{m \in R(\Sigma); m < M\}$$

Il faut montrer que $B(M) \subseteq A \Rightarrow M \in A$ pour en déduire $A = R(\Sigma)$ et par conséquent H espace d'accueil.

Si $M \in H$, alors $B(M) = \emptyset \subseteq A$ et $M \in A$ (on prend $\sigma = \lambda$).

Si $M \notin H$ et $B(M) \subseteq A$. Par hypothèse (du théorème), il existe σ, $M \xrightarrow{\sigma} m$ et $m < M$, c-à-d $m \in B(M)$. Par hypothèse d'induction, il existe σ' telle que $m \xrightarrow{\sigma'} m' \in H$, et donc $M \xrightarrow{\sigma''} m'$ où $\sigma'' = \sigma\sigma'$. D'où, $M \in A$. □

Quand on prouve un espace d'accueil par raffinements successifs, on part d'un espace global E_0 (contenant l'ensemble d'accessibilité), et on montre qu'il existe une suite d'espaces $(E_i)_{i=0,n}$ tels qu'on puisse atteindre E_{i+1} à partir de E_i, $E_{i+1} \subseteq E_i$ et $E_n = H$. L'ordre sous-jacent ici, est $M' < M$ ssi il existe $i < j$ tels que $M' \in E_j$ et $M \in E_i$.

Une norme classique est une application de l'ensemble des états accessibles vers $\mathbf{N}$, et donc transporte l'ordre de $\mathbf{N}$ sur ces états. Sa preuve part aussi d'un espace global et se fait par disjonction de cas (qui correspond à une partition de cet espace), et on montre que dans chaque cas il est possible d'atteindre un état de norme inférieure.

I-2 Normes

Dans tous les cas, un pas de preuve d'espace d'accueil consiste à montrer qu'il existe une séquence menant d'un ensemble d'états à un autre ensemble d'états d'ordre strictement inférieur. Le concept de norme que nous définissons représente ce pas de preuve, et répond au souci d'avoir un outil maniable de preuve qui se prête à la composition. Notons que la norme est définie pour un réseau non marqué, et que c'est uniquement une relation d'accessibilité.

Pour ordonner les états, nous considérons des normes qui sont des applications à valeurs dans $\mathbf{N}^k$ muni de l'ordre lexicographique. Le choix de cet ordre est justifié par la définition des normes linéaires et les compositions de normes définies dans la suite.

Définition I-3 (Norme) *Soit $N = (P, T; W)$ un réseau de Petri, J et K deux sous-ensembles de $\mathbf{N}^P$ tels que $J \supseteq K$. Une (J, K)-norme sur N est une fonction $\nu : \mathbf{N}^P \to \mathbf{N}^k$ $(k > 0)$ telle que*

- $\forall m \in J, \nu(m) = 0 \Leftrightarrow m \in K$

- *si* $m \in J \wedge \nu(m) > 0$ *(ordre lexicographique), alors*

$$\exists m' \in J, \exists \sigma \in T^*, m \xrightarrow{\sigma} m' \wedge \nu(m') < \nu(m)$$

J est appelé le domaine de ν et K son noyau. L'ensemble des (J,K)-normes sur N est noté $\mathcal{N}(N,J,K)$; N est omis quand le contexte le permet.

Une norme est censée représenter la preuve en entier ou seulement un pas de preuve (qui est la concaténation de tous les pas). Pour que ce soit une preuve d'espace d'accueil, il faut que son domaine contienne l'ensemble d'accessibilité du réseau marqué considéré.

Corollaire I-1 *Si ν est une (J,K)-norme telle que $J \supseteq R(N;M_0)$, alors K est un espace d'accueil de $(N;M_0)$.*

Preuve On considère l'ordre défini sur $R(\Sigma)$ par $M < M'$ si $\nu(M) < \nu(M')$ et on applique le théorème I-1. □

La généralisation des normes qui sont des combinaisons linéaires des marquages de places, donne des vecteurs de marquages de places. L'intérêt est de ne plus avoir de coefficients à gérer mais un ordre, ce qui facilite les choses lors de la composition: insérer une place dans un ordre est plus simple que translater les coefficients ou trouver un coefficient intermédiaire.

