DE NOUVELLES REDUCTIONS COLOREES POUR LA VALIDATION DE LOGICIELS

30/09/2017

Auteurs : Sami Evangelista, Serge Haddad, Jean-François Pradat-Peyre

Publication e-STA N° e-STA 2004-3


DOI :

Télécharger
Le téléchargement implique l’acceptation de nos conditions d’utilisation

e-STA 2004-3

• Abstract
• Authors
• Metrics
• License

Abstract

Authors

Sami Evangelista

DE NOUVELLES REDUCTIONS COLOREES POUR LA VALIDATION DE LOGICIELS

Serge Haddad

ÉVALUATION DE PERFORMANCE DES SYSTÈMES STOCHASTIQUES À ÉVÉNEMENTS DISCRETS NON MARKOVIENS - UNE NOUVELLE APPROCHE

Jean-François Pradat-Peyre

DE NOUVELLES REDUCTIONS COLOREES POUR LA VALIDATION DE LOGICIELS

Metrics
La SEE (Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication – Association reconnue d’utilité publique, régie par la loi du 1er juillet 1901) met à la disposition de ses adhérents et des abonnés à ses publications, un ensemble de documents numériques accessibles à partir de son portail des publications. Ces documents incluent notamment les articles des revues REE, 3 EI et e-STA disponibles sous forme numérique ainsi que des publications additionnelles regroupées dans l’espace eREE. Les présentes conditions précisent les conditions de diffusion et d’utilisation de ces documents et des informations qu’ils contiennent. L’accès à ces documents, qu’il se fasse de façon gratuite ou dans le cadre d’abonnements ou d’achats faits à titre onéreux, implique l’acceptation sans restriction de ces dispositions.

Droits de propriété et de diffusion des contenus téléchargés sur le portail des publications

Les contenus rendus accessibles sur le portail des publications sont, en règle générale, protégés par le droit d’auteur. En tant que producteur, et le cas échant d’auteur, des informations rassemblées dans les contenus accessibles par ce portail, SEE se réserve l’exclusivité des droits de copie et de diffusion de tout ou partie de ces contenus.

Les contenus sont rendus accessibles à titre individuel, pour les besoins de la personne en détenant des droits d’accès en cours de validité. Aussi, la modification, la reproduction et/ou la diffusion via Internet ou le Web, intranet, extranet ou toute autre forme numérique ou imprimée, de tout ou partie des contenus téléchargés sont interdites. Une tolérance est consentie quant à la reproduction d’extraits limités de ces contenus, dans le cadre de travaux ou d’activités auxquels ils sont utiles, à la condition que l’origine de ces reproductions partielles soit mentionnée de façon lisible et sans ambiguïté. Figureront en particulier : la REE (ou toute autre revue accessible sur le portail) en tant que la source, la référence de la publication et le nom de l’auteur (s’il figure dans la revue).

Ces dispositions s’appliquent également aux figures, illustrations, logos ou images.

Publication externe des contenus du portail des publications

Tout extrait des contenus du portail destiné à être utilisé dans des publicités, des communiqués de presse ou du matériel de promotion nécessite un accord préalable écrit de la SEE. Une version préliminaire du document proposé contenant ces extraits doit accompagner chacune de ces demandes. SEE se réserve le droit de refuser un tel usage externe pour quelque raison que ce soit.

Responsabilités
La SEE apporte tout le soin possible à la préparation des informations délivrées dans les contenus produits. Cependant elle ne peut être tenue pour responsable d’aucune perte ou frais qui pourrait résulter d'imprécisions, d'inexactitudes, d'erreurs ou de possibles omissions portant sur des informations publiées, ni des résultats obtenus par l'utilisation et la pratique des informations délivrées.

Utilisation des informations recueillies lors du téléchargement de contenu

Le portail des publications est susceptible d'utiliser des « cookies » afin notamment de permettre l'utilisation de paniers d'achat et de personnaliser les parcours sur le site. SEE se réserve la possibilité d'utiliser les informations recueillies lors des téléchargements pour ses besoins internes et notamment pour l'amélioration de ses services, sans qu'elles puissent être cédées à des partenaires commerciaux. Conformément à la loi "informatique et libertés" du 6 janvier 1978, chaque utilisateur du portail dispose d'un droit d'accès et de rectification aux informations qui le concernent. Pour exercer ce droit, les utilisateurs doivent s'adresser à SEE – 17 rue de l'amiral Hamelin – 75783 Paris Cedex 16, par simple lettre ou en utilisant le formulaire de contact disponible sur son site.

