NEW COLOURED REDUCTIONS FOR SOFTWARE VALIDATION

Sami Evangelista [*] **Serge Haddad** [**]
Jean-François Pradat-Peyre [*]

[*] *CEDRIC-CNAM Paris 292, rue St Martin, 75003 Paris*
[**] *LAMSADE-CNRS UMR 7024 Université Paris 9*
Place de Lattre de Tassigny 75775 Paris Cedex 16

Abstract: Structural model abstraction is a powerful technique for reducing the complexity of a state based enumeration analysis. We present in this paper accurate reductions for high-level Petri nets based on new ordinary Petri nets reductions. These reductions involve only structural and algebraical conditions. They preserve the liveness of the net and any LTL formula that does not observe the reduced transitions of the net. The mixed use of structural and algebraical conditions significantly enlarges their application area. Furthermore the specification of the transformation is parametric with respect to the cardinalities of coloured domains.

Keywords: Software Validation, Reductions, High-level Petri nets

1. INTRODUCTION

The use of formal methods in software design may be decomposed in two steps: a modelling stage which must lead to a model as close as possible to the analysed software and a verification stage involving properties expression and model checking via adequate algorithms.

Two kinds of verification techniques can be used. The state enumeration based methods lead to a complete verification but the analysis is restricted by the combinatory explosion factor. The structural methods are generally efficient but they do not ensure the complete correctness of the modelled system.

Thus an attractive trade-off would be to first perform structural abstractions in order to obtain a simplified model on which an enumeration based method can more easily be applied. The model may be abstracted in two ways: data abstraction and operation abstraction. Here we will focus on the latter one which merges consecutive instructions into a virtual atomic one. Such a transformation drastically reduces the combinatory explosion due to the elimination of the intermediate states. In the context of (high-level) Petri nets this abstraction is called a net reduction. A reduction is characterised by some application conditions, a transformation rule and the properties for which the initial and the reduced models are equivalent. In order to obtain reductions with a broad range of applications while preserving a large set of properties, we base our coloured reductions on new efficient ordinary Petri nets reductions (see Haddad and Pradat-Peyre (2004)) and we use the following approach to extend them to coloured models. We characterise some properties of the coloured functions labelling an arc which ensure that the unfolding of this arc will be appropriate for the conditions involved in ordinary reductions. We exhibit coloured flows which lead to the satisfaction of the algebraic conditions of ordinary reductions. We show how the use of composition, inverse and transpose of mappings enables us to handle the transformation of the labelling of arcs in the reduced net. Given a subclass of the Well-formed nets, Chiola et al. (1990), we specify reductions at a syntactic level in order to efficiently check the conditions and apply the transformations. We will not describe this part which can be found in Evangelista et al. (2004). Compared to previous works concerning high-level nets reductions, Colom et al. (1986), Genrich (1991), Haddad (1991), our new coloured reductions lie on accurate application conditions (since they are based on efficient ordinary Petri nets reductions) and then permit to reduce more realistic models. Moreover, this analysis does not need to fix a value for the parameters of the model (which is not the case for methods that reduce the reachability graph) and can be followed by any other analysis method.

The paper is organised as follows. In the next section, we recall the basics of coloured Petri nets with a focus on the coloured functions. In the third section, we first demonstrate that existing reductions do not cover typical patterns of concurrent programming. Then we show how the analysis of coloured functions and coloured invariants helps to accurately characterise behavioural conditions on the net. At last, we formally develop the post-agglomeration. In the fourth section, an example illustrates the power of these new reductions. The appendix includes additional definitions.

2. DEFINITIONS AND NOTATIONS

Coloured Petri nets handle tokens that are typed (or coloured) upon non empty finite sets called colour domains; a marking is then a multi-set over a colour domain and we denote $Bag(C)$ the set of multi-sets over C (the related definitions can be found in the appendix).

Definition *2.1.* A coloured net is a 5-tuple $CN = \langle P, T, \mathcal{C}, W^+, W^- \rangle$ with:

- P a non empty and finite set of places;
- T a non empty and finite set of transitions (disjoint of P);
- $\mathcal{C}$ is the colour mapping from $P \bigcup T$ to ω where ω is a set of finite and non empty sets. An item of $\mathcal{C}(s)$ is called a colour of s and $\mathcal{C}(s)$ denotes the colour domain of s.
- W^+ (resp. W^-) is the post (resp. pre) incidence mapping that associates to each place p and each transition t a colour mapping form $\mathcal{C}(t)$ to $Bag(\mathcal{C}(p))$. We note $W = W^+ - W^-$.

We note $\epsilon = \{\bullet\}$ the domain reduced to the single value $\bullet$ (the neutral token); so, ordinary Petri nets can be viewed as particular coloured Petri nets (the unique and common colour domain is ϵ).