Définition I-4 (Norme linéaire) *Une norme ν est dite linéaire s'il existe $\{p_1,\ldots,p_k\} \subseteq P$, tel que $\nu(m) = (m(p_1),\ldots,m(p_k))$. On note $\nu = (p_1,\ldots,p_k)$.*

Remarquons que si $\nu = (p_1,\ldots,p_k)$ est une (J,K)-norme linéaire telle que J contienne l'ensemble d'accessibilité, l'ensemble des marquages où $M(p_1) = \cdots = M(p_k) = 0$ est un espace d'accueil.

La notion de norme linéaire est une des raisons du choix de l'ordre lexicographique sur N^k, comme le montre l'exemple suivant.

Le réseau de la figure I-1 modélise le problème des lecteurs-écrivains avec priorité alternée. La place LA représente les processus en attente de lecture, EA ceux en attente d'écriture. Les places LX et EX représentent les processus respectivement en cours de lecture et en cours d'écriture. Quand PE est marquée, la priorité est aux écrivains, et quand PL est marquée, elle est aux lecteurs.

La transition *rl* est la demande de lecture, *dl* le début de lecture et *fl* la fin de lecture; les événements analogues pour l'écriture sont *re*, *de* et *fe*. *fp* est l'événement qui met fin à la priorité aux lecteurs. *tl* fait passer des lecteurs de l'état d'attente à l'état d'exécution, quand la priorité est aux lecteurs.

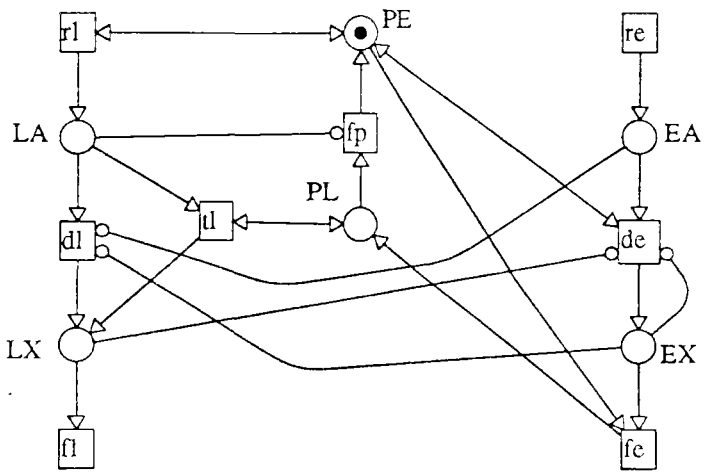

Figure I-1: Lecteurs-écrivains avec priorité alternée

Initialement, seule PE est marquée. Un écrivain en attente ne peut passer en exécution (de) que si la priorité est aux écrivains et qu'il n'y a pas de lecteurs ou d'écrivains en exécution. Quand un écrivain termine, la priorité passe aux lecteurs. S'il n'y a pas de lecteurs en attente, la priorité repasse aux écrivains. Un lecteur en attente ne peut commencer l'exécution que si la priorité est aux lecteurs, ou que la priorité est aux écrivains et qu'il n'y a pas d'écrivains en attente ou en exécution.

Nous allons montrer au moyen de la norme linéaire $\nu = (LA, EA, EX, PL, LX)$ que l'état initial est un état d'accueil. Les invariants du réseau sont les suivants:

$$M(PE) + M(PL) = 1 \quad \text{(I.1)}$$

$$M(EX) \leq 1 \quad \text{(I.2)}$$

$$M(EX) = 1 \Rightarrow M(PE) = 1 \quad \text{(I.3)}$$

L'invariant I.1 signifie que la priorité est soit aux écrivains, soit aux lecteurs; l'invariant I.2 exprime qu'il y a au plus un écrivain en exécution; l'invariant I.3 dit que, quand il y a un écrivain en exécution, alors la priorité est aux écrivains. Le premier invariant est linéaire et déduit du flot $PE+PL$, les deux autres se montrent par induction. Notons E l'ensemble des marquages vérifiant ces invariants (et donc qui contient tous les marquages accessibles). Nous allons montrer que ν est une $(E, \{M_0\})$-norme.

- $\nu(M) = 0 \Leftrightarrow M(LA) = M(EA) = M(EX) = M(PL) = M(LX) = 0 \Leftrightarrow M = M_0$, car $M(PL) = 0 \Rightarrow M(PE) = 1$ d'après l'invariant I.1.

