DE NOUVELLES RÉDUCTIONS COLORÉES
POUR LA VALIDATION DE LOGICIELS
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 Cédex 16

Abstract: Une abstraction structurelle du modèle analysé permet de réduire très efficacement la complexité d’une méthode d’analyse basée sur l’énnumération des états accessibles. Nous présentons dans cet article des réductions pertinentes de réseaux colorés construites sur de nouvelles réductions de réseaux de Petri ordinaires. Ces réductions ne font appel qu’à des conditions structurelles ou algébriques. Elles préservent la vivacité du modèle mais aussi toute formule LTL qui n’observe pas les transitions réduites du réseau. L’utilisation conjointe de conditions structurelles et algébriques permet d’élargir significativement le domaine d’application de ces réductions. De plus la définition de ces réductions est paramétrée vis à vis du cardinal des domaines de couleurs.

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 instruc-
tions into a virtual atomic one. Such a transformation drastically reduces the combinatorial 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 Petri nets reductions, Colom et al. (1986), Genrich (1990), Haddad (1990), 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.

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 $\text{Bag}(C)$ 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 $\mathrm{CN} = (P, T, C, W^+, W^-)$ with:

- $P$ a non empty and finite set of places;
- $T$ a non empty and finite set of transitions (disjoint of $P$);
- $C$ is the colour mapping from $P \cup T$ to $\omega$ where $\omega$ is a set of finite and non empty sets. An item of $C(s)$ is called a colour of $s$ and $C(s)$ 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 $C(t)$ to $\text{Bag}(C(p))$. 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 $\epsilon$).

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

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

The firing of $t, c_i$ from $m$ leads to the marking $m'(m[t, c_i]m')$ defined by $\forall p \in P, m'(p) = m(p) + W(p, t)(c_i)$. 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 $m[t_1, c_1]m_1, m_1[t_2, c_2]m_2, \ldots, m_{k-1}[t_k, c_k]m'$. We denote by $\text{Reach}(\mathrm{CN}, m_0)$ 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 $c_p \in C(p)$ and the set of transitions $t[c_t]$, $t \in T, c_t \in C(t)$. 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 $\text{Bag}(D)$ to a function from $\text{Bag}(C)$ to $\text{Bag}(C(F))$ such

**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 $\text{Bag}(C(p))$ to $\text{Bag}(C(\mathcal{F}))$ such
that: \( \forall t \in T, \sum_{p \in P} \lambda_p \cdot \mathcal{F}_p \circ W(p, t) = 0 \).

\( \mathcal{F} \) induces the invariant:
\[ \forall m \in \text{Reach}(CN, m_0), \sum_{p \in P} \lambda_p \cdot \mathcal{F}_p(m(p)) = \sum_{p \in P} \lambda_p \cdot \mathcal{F}_p(m_0(p)) \]
An invariant \( \mathcal{F} \) is positive if \( \forall p \in P, \lambda_p \geq 0 \). It is binary if \( \forall c \in \mathcal{C}(\mathcal{F}), \sum_{p \in P} \lambda_p \cdot \mathcal{F}_p(m_0(p))(c) = 1. \)
It is a \textit{synchronisation} invariant if \( \forall c \in \mathcal{C}(\mathcal{F}), \sum_{p \in P} \lambda_p \cdot \mathcal{F}_p(m_0(p))(c) = 0. \)

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 \( \text{Bag}(C) \) to \( \text{Bag}(C') \).

- \( f' \) is the mapping defined from \( \text{Bag}(C') \) to \( \text{Bag}(C) \) by \( (f'(c'))(c) = f(c)(c') \)
- \( \overline{f} \) is defined from \( \mathcal{P}(C) \) to \( \mathcal{P}(C') \) by \( \overline{f}(D) = \{ c' \in C' | \exists d \in D, f(d)(c') \neq 0 \} \) 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 \( f \subseteq g \) if \( \forall c \in \text{Bag}(C), f(c) \subseteq g(c) \).