Definition *2.2.* A marking is a mapping that associates to each place p a value in $Bag(\mathcal{C}(p))$. We note m_0 the initial marking of a net. A transition t is fireable for an instance $c_t \in \mathcal{C}(t)$ from a marking m (denoted by $m[t, c_t\rangle$) if

$$\forall p \in P, m(p) \geq W^-(p,t)(c_t)$$

The firing of t, c_t from m leads to the marking m' ($m[t, c_t\rangle m'$) defined by $\forall p \in P, m'(p) = m(p) + W(p,t)(c_t)$. A marking m' is reachable from a marking m if there exists a sequence $t_1, c_1, \ldots, t_k, c_k$ such that $m[t_1, c_1\rangle m_1$, $m_1[t_2, c_2\rangle m_2$, $\ldots$, $m_{k-1}[t_k, c_k\rangle m'$. We denote by $Reach(CN, m_0)$ the set of all reachable markings from m_0. As usual, an infinite sequence is a firing sequence iff all its finite prefixes are firing sequences.

To each coloured net corresponds a unique Petri net which is called the *underlying* Petri net. This net is composed by the set of places, $p[c_p]$ where $p \in P$ and $c_p \in \mathcal{C}(p)$ and the set of transitions $t[c_t]$, $t \in T$, $c_t \in \mathcal{C}(t)$. The pre and the post conditions are defined by the instantiation of colour function. This unfolded net is defined in the appendix.

We now introduce the coloured flows and invariants. These invariants can be used to characterise specific behaviours like, for instance, mutual exclusion. In order to obtain a sound definition of flows, we extend by linearity a function from C to $Bag(D)$ to a function from $Bag(C)$ to $Bag(D)$.

Definition *2.3.* A flow $\mathcal{F}$, on a domain $\mathcal{C}(\mathcal{F})$, is a vector over P, noted as the formal sum $\mathcal{F} = \sum_{p \in P} \lambda_p . \mathcal{F}_p . p$, where $\forall p \in P$, $\lambda_p \in \mathbb{Z}$ and $\mathcal{F}_p$ a mapping from $Bag(\mathcal{C}(p))$ to $Bag(\mathcal{C}(\mathcal{F}))$ such that: $\forall t \in T, \sum_{p \in P} \lambda_p . \mathcal{F}_p \circ W(p,t) = 0$ [1].
$\mathcal{F}$ induces the invariant:
$\forall m \in Reach(CN, m_0)$,
$\sum_{p \in P} \lambda_p . \mathcal{F}_p(m(p)) = \sum_{p \in P} \lambda_p . \mathcal{F}_p(m_0(p))$
An invariant $\mathcal{F}$ is **positive** if $\forall p \in P$, $\lambda_p \geq 0$. It is **binary** if $\forall c \in \mathcal{C}(\mathcal{F})$, $\sum_{p \in P} \lambda_p . \mathcal{F}_p(m_0(p))(c) = 1$. It is a **synchronisation** invariant if $\forall c \in \mathcal{C}(\mathcal{F})$, $\sum_{p \in P} \lambda_p . \mathcal{F}_p(m_0(p))(c) = 0$.

When no confusion is possible (i.e. the initial marking is given), we will not distinguish the flow and its corresponding invariant. We want to analyse the structure of the underlying Petri net using the structure and the functions of the coloured Petri net. This requires to characterise and manipulate coloured functions. The following definition and notations are enough for our purposes.

Definition *2.4.* Let f be a mapping from $Bag(C)$ to $Bag(C')$.

[1] 0 denotes here the null mapping from $\mathcal{C}(t)$ to $Bag(\mathcal{C}(\mathcal{F}))$

- ${}^t(f)$ is the mapping defined from $Bag(C')$ to $Bag(C)$ by ${}^t(f)(c')(c) = f(c)(c')$
- $\overline{f}$ is defined from $\mathcal{P}(C)$ to $\mathcal{P}(C')$ by $\overline{f}(D) = \{c' \in C' \mid \exists d \in D, f(d)(c') \neq 0\}$ where $\mathcal{P}(C)$ denotes the power set of C. Note that the linearity is preserved by this transformation (substituting $\cup$ to $+$) and that $\overline{f}$ may be viewed as a function from C to $\mathcal{P}(C')$.

DEFINITION *2.5.* Let f and g be two linear mappings from $\mathcal{P}(C)$ to $\mathcal{P}(C')$. We note $f \sqsubseteq g$ if $\forall c \in Bag(C), f(c) \subseteq g(c)$.