- Si $\nu(M) > 0$, alors il existe $p \in \{LA, EA, EX, PL, LX\}$ telle que $M(p) > 0$. On distingue donc cinq cas, en supposant à chaque fois que les places de poids inférieur sont vides:

  1. Si $M(LX) > 0$, on franchit fl.
  2. Si $M(PL) > 0$ et $M(LX) = 0$: si $M(LA) = 0$, on franchit fp, sinon on franchit tl. Le dernier cas diminue le marquage de LA et augmente celui de LX, mais comme on adopte l'ordre lexicographique ν diminue.
  3. Si $M(EX) > 0$ et $M(PL) = M(LX) = 0$, on franchit fe.
  4. Si $M(EA) > 0$ et $M(EX) = M(PL) = M(LX) = 0$, on franchit de.
  5. Si $M(LA) > 0$ et $M(EA) = M(EX) = M(PL) = M(LX) = 0$, on franchit dl.

I-3 Composition de normes

L'intérêt de définir des compositions de norme est double:

- Pour un système donné $(N; M_0)$, décomposer hiérarchiquement la vérification d'un espace d'accueil E en plusieurs "sous-vérifications," au moyen d'un ensemble de normes $(\nu_i)_{i=1,n}$ qui, composées d'une certaine façon, donnent une norme associée à E.

- Pour un système $(N; M_0)$, lui-même construit hiérarchiquement par composition d'un ensemble de sous-systèmes $(N_i; M_{0i})_{i=1,n}$ ayant chacun une norme ν_i, construire une norme ν sur $(N; M_0)$ par composition des $(\nu_i)_{i=1,n}$.

Dans cette section, nous définissons deux opérations de compositions: l'ordonnancement et la somme de deux normes. La section suivante présente une méthode d'utilisation illustrée d'exemples.

La première opération de composition de norme correspond à la preuve par raffinements successifs ou par disjonction de cas. On a une norme ν_1 qui prouve qu'on peut aller de J_0 vers J_1, et une norme ν_2 qui prouve qu'on peut aller de J_1 vers J_2: on construit une norme ν qui prouve qu'on peut aller de J_0 vers J_2. Cette opération justifie le choix de l'ordre lexicographique sur $\mathbf{N}^k$ (cf. la preuve).

Proposition I-1 (Ordonnancement de normes) *Si $\nu_i \in \mathcal{N}(N, J_{i-1}, J_i)$ pour $i = 1, 2$ sont deux normes telles que $\nu_i : \mathbf{N}^P \to \mathbf{N}^{k_i}$, alors la fonction $\nu : \mathbf{N}^P \to \mathbf{N}^{k_1+k_2}$ définie par*

$$\nu(m) = (\nu_1(m), \nu_2(m))$$

est une (J_0, J_2)-norme sur N. On note $\nu = (\nu_1, \nu_2)$.

Preuve Il faut vérifier les conditions de la définition d'une norme.
D'abord $J_0 \supseteq J_1 \supseteq J_2$ et pour tout $m \in J_0$, $\nu(m) = 0$ ssi $\nu_1(m) = 0$ et $\nu_2(m) = 0$, c-à-d $m \in J_1 \cap J_2 = J_2$.

Il reste à prouver qu'on peut faire décroître ν si $\nu(m) > 0$. Si $m \in J_0$ et $\nu(m) > 0$, on distingue deux cas:

1. $\nu_1(m) > 0$: comme ν_1 est une (J_0, J_1)-norme, il existe $m' \in J_0$, tel que $m \xrightarrow{\sigma} m'$ et $\nu_1(m') < \nu_1(m)$. On en déduit $\nu(m') < \nu(m)$, puisque $<$ est l'ordre lexicographique (peu importe la relation de $\nu_2(m)$ et $\nu_2(m')$).

2. $\nu_1(m) = 0$ et $\nu_2(m) > 0$. $\nu_1(m) = 0$ entraîne $m \in J_1$. ν_2 étant une (J_1, J_2)-norme, il existe $m' \in J_1$, $m \xrightarrow{\sigma} m'$ et $\nu_2(m') < \nu_2(m)$. Comme $m' \in J_1$, $\nu_1(m') = 0$ et donc $\nu(m') < \nu(m)$.

□

La deuxième opération de composition est une somme de normes et correspond par rapport à la combinaison de marquages de places à donner le même coefficient à deux places: on veut composer deux normes sans les ordonner. Cette opération ne peut se faire que pour des normes indépendantes, c-à-d telles que la diminution de l'une n'augmente pas l'autre.