Paris, le 28 avril 2013

Metadata Datacite XML candidate:

```
<resource xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns="http://datacite.org/schema/kernel-4"
  <identifier identifierType="DOI">10.23723/545:2004-3/20046</identifier>
  <creator><creatorName>Sami Evangelista</creatorName></creator>
  <creator><creatorName>Serge Haddad</creatorName></creator>
  <creator><creatorName>Jean-François Pradat-Peyre</creatorName></creator>
  <title>DE NOUVELLES REDUCTIONS COLOREES POUR LA VALIDATION DE LOGICIELS</title>
  <publisher>SEE</publisher>
  <publicationYear>2017</publicationYear>
  <resourceType resourceTypeGeneral="Text">Text</resourceType>
  <dates>
    <date dateType="Created">Sat 30 Sep 2017</date>
    <date dateType="Updated">Sat 30 Sep 2017</date>
    <date dateType="Submitted">Sun 17 Nov 2019</date>
  </dates>
  <alternateIdentifiers>
    <alternateIdentifierType="bitstream">aa9eed7f99938ee03cf46d2ef3f0046a056fd967</alternateIdentifier>
  </alternateIdentifiers>
  <formats>
    <format>application/pdf</format>
  </formats>
  <version>34063</version>
  <descriptions>
    <description descriptionType="Abstract"></description>
  </descriptions>
</resource>
```

DE NOUVELLES REDUCTIONS COLOREES 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 Latte de Tassigny 75775 Paris Cedex 16 Abstract: Une abstraction structurelle du modèle analysé permet de réduire très efficacement la complexité d’une méthode d’analyse basée sur l’énumération 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 conservent 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 combinatorial explosion factor. The structural methods are generally efficient but they do not ensure the complete correctness of the model-elled system. Thus an attractive trade-off would be to first per-form 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 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 satisfying 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 re-ductions at a syntactic level in order to efficiently check the conditions and apply the transformation. We will not describe this part which can be found in Evangelista et al. (2004).

Compared to previous work concerning high-level 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 reducing- tions 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 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 = hP, T, C, W+, W− , i with : α P a non empty and finite set of places; α T a non empty and finite set of transitions (disjoint of P); α C is the colour mapping from P to where ω 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. α 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 Bag(C(p)). We note W = W − +W+. We note = ⊑ the domain reduced to the single value α (the neutral token); so, ordinary Petri nets can be viewed as particular coloured Petri nets (the unique and common colour domain is ). Definition 2.2. A marking is a mapping that associates to each place p a value in Bag(C(p)). We note m0 the initial marking of a net. A transition t is fireable for an instance ct ∈ C(t) from a marking m (denoted by [m[t], ct]) if ∀p ∈ P, m(p) ≥ W− (p, t)(ct) The firing of t, ct from m leads to the marking m0 (m0, ct]) defined by ∀p ∈ P, m0 (p) = m(p) + W+(p, t)(ct). A marking m0 is reach-able from a marking m if there exists a sequence t1, t2, . . . , tk such that m1[t1, c1]m2[c2, t2]m3[c3, t3] . . . mk−1[tk, cmk−1] We denote by Reach(CN, m0) the set of all reachable markings from m0. 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] where p ∈ P and cp ∈ C(p) and the set of transitions [ct], t ∈ T, ct ∈ 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 invari- ants. 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 F, on a domain C(F), is a vector over P, noted as the formal sum F = P p∈P χ(F) F(p), where χ(F) ∈ Z and F(p) a mapping from Bag(C(p)) to Bag(C(F)) such that: ∀t ∈ T, P p∈P χ(F)p − · W+(p, t) = 0. F induces the invariant: ∀m ∈ Reach(CN, m0), P p∈P χ(F)p(m0(p)) = P p∈P χ(F)p(m0(p)) An invariant F is positive if ∀p ∈ P, χ(F)p ≥ 0. It is binary if ∀p ∈ C(F), P p∈P χ(F)p(m0(p))(c) = 1. It is a synchronisation invariant if ∀c ∈ C(F), P p∈P χ(F)p(m0(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(C0) . α f is the mapping defined from Bag(C0 ) to Bag(C) by t f(c0)(c) = f(c)(c0 ) . α f is defined from P(C) to P(C0 ) by f(D) = {c0 ∈ C0 | 3d ∈ D, f(d)(c0 ) = 0} where P(C) denotes the power set of C. Note that the linearity is preserved by this.
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.