Below we list particular mappings. An **orthonormal** mapping is a colour domain permutation, a **unitary** mapping produces at most one token per colour, a **projection** is a canonic mapping from $Bag(C \times D)$ to $Bag(C)$, an **ortho-projection** is the composition of an orthonormal mapping with a projection. f is a **quasi-one to one** mapping if $\forall c \neq d$ $\overline{f}(c) \cap \overline{f}(d) = \emptyset$. f is a **quasi-onto** mapping from $Bag(C)$ to $Bag(D)$ if $\overline{f}(C) = D$. The complete definitions are given in the appendix.

3. COLOURED AGGLOMERATIONS

We suppose in the sequel that the set of transitions of the net is partitioned as : $T = T_0 \uplus H \uplus F$. The underlying idea of this decomposition is that the couple (H, F) defines transitions sets that are causally dependent : an occurrence of $f \in F$ in a firing sequence may always be related to a previous occurrence of some $h \in H$ in this sequence.

We have extended two kinds of agglomerations: the pre and the post agglomeration. Informally stated, in the **pre-agglomeration** scheme, firing a transition $h \in H$ is only useful for firing any transition of $f \in F$. Thus in the reduced net, the firings of h are postponed until the corresponding firing of f. In the **post-agglomeration** scheme, the firing of any transition $f \in F$ is mainly conditioned by the firing of the transitions of H. Thus, in the reduced net, one fires f immediately after the firing of some $h \in H$.

3.1 An introducing example

In the following coloured net (see Fig.1), the transition h models the update of a variable modelled by the place $V1$: the value X is replaced by the value $G1(X)$ where $G1$ models a mapping from C to C. Initially, this variable has the value $x0$. Similarly, the transition f models the update of a second variable modelled by the place $V2$. Generally, this model does not have the same behaviour as the one of the model depicted in Fig.2 where the two updates are performed simultaneously.

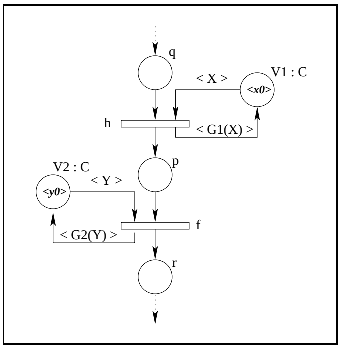

Fig. 1. Updating variables sequentially

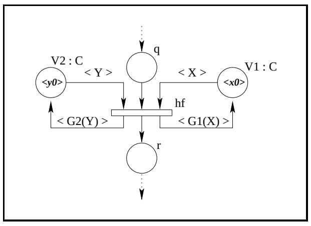

Fig. 2. Updating variables atomically

However, there exist many cases for which these two models are equivalent. In particular, as soon as we can prove that either the value of $V1$ does not change when q or p are marked or the value of $V2$ does not change when p is marked, the two models share a large set of properties.

Indeed let us suppose that, in the first model, the value of $V1$ does not change when q is marked. The variable $V1$ cannot be modified when p is marked. So, we can delay the update of the variable $V1$ until we are ready to perform the update of the variable $V2$ without modifying the properties of the model. This corresponds to the scheme of the pre-agglomeration: h can be delayed until f is fireable. In the second case, updating $V2$ after having waited in state p or updating $V2$ just after having updated $V1$ is equivalent since value of $V2$ cannot change when p is marked. This corresponds to the scheme of the post-agglomeration: f is fireable as soon as h is fired.

Nevertheless, whereas these behaviours correspond to the scheme of the pre or of the post agglomeration, none of the previously defined reductions cover such behaviours. The present work is based on reductions for ordinary Petri nets that we proposed in Haddad and Pradat-Peyre (2004). Such reductions cover a large range of patterns by introducing algebraical conditions whereas the previously defined ones solely lie on structural conditions. However the extension of the conditions and the transformation of these reductions to high-level nets require careful analysis of the coloured functions labelling the arcs of the net. Due to the lack of space, we focus in this paper on the post-agglomeration; complete results can be found in Evangelista et al. (2004).

3.2 Exploiting coloured functions and invariants

The structure of a coloured net does not necessarily reflect the structure of the underlying Petri net since we have to take into account colour mappings. Especially, we need to follow colour transformation using composition or transposition of colour mappings. Let us consider the following coloured Petri net and suppose that, given a colour $c_f \in \mathcal{C}(f)$, we want to compute the colours $\{c_h \in \mathcal{C}(h)\}$ such that the firing of h for a colour c_h may help the firing of f for the instance c_f (by producing useful tokens in place p). We have to start from c_f and to find the instances of p that are linked to $f[c_f]$. By definition, this set is $\overline{\Phi}(c_f)$. Then we have to find instances of h that are linked to a place $p[c_p]$, $c_p \in \overline{\Phi}(c_f)$. These instances are the set $\{c_h \in \mathcal{C}(h), \overline{\Psi}(c_h) \cap \overline{\Phi}(c_f) \neq \emptyset\}$. By definition of the transposition of a function, this set is $\overline{{}^t\Psi}(\overline{\Phi}(c_f))$. Thus, the set of colours we look for is $(\overline{{}^t\Psi} \circ \overline{\Phi})(c_f)$. In an opposite way, the set of instances of f that are causally dependent of an instance c_h of h, are $(\overline{\Psi} \circ \overline{{}^t\Phi})(c_h)$.