Définition I-5 (Normes indépendantes) *Deux normes ν_1 et ν_2 de même domaine J sont dites indépendantes si pour tout $\{i, j\} = \{1, 2\}$ on a*

$$\begin{array}{c} m \in J \wedge \nu_i(m) > 0 \\ \Downarrow \\ \exists m' \in J, \exists \sigma, [(m \xrightarrow{\sigma} m') \wedge (\nu_i(m') < \nu_i(m)) \wedge (\nu_j(m') \leq \nu_j(m))] \end{array}$$

Proposition I-2 (Somme de normes) *Si deux normes $\nu_i \in \mathcal{N}(N, J, K_i)$ sont indépendantes, alors $\nu = \nu_1 + \nu_2$ est une $(J, K_1 \cap K_2)$-norme. La somme sur $\bigcup_{k \in \mathbf{N}} \mathbf{N}^k$ est définie par (si $k \geq k'$)*

$$(a_1, \ldots, a_k) + (b_1, \ldots, b_{k'}) = (a_1, \ldots, a_{k-k'}, a_{k-k'+1} + b_1, \ldots, a_k + b_{k'})$$

Preuve Si $m \in J$, $\nu(m) = 0 \Leftrightarrow (\nu_1(m) = 0 \wedge \nu_2(m) = 0) \Leftrightarrow m \in K_1 \cap K_2$.

Si $\nu(m) > 0$ pour $m \in J$, il existe i tel que $\nu_i(m) > 0$. Alors il existe $m' \in J$, tel que $m \xrightarrow{\sigma} m'$, $\nu_i(m') < \nu_i(m)$, et $\nu_j(m') \leq \nu_j(m)$.

On en déduit $\nu(m') < \nu(m)$. □

Quand $J \supseteq R(\Sigma)$, alors K_1 et K_2 sont des espaces d'accueil; si en plus, la somme des deux normes est définie, $K_1 \cap K_2$ est aussi un espace d'accueil. Donc une condition suffisante pour que l'intersection de deux espaces d'accueil soit un espace d'accueil, est que la somme de leurs normes associées existe.

Ainsi cette opération fournit une méthode de vérification que l'intersection de deux espaces d'accueil en est un. (Rappelons que la propriété d'espace d'accueil est stable par réunion mais non par intersection.)

I-4 Vérification de normes

Dans [23] et [12], nous avons présenté une étude de cas de conception descendante de protocole, accompagnée d'une preuve descendante d'espace d'accueil. L'objectif de cette étude de cas était d'illustrer une méthode de *réutilisation de preuve* dans la conception progressive de systèmes.

La réutilisation de preuve, dans la conception hiérarchique, signifie qu'on tente de prouver des propriétés du système de niveau n en s'appuyant sur les preuves des sous-systèmes de niveau $n-1$.

Dans le cas des normes, le problème est le suivant: on a deux systèmes (N_i, M_{0i}) ayant chacun une norme ν_i; on obtient $(N; M_0)$ par composition de $(N_1; M_{01})$ et $(N_2; M_{02})$, et on voudrait savoir s'il existe une norme ν sur $(N; M_0)$ qui soit la composition de ν_1 et ν_2, ou de ν_1' et ν_2' qui sont obtenues par transformation des ν_i.

Plutôt que de poser des restrictions sur la nature de la composition des réseaux et des normes pour avoir cette propriété de "conservation", l'idée est alors d'associer à chaque norme un objet représentant sa preuve, et tester si cette preuve est encore applicable après la composition, et tester si la composition de normes est valide. Si oui, il faut que les preuves soient composables pour continuer ce processus.

Dans cette section, nous donnons un sens précis à une preuve de norme, et nous montrons que la preuve d'une composition de ν_1 et ν_2 s'obtient par une certaine combinaison de leurs preuves. La méthode d'utilisation de ces notions est illustrée par des exemples.

Nous définissons aussi une notion d'espace d'accueil plus précise, A-espace d'accueil, qui donne des informations sur une preuve possible de la propriété d'espace d'accueil. Cette notion apparaîtra dans les chapitres suivants sur le remplacement de sous-réseaux et la composition de réseaux.

I-4.1 Preuve de norme

On a vu que, fondamentalement, une norme est un ordre sur les éléments de J tel qu'il existe une séquence de n'importe quel élément vers un élément de rang strictement inférieur. Nous représentons alors la preuve d'une norme en regroupant les éléments admettant la même séquence qui fait décroître la norme.

Ainsi une preuve est un ensemble de couples (E, σ), où E est un sous-ensemble de J, et σ une séquence franchissable en tout marquage de E menant à un élément de rang strictement inférieur.

