Coloured Petri net refinement specification and correctness proof with Coq

Christine Choppy, Micaela Mayero and Laure Petrucci *
LIPN, UMR CNRS 7030, Université Paris 13
FRANCE
firstname.lastname@lipn.univ-paris13.fr

Abstract

In this work, we address the formalisation of symmetric nets, a subclass of coloured Petri nets, refinement in COQ. We first provide a formalisation of the net models, and of their type refinement in COQ. Then the COQ proof assistant is used to prove the refinement correctness lemma. An example adapted from a protocol example illustrates our work.

1 Introduction

Modelling and analysing large and complex systems requires elaborate techniques and support. To harness the problems inherent to designing and model-checking a large system (such as the state space explosion problem), a specification is often developed step by step. First, an abstract model is designed, and its properties are verified. Once it is proven correct, a refinement step takes place, introducing further detail. Such an addition can either be enhancing the description of the actual functioning of part of the system, or introducing an additional part. This new refined model is then verified, and another refinement step can take place. This process is applied until an adequate level of description is obtained.

There are several advantages to using refinement and hence to start with a more abstract model. It gives a better and more structured view of the system under study. The components within the system are clearly identified and the modelling process is eased. The modeller does not have to bother with spurious details. The validation process also becomes easier: the system properties are checked at each step. Thus, abstract models are validated before new details are added. Moreover, when model-checking is used, the analysis of a full concrete model may not be amenable, due to its very large state space. Refinement helps in coping with this problem since it may preserve some properties, or analysis results obtained at an earlier step for a more abstract model may be used for the analysis of the refined model. For example, Lakos and Lewis [9] use the state space of the abstract model to compute the state space of the refined one: some tests for enabledness of transitions are avoided, as well as the construction of partial markings that have already been computed. Moreover, the state space can be structured. Hence, this approach saves both space and time in the analysis, countering the state space explosion problem.

In this paper, we consider specifications written as symmetric nets, a subclass of coloured Petri nets [7]. Lakos and Lewis [8, 9] consider three kinds of Petri nets refinements for coloured Petri nets, node (place or transition) refinement, subnet refinement, and type refinement. Our work provides a formalisation in COQ [5] of both the abstract Petri net and the refined net, as well as refinement correction lemmas, together with the refinement correction proof.

In a previous work [4], we considered mainly place/transition Petri nets (sketching how coloured nets might be taken into account), and the subnet refinement (the node refinement processing being similar).

In this paper, we address coloured nets, which are more complex in nature, and the formalisation in COQ had to be significantly changed to take the typing issues into account. The *type refinement* formalisation and correction lemma are also addressed, thus pursuing the initial work of [4]. A protocol example adapted from [7] illustrates our work.

E. Denney, D. Giannakopoulou, C.S. Păsăreanu (eds.); The First NASA Formal Methods Symposium, pp. 156-165
*http://www-lipn.univ-paris13.fr/~lastname

This type refinement is interesting as it allows for specification of concrete and useful properties in practice. It requires a more complete formalisation, since colours (seen as types) are necessary. When compared to places/transitions nets, the use of colours lead to decrease the size of nets, leading to more amenable models.

The paper is structured as follows. Section 2 recalls the definitions of coloured Petri nets. Section 3 recalls the different refinements. Then, section 4 describes the case study (a protocol example) and formalisations for proving the type refinement of the net in this example. Conclusions and future work are finally discussed in section 5.

2 Coloured Petri nets definition

The definition of coloured Petri nets [8, 9] used in this paper is the following:

Definition 2.1 (Coloured Petri net)**.** *A Coloured Petri net $\mathscr{R}$ is an 8-tuple $\mathscr{R} = \langle P, T, A, C, E, \mathbb{M}, \mathbb{Y}, M_0 \rangle$ where:*

1. *P is a set of places*
2. *T is a set of transitions, such that $P \cap T = \emptyset$*
3. *A is a set of arcs, such that $A \subseteq (P \times T) \cup (T \times P)$*
4. *C: $P \cup T \rightarrow \Sigma$ where Σ is a universe of non-empty colour sets (or types), determines the colours of places and the transition modes.*
5. *E: $A \rightarrow \Phi\Sigma$ yields the arc inscriptions, such that $E(p,t), E(t,p)$: $C(t) \rightarrow \mu C(p)$*
6. *$\mathbb{M} = \mu\{(p,c) | p \in P, c \in C(p)\}$ is a set of markings, that associate a value c with a place p of P.*
7. *$\mathbb{Y} = \mu\{(t,c) | t \in T, c \in C(t)\}$ is a set of steps (multisets of transitions with their firing mode).*
8. *M_0 is the initial marking, $M_0 \in \mathbb{M}$.*

where $\Phi\Sigma$ is a function over Σ defined by $\Phi\Sigma = \{X \rightarrow Y \mid X, Y \in \Sigma\}$ and $\mu X = \{X \rightarrow \mathbb{N}\}$ are multisets over a set X, where $\mathbb{N}$ is the set of natural numbers.