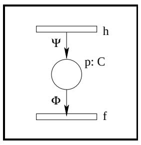

Fig. 3. Colour mapping manipulation illustration

Let us consider now the following coloured Petri net where p is an ordinary place (see Fig.4).

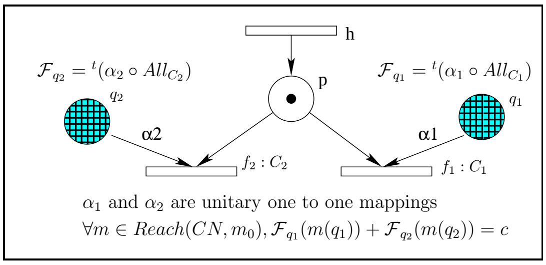
h
$\mathcal{F}_{q_2} = {}^t(\alpha_2 \circ All_{C_2})$
q_2
p
$\mathcal{F}_{q_1} = {}^t(\alpha_1 \circ All_{C_1})$
q_1
α2
α1
$f_2 : C_2$
$f_1 : C_1$
α_1 and α_2 are unitary one to one mappings
$\forall m \in Reach(CN, m_0), \mathcal{F}_{q_1}(m(q_1)) + \mathcal{F}_{q_2}(m(q_2)) = c$

Fig. 4. An invariant controlling f_1 and f_2

Let us prove that there is always an instance of f_1 or of f_2 that is fireable when p is marked.

- The interpretation of the invariant $\mathcal{F}$ is the following one: there is at least one token either in the place q_1 or in q_2 whose colour is either in the set $\overline{\alpha_1}(\overline{All_{C_1}(\bullet)})$ or in $\overline{\alpha_2}(\overline{All_{C_2}(\bullet)})$.
- Since ${}^t\alpha_{i\ (i=1,2)}$ is an unitary quasi-one to one mapping, each firing instance (f_i, c_i) requires, when $\alpha_i(c_i) \neq 0$, in addition to the token in p, exactly a token in the place q_i which colour is in the singleton $\overline{\alpha_i(c_i)}$.
- Combining these two facts, an instance (f_i, c_i) for some i is always fireable when p is marked.

Remark that this reasoning is still valid if we only require that $\forall i$, $\overline{\mathcal{F}_{q_i}} \sqsubseteq {}^t(\overline{\alpha_i} \circ \overline{All_{C_i}})$.

3.3 Post-agglomeration hypotheses

We present the four conditions of the post-agglomeration: the **potentially post-agglomerability**, the **HF-interchangeability**, the **F-independence** and the **F-continuation**.

The **potentially post-agglomerability** ensures that in any fireable sequence the number of occurrences of H is greater or equal than the number of occurrences of F.

DEFINITION *3.1.* (Hypothesis R1). A coloured net is potentially post-agglomerable (p-post-agglomerable) if $\exists\ H \subset T$, $F \subset T$, $p \in P$ such that

1. ${}^\bullet p = H$, $p^\bullet = F$ and $m_0(p) = 0$
2. $\forall f \in F$, $\mathcal{C}(f) = \mathcal{C}(p) \times C_f$ and $W^-(p, f)$ is an ortho-projection from $\mathcal{C}(p) \times C_f$ to $\mathcal{C}(p)$;
3. $\forall h \in H$ $W^+(p, h)$ is a unitary quasi-onto mapping such that ${}^t(W^+(p, h))$ is a quasi-onto mapping

The first point ensures that place p models an intermediate state between the firing of a transition in H and the firing of a transition in F. The second one ensures that any firing of a transition f requires exactly one token in p. The last point guarantees that all instances of any firing of $h \in H$ produces a token in the place p and that any coloured token of $\mathcal{C}(p)$ may be produced by a firing of some transition $h \in H$.

The **HF-interchangeability** hypothesis mainly restricts either the set H or F to be a singleton in order to avoid the case where $h \in H$ and $f \in F$ are live in the original net whereas the transition hf is not live in the reduced net.

DEFINITION *3.2.* (Hypothesis R2). A p-post-agglomerable coloured net is HF-interchangeable if one of these conditions is fulfilled :

1. $H = \{h\}$ and $W^+(p, h)$ is orthonormal
2. $F = \{f\}$, $\mathcal{C}(f) = \mathcal{C}(p)$ (thus $W^-(p, f)$ is orthonormal)

In the following, we will assume w.l.o.g. that depending on the item of the above definition either $W^+(p, h)$ is the identity function and $W^-(p, f)$ is a projection or $W^-(p, f)$ is the identity function. Indeed applying the reduction called orthonormalization leads to this situation (see Haddad (1991)).