Définition I-6 (Preuve d'une norme) *Une preuve d'une (J,K)-norme ν est un ensemble inclus dans $(\mathcal{B}(J) \times T^*)$, noté V tel que*

- $\{E; \exists \sigma, (E, \sigma) \in V\}$ *est une partition de* $J \setminus K$
- *si* $(E, \sigma) \in V$ *alors* $\forall m \in E, \exists m' \in J, m \xrightarrow{\sigma} m' \wedge \nu(m') < \nu(m)$

L'ensemble des preuves de ν est noté $PR(\nu)$.

Une preuve de la norme ν de l'exemple des lecteurs-écrivains (figure I-1) est (pour abréger les notations, l'ensemble $\{M; \mathcal{P}(M)\}$ sera noté $\mathcal{P}(M)$):

$$\left\{ \begin{array}{l} (M(LX) > 0, fl), \\ (M(PL) > 0 \wedge M(LX) = M(LA) = 0, fp), \\ (M(PL) > 0 \wedge M(LX) = 0 \wedge M(LA) > 0, tl), \\ (M(EX) > 0 \wedge M(PL) = M(LX) = 0, fe), \\ (M(EA) > 0 \wedge M(EX) = M(PL) = M(LX) = 0, de), \\ (M(LA) > 0 \wedge M(EA) = M(EX) = M(PL) = M(LX) = 0, dl) \end{array} \right\}$$

I-4.2 Composition de preuves

Il est possible de construire une preuve de (ν_1, ν_2) et de $\nu_1 + \nu_2$ par une certaine combinaison de leurs preuves V_1 et V_2. En plus, il est possible, sur les preuves de ν_1 et ν_2, de tester une condition suffisante de l'indépendance de ν_1 et ν_2, et donc de l'existence de $\nu_1 + \nu_2$.

Dans le cas de l'ordonnancement de deux normes, une preuve de la composition est obtenue en prenant la réunion des deux preuves.

Proposition I-3 (Preuve de (ν_1, ν_2)) *Si $(\nu_i)_{i=1,2}$ sont deux normes telles que $\nu = (\nu_1, \nu_2)$ soit définie, alors*

$$\forall i \in \{1,2\}, V_i \in PR(\nu_i) \Rightarrow V = (V_1 \cup V_2) \subseteq PR(\nu)$$

Preuve On note $d(X) = \{E; \exists\sigma, (E,\sigma) \in X\}$. On suppose que ν_i est une (J_{i-1}, J_i)-norme. Puisque $d(V_i)$ est une partition de $J_{i-1} \setminus J_i$, et $J_0 \supseteq J_1 \supseteq J_2$, $d(V_1) \cup d(V_2)$ est une partition de $(J_0 \setminus J_1) \cup (J_1 \setminus J_2) = J_0 \setminus J_2$.

Il reste à montrer que si $(E,\sigma) \in V$, alors pour tout $m \in E$, $m \xrightarrow{\sigma} m'$ et $\nu(m') < \nu(m)$.

Si $(E,\sigma) \in V_1$, alors $m \xrightarrow{\sigma} m'$ tel que $\nu_1(m') < \nu_1(m)$ et donc $\nu(m') < \nu(m)$.

Si $(E,\sigma) \in V_2$, alors $m \xrightarrow{\sigma} m'$ tel que $\nu_1(m) = \nu_1(m') = 0$ et $\nu_2(m') < \nu_2(m)$: d'où $\nu(m') < \nu(m)$. □

La somme de deux normes n'est définie que si elles sont indépendantes. Une condition suffisante d'indépendance peut être testée sur des preuves de ν_1 et ν_2, et alors une preuve de $\nu = \nu_1 + \nu_2$ est obtenue à partir de celles de ν_1 et de ν_2.

Proposition I-4 (Preuve de $\nu_1 + \nu_2$) *Soit ν_1 et ν_2 deux normes telles que $\nu_i \in \mathcal{N}(N, J, K_i)$, et $V_i \in PR(\nu_i)$.*

Si pour tout $i \neq j$, $\forall (E,\sigma) \in V_i$, $\forall m \in E$, $m \xrightarrow{\sigma} m'$ tel que $\nu_j(m') \leq \nu_i(m)$ alors ν_1 et ν_2 sont indépendantes.

De plus, $V_i \cup \{(E \cap K_i, \sigma); (E,\sigma) \in V_j\} \in PR(\nu_1 + \nu_2)$.