Below we list particular mappings. An orthonormal mapping is a colour domain permutation, a \textit{unitary} mapping produces at most one token per colour, a \textit{projection} is a canonic mapping from \( \text{Bag}(C \times D) \) to \( \text{Bag}(C) \), an \textit{orthoprojection} is the composition of an orthonormal mapping with a projection. \( f \) is a \textit{quasi-one to one} mapping if \( \forall c \neq d \exists (c) \cap \overline{f}(d) = \emptyset. \) A \textit{quasi-onto} mapping from \( \text{Bag}(C) \) to \( \text{Bag}(D) \) 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: \( T = \text{Pre} \sqcup H \sqcup F. \)

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

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

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

![Fig. 1. Updating variables sequentially](image1)

![Fig. 2. Updating variables atomically](image2)
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 $c_f \in C(f)$, we want to compute the colours \( \{c_h \in C(h)\} \) 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 $\Xi(c_f)$. Then we have to find instances of $h$ that are linked to a place $p[c_p]$, $c_p \in \Xi(c_f)$. These instances are the set $\{c_h \in C(h), \Xi(c_h) \cap \Xi(c_f) \neq \emptyset\}$. By definition of the transposition of a function, this set is $\Xi^T(\Xi(c_f))$. Thus, the set of colours we look for is $\Xi^T(\Xi(c_f))$. In an opposite way, the set of instances of $f$ that are causally dependent of an instance $c_h$ of $h$, are $\Xi^T(\Xi(c_h))$. Let us consider now the following coloured Petri net where $p$ is an ordinary place (see Fig.4).

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig3.png}
\caption{Colour mapping manipulation illustration}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig4.png}
\caption{An invariant containing $f_1$ and $f_2$}
\end{figure}

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

\begin{itemize}
  \item 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 $\Xi_1(\text{All}_{C_1}(\bullet))$ or in $\Xi_2(\text{All}_{C_2}(\bullet))$.
  \item Since $\{c_{\alpha_1}, c_{\alpha_2}\} = \text{unitary one to one mappings}$, 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 $\alpha_i(c_i)$.
  \item Combining these two facts, an instance $(f_i, c_i)$ for some $i$ is always fireable when $p$ is marked.
\end{itemize}

Remark that this reasoning is still valid if we only require that $\forall i, \mathcal{F}_{q_i} \subseteq 4(\alpha_i \circ \text{All}_{C_i})$.

3.3 Post-agglomeration hypotheses

We present the four conditions of the post-agglomeriation: 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. $p^* = H$, $p^* = F$ and $m_0(p) = 0$  
2. $\forall f \in F, C(f) = C(p) \times C_f$ and $W^-(p, f)$ is an ortho-projection from $C(p) \times C_f$ to $C(p)$;  
3. $\forall h \in H W^+(p, h)$ is a unitary quasi-onto mapping such that $\{W^+(p, h)\}$ 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 $C(p)$ 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 ∈ H and f ∈ 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}, C(f) = 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 (1990)).

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 ∀f ∈ F, ∀q ∈ (Φf \ {p}), ∀t ∈ Φq \ F, ∃p_h ∈ t, such that

1. there exists a binary coloured positive invariant F = ∑_t∈P F_r.t on a domain D
2. let us note
   \[ \phi = (W+(q, t)) \circ W−(q, f) \circ (W+(p, f)) \]
   \[ \psi = (W−(pq, t)) \circ (F_p) \circ F_p \]

then \( \phi \subseteq \psi \)

Furthermore, if there exists a binary positive invariant \( F^f \) on the domain C(p) such that \( F^f_p \) is a quasi-onto mapping then the net is strongly F-independent.

These two points ensure that the transitions of \( *\phi(f, e) \) (dashed transitions of figure Fig. 5) are not fireable when the related instance \( p_e[p] \) 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 \( p_e[p] \) with place \( p_0[p] \) which are pre-conditions of these transitions t. The mapping \( \psi \) allows us to highlight the instances of the transition t that are linked to an instance of \( p_0 \) covered by the a positive invariant (in the unfolded net) which covers a given instance of p.