The **F-independence** hypothesis ensures that when the place p is marked, no transition that can produce tokens useful for the firing of a transition in F can be fired.

Definition *3.3.* (Hypothesis R3). A p-post-agglomerable coloured net is F-independent if $\forall f \in F$, $\forall q \in ({}^\bullet f \setminus \{p\})$, $\forall t \in {}^\bullet q \setminus F$, $\exists p_t \in {}^\bullet t$, such that

(1) there exists a binary coloured positive invariant $\mathcal{F} = \sum_{r \in P} \mathcal{F}_r.r$ on a domain D

(2) let us note
$$\phi = \overline{{}^t(W^+(q,t))} \circ \overline{W^-(q,f)} \circ \overline{{}^t(W^-(p,f))}$$
$$\psi = \overline{{}^t(W^-(p_t,t))} \circ \overline{{}^t(\mathcal{F}_{p_t})} \circ \overline{\mathcal{F}_p}$$
then $\phi \sqsubseteq \psi$

Furthermore, if there exists a binary positive invariant $\mathcal{F}'$ on the domain $\mathcal{C}(p)$ such that ${}^t\mathcal{F}'_p$ is a quasi-onto mapping then the net is **strongly** F-independent.

These two points ensure that the transitions of ${}^\bullet({}^\bullet f[c_f])$ (dashed transitions of figure Fig. 5) are not fireable when the related instance $p[c_p]$ of place p is marked. This behaviour is obtained by the use of a binary positive invariant that ensures a mutual exclusion of the place $p[c_p]$ with place $p_t[c_{p_t}]$ which are pre-conditions of these transitions t. The mapping ψ allows us to highlight the instances of the transition t that are linked to an instance of p_t covered by the a positive invariant (in the unfolded net) which covers a given instance of p.

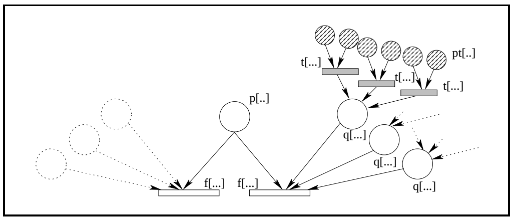

Fig. 5. A subset of $\phi(c_p), c_p \in \mathcal{C}(p)$

The third hypothesis, the F**-continuation**, means that an excess of occurrences of $h \in H$ can always be reduced by subsequent firings of transitions of F (when the place p is marked, a transition of F is necessarily fireable).

Definition *3.4.* (Hypothesis R4). A p-post-agglomerable net is F-continuable if either $\exists f \in F$ such that ${}^\bullet f = \{p\}$ or $\exists\ F_s \subset F$ such that :

(1) $\forall f \in F_s$, ${}^\bullet f = \{p, p_f\}$,

(2) $\forall f \in F_s$, ${}^t(W^-(p_f, f))$ is a quasi-one to one mapping,

(3) there exists a flow on $\mathcal{C}(p)$ with
$$\mathcal{F} = \sum_{f \in F_s} \mathcal{F}_{p_f}.p_f - \lambda.\mathcal{F}_p.p$$
$\forall f \in F_s$, $W^-(p_f, f) \circ \langle X_{\mathcal{C}(p)}, All_{C_f} \rangle = {}^t\mathcal{F}_{p_f}$ and such that
   (a) either $\lambda = 0$ and $\mathcal{F}$ induces a binary positive invariant
   (b) or $\lambda = 1$ and $\mathcal{F}$ induces a synchronisation invariant

3.4 Post-agglomeration transformation

We define now the transformation associated to the coloured post-agglomeration. The reduced net is the same as the original one except that we merge any transition of H with transitions of F (we form couples (hf)).

Definition *3.5.* The reduced net (CN_r, m_{0r}) obtained from a coloured net (CN, M_0) by a coloured post-agglomeration is defined by:

- $P_r = P$ and $T_r = T \setminus (H \cup F) \cup (H \times F)$; we note hf a new transition $(h, f) \in H \times F$.
- $\forall p' \in P_r, m_{0r}(p') = m_0(p')$
- $\forall t \in T_r \setminus (H \times F)$, $\forall p' \in P_r$, $W_r^-(p', t) = W^-(p', t)$ and $W_r^+(p', t) = W^+(p', t)$
- $\forall hf \in (H \times F)$, $\forall q \in P_r$
  · $W_r^-(q, hf) = max(\Gamma_1, \Gamma_2)$
  · $W_r^+(q, hf) = \Upsilon + W_r^-(q, hf))$
  where
  when $H = \{h\}$, then, $\mathcal{C}(hf) = \mathcal{C}(f)$ and
  · $\Gamma_1 = W^-(q, h) \circ W^-(p, f)$,
  · $\Gamma_2 = W^-(q, f) - W(q, h) \circ W^-(p, f)$
  · $\Upsilon = W(q, f) + W(q, h) \circ W^-(p, f)$
  when $F = \{f\}$, then $\mathcal{C}(hf) = \mathcal{C}(h)$ and
  · $\Gamma_1 = W^-(q, h)$
  · $\Gamma_2 = W^-(q, f) \circ W^+(p, h) - W(q, h)$
  · $\Upsilon = W(q, f) \circ W^+(p, h) + W(q, h)$