Preuve Puisque $J \setminus K_i = \{m \in J; \nu_i(m) > 0\}$, et l'ensemble des E tels que $(E,\sigma) \in V_i$ est une partition de $J \setminus K_i$, l'indépendance de ν_1 et ν_2 découle immédiatement de la définition.

Prouvons, par exemple, que $V = V_1 \cup \{(E \cap K_1, \sigma); (E,\sigma) \in V_2\} \in PR(\nu_1 + \nu_2)$. $\{E; \exists\sigma, (E,\sigma) \in V_1\}$ est une partiton de $J \setminus K_1$ et $\{(E \cap K_1); (E,\sigma) \in V_2\}$ est une partition de $(J \setminus K_2) \cap K_1 = K_1 \setminus K_2$: donc $\{E; (E,\sigma) \in V\}$ est une partition de $(J \setminus K_1) \cup (K_1 \setminus K_2) = J \setminus (K_1 \cap K_2)$.

On vérifie facilement que si $(E,\sigma) \in V$, alors pour tout $m \in E$, $m \xrightarrow{\sigma} m'$ avec $\nu(m') < \nu(m)$, où $\nu = \nu_1 + \nu_2$. □

Exemples

Dans les exemples suivants, P_i est l'ensemble des places du réseau N_i, et $P = P_1 \cup P_2$.

Dans la figure I-2, $\nu_1 = (B,C)$ est une (J_1, K_1)-norme linéaire de N_1 où

$$J_1 = \mathbf{N}^{P_1} \bigwedge K_1 = \{M \in \mathbf{N}^{P_1}; M(B) = M(C) = 0\}$$

Une preuve V_1 de cette norme est

$$V_1 = \{(E_{11}, t_2), (E_{21}, t_3)\}$$

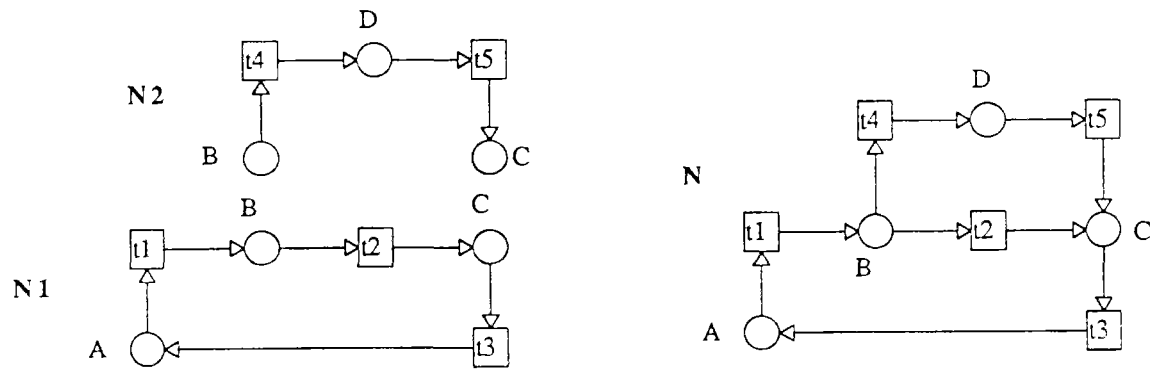

Figure I-2: Ordonnancement de normes associé à la composition de réseaux

où

$$E_{11} = \{M \in \mathbf{N}^{P_1}; M(B) > 0 \wedge M(C) = 0\} \bigwedge E_{21} = \{M \in \mathbf{N}^{P_1}; M(C) > 0\}$$

$\nu_2 = (D)$ est une (J_2, K_2)-norme de N_2 où

$$J_2 = \mathbf{N}^{P_2} \bigwedge K_2 = \{M \in \mathbf{N}^{P_2}; M(D) = 0\}$$

Une preuve V_2 de cette norme est

$$V_2 = \{(E_{12}, t_5)\}$$

où

$$E_{12} = \{M \in \mathbf{N}^{P_2}; M(D) > 0\}$$

On compose N_1 et N_2 par fusion de places et on obtient le réseau N. Dans N_1, on a construit une norme ν_1 et sa preuve montrant qu'il est possible de vider les places B et C. Dans N_2, on a procédé de même avec la norme ν_2 pour montrer qu'on peut vider D.

La question est alors de savoir s'il existe des transformations des preuves de ν_1 et ν_2 pour obtenir une norme ν' sur N avec sa preuve montrant qu'on peut vider les places B, C et D. Nous n'avons pas encore une réponse générale à ce problème, mais nous allons montrer que c'est possible dans cet exemple.