The third hypothesis, the F-continuation, means that an excess of occurrences of h ∈ 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 ∃f ∈ F such that \( *f = \{p, g\} \),

1. ∀f ∈ F, \( *f = \{p, g\} \),
2. \( t(W^-(p, f)) \) is a quasi-one to one mapping,
3. there exists a flow on C(p) with
   \[ F = \sum_{f \in F} F_{p,f} - \lambda . F_{p,p} \]

∀f ∈ F, \( W^-(p, g) \circ 2. \lambda . (C_{p,f}) = tF_{p,f} \)

and such that
1. either \( \lambda = 0 \) and \( F \) induces a binary positive invariant
2. or \( \lambda = 1 \) and \( F \) 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 (h, f)).

**Definition 3.5.** The reduced net \( (CN_r, m_0_r) \) 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 \((h, f) \in H \times F\).
- \( \forall p' \in P_r, m_0(p') = m_0(p) \)
- \( \forall t \in T_r \setminus (H \times F), \forall p' \in P_r, W^-(p', t) = W^-(p', t) \) and \( W^+(p', t) = W^+(p', t) \)
- \( \forall h, f \in (H \times F), \forall q \in P_r, \)
  - \( W_r^-(q, hf) = \max(\Gamma_1, \Gamma_2) \)
  - \( W_r^+(q, hf) = T^+ + W_r^-(q, hf) \)

where

- when \( H = \{h\} \), then \( C(h, f) = C(f) \) and
  - \( \Gamma_1 = W^-(q, h) \circ W^-(p, f) \),
  - \( \Gamma_2 = W^-(q, h) \circ W^-(p, f) \)
  - \( T = W(q, f) + W(q, h) \circ W^-(p, f) \)

when \( F = \{f\} \), then \( C(h, f) = C(h) \) and
  - \( \Gamma_1 = W^-(q, h) \)
  - \( \Gamma_2 = W^-(q, f) \circ W^+(p, h) - W(q, h) \)
  - \( T = W(q, f) \circ W^+(p, h) + W(q, h) \)

This transformation preserves the Petri net liveliness 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 (1990). But

Fig. 6. Typed resource allocation

on the reduced net of Fig.7 no reductions previously defined are applicable. However, the post-agglomeration of h = ts1 with f = t2 around the place p = Ack1 is applicable. Indeed, C(f) = C(p) × 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-independence hypothesis is the transition t1 (which may put token in place Att). The flow F = (AllC1).Lock + (AllC1).Mess1 + (AllC1).Ack1 on C1 induces the binary positive invariant: \( \forall m \in Reach(N, m_0), \sum_{c \in C1} m(Mess1)(c) + \sum_{c \in C2} m(Ack1)(c) = 1 \). Using notation of the hypothesis conditions, \( \phi = AllC1 \) and \( \psi = AllC1 \). So, \( \phi \subseteq \psi \) and since \( \forall (AllC1) = AllC1 \) is a quasi-mapping the net is strongly F-independent.

At last, the flow \( F = (AllC2).Mess1 + (AllC2).Ack1 - (AllC2).Att1 \) induces the synchronisation invariant \( \forall m \in Reach(N, m_0), \sum_{c \in C1} m(Mess1)(c) + \sum_{c \in C2} m(Ack1)(c) - \sum_{c \in C1} m(Att1)(c) = 0 \) which fulfills 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

Fig. 7. No more standard reductions

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

Fig. 8. Application of a post-agglomeration

one is also live (see Theorem 1 in appendix).

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).
5. ACKNOWLEDGMENTS

A first version of this paper was published at IFAC Workshop on Discrete Event Systems, WODES'04, 22-24 September 2004.

6. ACKNOWLEDGMENTS

REFERENCES