The potentially post-agglomerability ensures that in any fireable sequence the occurrence of \( f \in F \) in a firing sequence may always be related to a previ- ous 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 \( C(t) \to Bag(C(F)) \) 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 trans- \( p \to h \to q \) \( V_1 : C < X > \to G_1(X) > < G_2(Y) > I < Y > V_2 : C \to C(F) \) Fig. 1. Updating variables sequentially sition \( h \) models the update of a variable modelled by the place \( V_1 \): the value \( X \) is replaced by the value \( G_1(X) \) where \( G_1 \) models a mapping from \( C \) to \( C \). Initially, this variable has the value \( x_0 \). Similarly, the transition \( f \) models the update of a second variable modelled by the place \( V_2 \). Gener- ally, this model does not have the same behaviour as the one of the model depicted in Fig.2 where \( r < G_2(Y) > < Y > V_2 : C \to q \) \( V_1 : C < X > < G_1(X) > \to G_2(X) \) Fig. 2. Updating variables atomically the two updates are performed simultaneously. 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 \( V_1 \) does not change when \( q \) p are marked or the value of \( V_2 \) 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 \( V_1 \) does not change when \( q \) is marked. The variable \( V_1 \) cannot be modified when \( p \) is marked. So, we can delay the update of the variable \( V_1 \) until we are ready to perform the update of the variable \( V_2 \) 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 \( V_2 \) after having waited in state \( p \) or updating \( V_2 \) just after having updated \( V_1 \) is equivalent since value of \( V_2 \) 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 corre- spond to the scheme of the pre or of the post agglomeration, none of the previously defined re- ductions cover such behaviours. The present work is based on reductions for ordinary Petri nets that we proposed in Haddad and Pradet-Peyre (2004). Such reductions cover a large range of patterns by introducing algebraic conditions whereas the previously defined ones solely lie on structural conditions. However the extension of the condi- tions 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 necessar- ily 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 follow- ing coloured Petri net and suppose that, given a \( h \to p : C \to \Phi \) Fig. 3. Colour mapping manipulation illustration colour cf \( \in C(f) \), we want to compute the colours \( ch \in C(h) \) such that the firing of \( h \) for a colour \( ch \) may help the firing of \( f \) for the instance \( cf \) (by producing useful tokens in place \( p \)). We have to start from \( cf \) and to find the instances of \( p \) that are linked to \( f(cf) \). By definition, this set is \( \Phi(cf) \). Then we have to find instances of \( h \) that are linked to a place \( p(cp) \), \( cp \in \Phi(cf) \). These instances are the set \( \{ ch \in C(h) | \Phi(ch) \cap \Phi(cf) \neq \emptyset \} \). By definition of the transposition of a function, this set is \( \Phi(ch) \cap \Phi(cf) \). Thus, the set of colours we look for is \( \Phi(cf) \to \Phi(ch) \). In an opposite way, the set of instances of \( f \) that are causally dependent of an instance \( ch \in h \) are, \( \Phi(ch) \cap \Phi(cf) \). Let us consider now the following coloured Petri net where \( p \) is an ordinary place (see Fig.4).

\h h \to a_2 a_1 \to q_2 \to f \to C_2 : f_1 : C \to F \to q_2 - t (a_2 \to AllC_2 ) a_1 a_2 are unitary one to one mappings \( \forall m \in \text{Reach}(CN, m_0), F(q_1 (m_1)) \to F(q_2 (m_2)) = q_1 = t (a_1 \to AllC_1 ) \) 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 \( F \) is the following one: there is at least one to- ken either in the place \( q_1 \) or in \( q_2 \) whose colour is either in the set \( a_1(AllC_1 (\bullet )) \) or in \( a_2(AllC_2 (\bullet )) \). • Since \( t \to a_1 (i=1,2) \) is an unitary quasi-one to one mapping, each firing instance \( f_1, f_2 \) re- quires, when \( a_2 a_1 \to 0 \), in addition to the token in \( p \), exactly a token in the place \( q_i \) which colour is in the singleton \( a_2 a_1 \). • Combining these two facts, an instance \( f \) can come up when \( p \) is marked. Remark that this reasoning is still valid if we only require that \( f \to q \) \( t (a_1 \to AllC_1 ) \). 3.3 Post-agglomeration hypotheses We present the four conditions of the post- agglomeration: the potentially post-agglomera- bility, the HF-interchangeability, the F- independence and the F-continuation. The potentially post-agglomerability ensures that in any fireable sequence the number of occur- rences 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-agglomer- merable) if \( 3H \to T, F \to T, p \in F \) such that (1) \( \bullet p \to H, p \to F, m_0(p) = 0 \) (2) \( \forall i \to F, C(f) \to C(p) \to C(f) \) \( \bullet \text{and} \) \( W - (f, p) \) is an ortho- projection from \( C(p) \to C(f) \); (3) \( W \in H \in W^+ (p, h) \) 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 a transition of \( H \) 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 \( h \in H \) 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-agglomer- merable coloured net is HF-interchangeable if one of these conditions is fulfilled: (1) \( H = \{ h \} \) and \( W + (p, h) \) is othonormal
symbolic reachability graph. In ICATPN, Paris-France, June 1990. J.M. Colom, J. Martinez, and M. Silva. Packages for validating discrete production systems using linear invariants that cover more realistic concurrent software behaviours (compared to initial conditions which were only based on the structure of the system). Figure 9. A live net one is also live (see Theorem 1 in appendix).

4. CONCLUSION We have presented the flow \( F = h_{\text{AllC1}} \cdot \text{Lock} + h_{\text{AllC1}} \cdot \text{Mess1} + h_{\text{AllC1}} \cdot \text{Ack1} \) on \( C1 \) induces the binary positive invariant:

\[ h = ts1 \quad \text{with} \quad f = t2 \quad \text{around the place} \quad p = Ack1 \]

Indeed, \( \lambda = 1 \) 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 its corresponding transition of \( C(p) \).

\[ \phi \]

Furthermore, if there exists a binary positive invariant \( F0 \) on the domain \( C(p) \) such that \( t \cdot F0 \) is a quasi-onto mapping then the net is strongly F-independent.

\[ \Gamma \]


https://www.see.asso.fr/en/node/20046/landing