Nous montrons qu'il est d'abord possible de vider D en réutilisant ν_2 puis de vider B et C en réutilisant ν_1.

D'abord, on cherche une transformation de la preuve V_2 pour obtenir une norme sur N associée au vidage de la place D. Il est facile de vérifier que V_2' définie par

$$V_2' = \{(E, \sigma); \exists (G, \sigma) \in V_2 \wedge E = G\uparrow^P\}$$

est une preuve de la norme $\nu_2' : \mathbf{N}^P \to \mathbf{N}$ définie par $\nu_2'(M) = \nu_2(M{\downarrow_{P_2}})$ (il suffit de vérifier que les séquences restent franchissables et diminuent la norme). C'est alors une (J_2', K_2')-norme sur N où $J_2' = J_2{\uparrow^P}$ et $K_2' = K_2{\uparrow^P}$.

Maintenant, nous transformons V_1 en supposant que D est vide: on ne se contente pas d'étendre les marquages de V_1 à P, mais on prend leur intersection avec

$$F = \{M \in \mathbf{N}^P; M(D) = 0\} = K_2'$$

Ce qui donne

$$V_1' = \{(E, \sigma); \exists (G, \sigma) \in V_1 \wedge E = G{\uparrow^P} \cap F\}$$

On vérifie alors que c'est une preuve de $\nu_1' : \mathbf{N}^P \to \mathbf{N}$ définie par $\nu_1'(M) = \nu_1(M{\downarrow_{P_1}})$, qui est une (J_1', K_1')-norme sur N où $J_1' = J_1{\uparrow^P} \cap F$ et $K_1' = K_1{\uparrow^P} \cap F$.

Finalement, on a $K_2' = J_1'$, et donc, $\nu' = (\nu_2', \nu_1')$ est définie, et une de ces preuves est obtenue par $V' = V_1' \cup V_2'$.

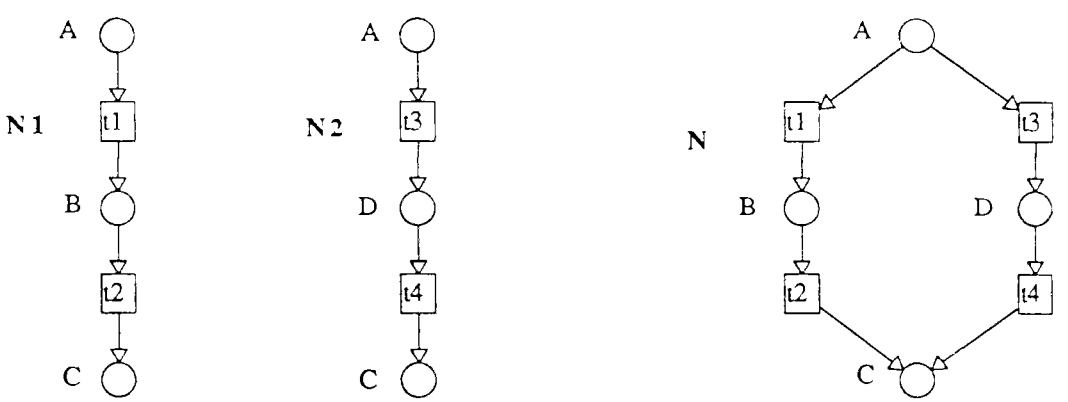

Figure I-3: Somme de normes associée à la composition de normes

Le deuxième exemple (figure I-3) illustre l'utilisation de la somme de normes. $\nu_1 = (A, B)$ est une (J_1, K_1)-norme sur N_1, où

$$J_1 = \mathbf{N}^{P_1} \bigwedge K_1 = \{M \in \mathbf{N}^{P_1}; M(A) = M(B) = 0\}$$

Une preuve de cette norme est

$$V_1 = \{(E_{11}, t_1), (E_{21}, t_2)\}$$

où

$$E_{11} = \{M \in \mathbf{N}^{P_1}; M(A) > 0 \wedge M(B) = 0\} \bigwedge E_{21} = \{M \in \mathbf{N}^{P_1}; M(B) > 0\}$$

$\nu_2 = (A, D)$ est une (J_2, K_2)-norme sur N_2, où

$$J_2 = \mathbf{N}^{P_2} \bigwedge K_2 = \{M \in \mathbf{N}^{P_2}; M(A) = M(D) = 0\}$$