This transformation preserves the Petri net liveness and the properties related to the maximal or infinite sequences (e.g. deadlock, fairness, mutual-exclusion,etc.). The corresponding theorem can be found in the appendix.

3.5 An example

The following coloured net (Fig. 6) models the allocation of resources ($C2$) to processes ($C1$). When receiving a request from a process X, the server chooses a free resource Y, sends this resource identity to the process and stores locally (in place `Taken`) this allocation (`ts1`). Upon reception of a resource release request (`t3`) the server services this request (`ts2`) when the request corresponds to an already stored allocation (a token `(X,Y)` is in the place `Taken`).

Let us describe the reduction process on this net in order to look for possible deadlocks. At first, we delete the implicit places `Server` and `Att2`. Then we apply a post-agglomeration of the transition `t2` with the transition `t3` and a post-agglomeration of the transition `ts2` with the transition `t4`. Note that these agglomerations would be still possible with the reductions of Haddad (1991). But on the reduced net of Fig.7 no reductions previously defined are applicable. However, the post-agglomeration of h = `ts1` with f = `t2` around

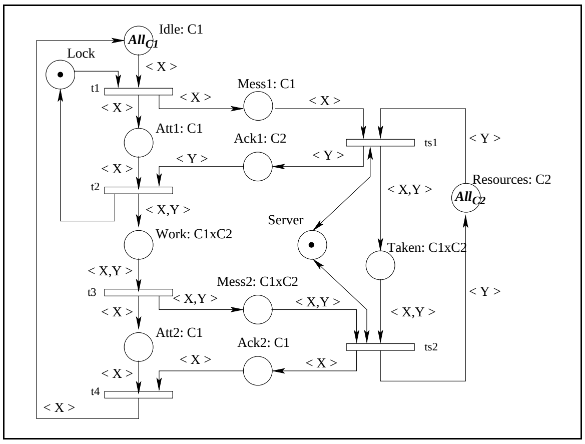

Fig. 6. Typed resource allocation

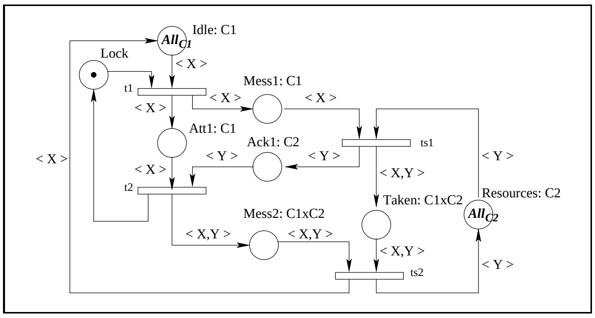

Fig. 7. No more standard reductions

the place $p =$ Ack1 is applicable. Indeed, $\mathcal{C}(f) = \mathcal{C}(p) \times C2$, $W^-(p, f)$ is an ortho-projection, $H = \{h\}$, $W^+(p, h)$ is an ortho-projection so the net is p-post agglomerable (but does not verify the HF-interchangeability).

The unique transition related to the F-independency hypothesis is the transition $t1$ (which may put token in place Att). The flow $\mathcal{F} = \langle All_{C1}\rangle.Lock + \langle All_{C1}\rangle.Mess1 + \langle All_{C1}\rangle.Ack1$ on $C1$ induces the binary positive invariant: $\forall m \in Reach(N, m_0)$, $m(Lock) + \sum_{c\in C1} m(Mess1)(c) + \sum_{c\in C2} m(Ack1)(c) = 1$. Using notation of the hypothesis conditions, $\phi = All_{C1}$ and $\psi = All_{C1}$. So, $\phi \sqsubseteq \psi$ and since ${}^t(All_{C1}) = All_{C1}$ is a quasi-onto mapping the net is strongly F-independent.

At last, the flow $\mathcal{F} = \langle All_{C2}\rangle.Mess1 + \langle All_{C2}\rangle.Ack1 - \langle All_{C2}\rangle.Att1$ induces the synchronisation invariant $\forall m \in Reach(N, m_0)$, $\sum_{c\in C1} m(Mess1)(c) + \sum_{c\in C2} m(Ack1)(c) - \sum_{c\in C1} m(Att11)(c) = 0$ which fulfils the conditions of the F-continuation hypothesis (t2 is fireable as soon as Att1 is marked). Applying this reduction leads to the net depicted Fig.8. Finally the implicit places Mess2 and Att1 are deleted and then a post-agglomeration of ts1 with ts2 followed by a post-agglomeration of t1 with ts1 produces the net depicted Fig.9 where all the places being implicit may be deleted. As the final net is live, the original one is also live (see Theorem 1 in appendix).

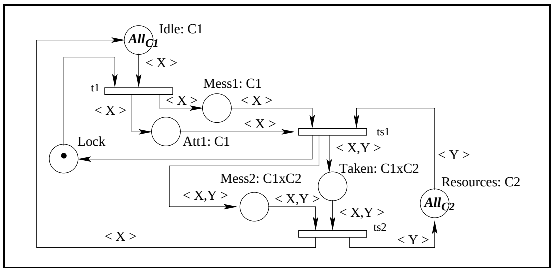

Fig. 8. Application of a post-agglomeration

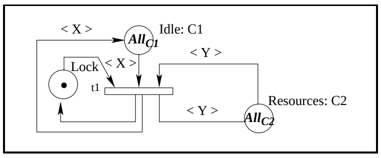

Fig. 9. A live net

4. CONCLUSION

We have presented in this paper new coloured reductions and we have precisely defined one of them: the post-agglomeration. These reductions are based on accurate conditions using linear invariants that cover more realistic concurrent software behaviours (compared to initial conditions which were only based on the structure of the model). We are integrating a syntactic version of these reductions in the Quasar tool, a framework for verifying concurrent programs (see http://quasar.cnam.fr).

REFERENCES

C. Chiola, C. Dutheillet, G. Franceschinis, and S. Haddad. On well-formed colored nets and their symbolic reachability graph. In *ICATPN*, Paris-France, June 1990.

J.M. Colom, J. Martinez, and M. Silva. Packages for validating discrete production systems modeled with Petri nets. In *IMACS-IFAC Symposium*, Lille, France, 1986.

S. Evangelista, S. Haddad, and J.F. Pradat-Peyre. Petri nets reductions for software validation. Technical report, CEDRIC, CNAM, Paris, 2004.

H.J. Genrich. Equivalence transformations of prt-nets. In Jensen and Rozenberg, editors, *High-level Petri Nets, Theory and Application*, pages 426–453. Springer-Verlag, 1991.

S. Haddad. A reduction theory for colored nets. In Jensen and Rozenberg, editors, *High-level Petri Nets, Theory and Application*, LNCS, pages 399–425. Springer-Verlag, 1991.

S. Haddad and J.F. Pradat-Peyre. Efficient reductions for LTL formulae verification. Technical report, CEDRIC, CNAM, Paris, 2004.

APPENDIX

Definition *.1.* (Multisets). A multiset over a finite and non empty set C is an application from C to $\mathbb{N}$. We note $Bag(C)$ the set of multisets over C and we represent a multiset by the formal sum $a = \sum_{y \in C} a(y).y$. If a and b are two multisets over C, then $a + b$ is the multiset over C defined by $a+b = \sum_{y \in C}(a(y)+b(y)).y$ and if λ is a natural, then $\lambda.a$ is the multiset over C defined by $\lambda.a = \sum_{y \in C}(\lambda.a(x)).x$. We define $a - b$ as the multiset over C by $\forall x \in C, (a-b)(x) = max(0, a(x)-b(x))$. One say that a is greater or equal than b, denoted $a \geq b$ if and only if $\forall y \in C, a(y) \geq b(y)$.

Definition *.2.* (Unfolded Petri net). Let $CN = \langle P, T, \mathcal{C}, W^+, W^- \rangle$ be a coloured net. The corresponding unfolded (or underlying) Petri net is the net $\langle P_d, T_d, W_d^+, W_d^- \rangle$ defined:

- $P_d = \cup_{p \in P, c_p \in \mathcal{C}(p)} p[c_p]$ the set of places;
- $T_d = \cup_{t \in T, c_t \in \mathcal{C}(t)} t[c_t]$ the set of transitions;
- W_d^+ (resp. W_d^-) is the forward (resp. backward) incidence mapping from $P_d \times T_d$ to $\mathbb{N}$ defined by: $\forall p[c_p] \in P_d, t[c_t] \in T_d$, $W_d^+(p[c_p], t[c_t]) = W^+(p,t)(c_t)(c_p)$ (resp. $W_d^-(p[c_p], t[c_t]) = W^-(p,t)(c_t)(c_p)$).