Une preuve de cette norme est

$$V_2 = \{(E_{12}, t_3), (E_{22}, t_4)\}$$

où

$$E_{12} = \{M \in \mathbf{N}^{P_2}; M(A) > 0 \wedge M(D) = 0\} \bigwedge E_{22} = \{M \in \mathbf{N}^{P_2}; M(D) > 0\}$$

La composition par fusion de places de N_1 et N_2 donne le réseau N. Là aussi on voit aisément que

$$V_i' = \{(E, \sigma); \exists (G, \sigma) \in V_i \wedge E = G\uparrow^P\}$$

est une preuve de la norme $\nu_i' : \mathbf{N}^P$ définie par $\nu_i'(M) = \nu_i(M\downarrow_{P_i})$ appartenant à $\mathcal{N}(N, J_i', K_i')$, où $J_i' = J_i\uparrow^P$ et $K_i' = K_i\uparrow^P$. $J_1' = J_2'$ et la condition d'indépendance peut être testée et vérifiée sur V_1' et V_2': donc $\nu' = \nu_1' + \nu_2'$ est une (J', K')-norme sur N, avec $J' = J_1' = J_2' = \mathbf{N}^P$ et

$$K' = K_1' \cap K_2' = \{M \in \mathbf{N}^P; M(A) = M(B) = M(D) = 0\}$$

Une preuve de ν' est construite à partir de V_1' et V_2' comme indiqué dans la proposition I-4.

I-4.3 A-espace d'accueil

Quand un réseau admet un espace d'accueil, il est assez indifférent de savoir comment on l'atteint tant qu'on s'intéresse aux propriétés du réseau isolé. Mais si on compose le réseau avec un environnement ou si on le raffine, on souhaite savoir ce qui est conservé de cette propriété d'accueil, et alors il est utile de connaître l'influence de certaines places ou certaines transitions sur la preuve.

Nous définissons la notion de A-espace d'accueil qui précise qu'il est possible de se restreindre à des transitions de A pour atteindre cet espace, et par conséquent la propriété d'accueil est indépendante du marquage des places adjacentes à $T \setminus A$.

Ce n'est pas une nouvelle notion d'espace d'accueil mais une indication sur une preuve possible d'un espace d'accueil. Elle sera souvent utilisée dans les chapitres suivants.

Définition I-7 (*A*-espace d'accueil) *H est un A-espace d'accueil de $(N; M_0)$ où $A \subseteq T$ ssi c'est un espace d'accueil accessible en franchissant uniquement des transitions de A, i.e.,*

$$\forall M \in R(N; M_0), \exists w \in A^*, M \xrightarrow{w} M' \in H$$

Noter la place de l'adverbe "uniquement:" ...accessible en franchissant uniquement..., et non pas ...uniquement accessible en franchissant... Autrement dit, un espace d'accueil est un A-espace d'accueil, *s'il existe* une preuve de norme associée à cet espace ne contenant que des séquences dans A^*. Ceci est exprimé par la notion de (J, A, K)-norme.

Définition I-8 *Une (J, A, K)-norme, où $A \subseteq T$, est une (J, K)-norme telle qu'il existe $V \subseteq PR(\nu)$, et $\forall (E, \sigma) \in V$, $\sigma \in A^*$.*

Conclusion

Nous avons défini des normes, munies d'opérations de composition, qui sont des nouveaux outils de vérification modulaire et hiérarchique des espaces d'accueil. Nous avons associé aux normes des objets représentant leurs preuves, telles que, la preuve de la composition de deux normes soit obtenue par combinaison de leurs preuves respectives.

L'objectif à long terme de ce travail est de formaliser la méthode de réutilisation de preuve esquissée et illustrée par des exemples dans la quatrième section: nous avons montré qu'il était possible d'obtenir une norme d'un réseau construit par composition de deux réseaux ayant chacun une norme ν_i, en transformant leurs preuves et en les composant.

Ceci devrait déboucher sur une mise en œuvre d'une méthode de "verification assistée" d'espace d'accueil: un système expert serait capable d'enregistrer les preuves (ce qui suppose qu'on sache les représenter en machine), et lors d'une transformation de modèles, de proposer une transformation de preuve et de vérifier sa validité dans le nouveau modèle (il pourraitt aussi se faire indiquer la transformation par l'utilisateur). Ces représentations devraient être étendues aux réseaux colorés paramétrés pour une plus grande applicabilité.