In the same way, each coloured marking m can be "unfolded" into a un-coloured marking m_d by: $\forall p[c_p] \in P_d, m_d(p[c_p]) = m(p)(c_p)$. Using these definitions we obtain obviously that the semantic of a coloured net is the same than the one of its corresponding underlying Petri net: $m[t, c_t > m'$ in CN if and only if $m_d[t[c_t] > m'_d$ in the underlying net.

Definition *.3.* (Tuple and composition). Let f_1 be a mapping from $Bag(C_1)$ to $Bag(C'_1)$, $f2$ a mapping from $Bag(C_2)$ to $Bag(C'_2)$ and g a mapping from $Bag(C)$ to $Bag(C_1)$.

- $< f_1, f_2 >$ is the mapping defined from $Bag(C_1) \times Bag(C'_1)$ to $Bag(C_2) \times Bag(C'_2)$ by $< f_1, f_2 > (c_1, c_2) =< f_1(c1), f_2(c_2) >$
- $f_1 \circ g$ is the mapping defined from $Bag(C)$ to $Bag(C'_1)$ by $(f_1 \circ g)(c) = f(g(c))$
- $\overline{f_1} \circ \overline{g} = \overline{f_1 \circ g}$
- if h is a mapping from $Bag(C)$ to $Bag(C_1)$ then $\overline{h} + \overline{g}$ is the mapping defined by: $\forall c \in Bag(C)$, $(\overline{h}+\overline{g})(c) = \overline{h}(c) \cup \overline{g}(c)$ (so $\overline{h}+\overline{g} = \overline{h+g}$)

Definition *.4.* (Mapping characterisation). Let f be a mapping from $Bag(C)$ to $Bag(C')$.

- f is **orthonormal** iff $C = C'$ and there exists a substitution σ of C such that $\forall c \in C, f(c) = \sigma(c)$
- f is **unitary** iff $\forall c' \in C', \forall c \in C, f(c)(c') = 0$ or $f(c)(c') = 1$
- f is a **projection** iff $C = C' \times C_1$ and $\forall c = (c', c_1) \in C$, $f(c) = c'$
- f is an **ortho-projection** iff $C = C' \times C_1$ and $f = f' \circ g$ with g a projection from C to C' and f' an orthonormal mapping on C'.

Definition *.5.* (Particular colour functions). We use in our models some specific colour functions. Let $C = C_1 \times C_2 \times \ldots \times C_k$ be a colour domain:

- $\langle X_{C_i} \rangle$ denotes the projection from C to C_i. When there is no ambiguity, we simply note $\langle X \rangle$ or $\langle Y \rangle$;
- $\langle All_{C'} \rangle$ denotes the constant broadcast defined by $\forall c \in C$, $All_{C'}(c) = \sum_{c' \in C'} c'$.

A coloured net defines a set of behaviours that can be characterised either by general properties (like liveness) or using maximal and infinite fireable sequences.

Definition *.6.* Let (CN, m_0) be a coloured net.

- (CN, m_0) is live iff $\forall m \in Reach(N, m_0)$, $\forall t \in T$, $\forall c_t \in \mathcal{C}(t)$, $\exists s \in T^*$ $m[s.(t, c_t)\rangle$;
- $L(N, m_0) = \{s \in (T \times \mathcal{C}(T))^* | m_0[s\rangle\}$ is the language of finite sequences,
- m is a dead marking if $\forall t \in T$, $\forall c_t \in \mathcal{C}(t)$, $NOT(m[t, c_t\rangle$;
- $L^{Max}(N, m_0) = \{s \in (T \times \mathcal{C}(T))^* | \exists m$ a dead marking, $m_0[s\rangle m\}$ is the language of finite maximal sequences,
- $L^\infty(N, m_0) = \{s \in (T \times \mathcal{C}(T))^\infty | m_0[s\rangle\}$ is the language of infinite sequences,

Theorem 1. Let $N = (CN, m_0)$ be a coloured net and $N_r = (CN_r, m_0)$ be the post-agglomerated net.

- If N verifies R1, R2 and R3 then
$$N \text{ is live} \Longrightarrow N_r \text{ is live}$$
- If N verifies R1, R3 and R4 then
$$N \text{ is live} \Longleftarrow N_r \text{ is live}$$
- If N verifies R1, R3 and R4 then
$$\Pi_{T_0 \cup F}(L^{max}(N)) = \Pi_{T_0 \cup F}(\phi_{hf}(L^{max}(N_r)))$$
- If N verifies R1, R3 (strong) and R4 then
$$\Pi_{T_0 \cup F}(L^\infty(N)) = \Pi_{T_0 \cup F}(\phi_{hf}(L^\infty(N_r)))$$

where ϕ_{hf} is the mapping from T_r^* to T^* (or its extension from T_r^∞ to T^∞) defined by $\forall t \in T_0$, $\phi_{hf}(t) = t$ and $\forall hf \in (H \times F)$, $\phi_{hf}(hf) = h.f$.