In the example in Figure 1, the marking of place `PacketsToSend` is the multiset 1‘1++1‘2++1‘3++1‘4++1‘5++1‘6, where 1‘6 denotes one occurrence of value 6, and ++ denotes the multiset addition operator.

Definition 2.2. *[8] The incremental effects $E^+, E^- : \mathbb{Y} \rightarrow \mathbb{M}$ of the occurrence of a step Y are given by:*

1. *$E^-(Y) = \sum_{(t,m) \in Y} \sum_{(p,t) \in A} \{p\} \times E(p,t)(m)$*
2. *$E^+(Y) = \sum_{(t,m) \in Y} \sum_{(t,p) \in A} \{p\} \times E(t,p)(m)$*

E^- defines the input arc inscriptions while E^+ defines the output arc inscriptions.

Type refinement modifies the information carried by the tokens (a colour is a value of a token) while the net structure is unchanged. Type refinement brings additional information, which may be done e.g. by adding components in a tuple, or by representing an abstract data type by a more concrete one. The properties of the refined type should be preserved, that is if type A is refined by type B, then type B should satisfy the properties of A after an adequate syntactic translation. As for nets, it should always be possible to associate a behaviour of the abstract net with a behaviour of the refined one. Type refinement issue is associated with the issue of abstraction and implementation in the context of formal specifications (e.g. algebraic specifications [12]), and with studies on subtyping in the context of object-oriented programming languages [11, 3]. In this work (as in the work of Lakos [8, 9]), the type refinement considered is adding components in a tuple.

Since coloured Petri nets can use very general types and functions over these types which are thus not amenable, we here restrict ourselves to the *symmetric Petri nets* subclass. Symmetric nets are defined as coloured Petri nets that allow only the use of particular types and functions: enumerated types, booleans, integer intervals, tuples and combinations of these, as well as the associated functions. We actually also handle lists of such types that can easily be manipulated by the COQ theorem prover.

3 Definitions of refinements

As mentioned previously, Lakos and Lewis [8, 9] consider three kinds of Petri nets refinements, node (place or transition) refinement, subnet refinement, and type refinement. *Node refinement* consists in replacing a place (transition) by a place- (transition-) bordered subnet. *Subnet refinement* consists in adding net components (places, transitions and arcs or even additional tokens). In this section the definition of type refinement is recalled, and we give the corresponding correctness lemma. The lemmas for subnet and node refinements can be found in [4]. Very little work as been achieved concerning type refinement.

In the following definition of *type refinement* [8], $\mathscr{N}_a = \langle P,T,A,C,E,\mathbb{M},\mathbb{Y},M_0\rangle$ is the abstract net and $\mathscr{N}_r$ is the refined net.

Definition 3.1 (Type refinement)**.** *A morphism $\phi : \mathscr{N}_a \to \mathscr{N}_r$ is a* type refinement *if:*

1. *ϕ is the identity function on P, T, A, i.e. $\forall p \in P$: $\phi(p) = p$, etc.*
2. *$\forall x \in P \cup T$: $C(x) <: \phi(C)(x)$*
3. *$\forall x \in P \cup T$: $\forall c \in C(x)$: $\phi(1`(x,c)) = 1`(x,\Pi_{\phi(C)(x)}(c))$*
4. *$\forall (p,t) \in A$: $\forall (t,c) \in \mathbb{Y}$:*
   $\phi(E^-(1`(t,c)))(p) = \Pi_{\phi(C)(p)}(E(p,t)(c)) = \phi(E)(p,t)(\Pi_{\phi(C)(t)}(c))$
   $\forall (t,p) \in A$: $\forall (t,c) \in \mathbb{Y}$:
   $\phi(E^+(1`(t,c)))(p) = \Pi_{\phi(C)(p)}(E(t,p)(c)) = \phi(E)(t,p)(\Pi_{\phi(C)(t)}(c))$

The following interpretation will be used in section 4.2,

Lemma 3.2.

1. *The network structure (places, transitions and arcs) is kept unchanged, i.e. $P = P'$, $T = T'$, $uA = uA'$ where P', T' et uA' are resp. the sets of places, transitions and arcs (without their associated type) of the refined net while P, T and uA are those of the abstract net.*

2. *For any token* $1`(x',c')$*, of value* $x'$ *for colour* $c'$ *in the initial marking of the refined net, there exists a corresponding token* $1`(x,c)$ *in the initial marking of the abstract net. They must be such that both the sub-typing and projection relations (resp. denoted* $<_:$ *and* $\prod$*) are satisfied:* $c <_: c'$ *and* $c = \prod_c(c')$.

3. *The arc expressions are refined according to the token refinement:* $\prod_{C_r(p)}(C_a(arc)) = C_r(arc)(C_r(t))$.

According to the formal definition of type refinement in [10], the net structure is unchanged. Since type refinement consists in incorporating additional information in token values, a token type in the refined net is a subtype of the one in the abstract net.

4 Case study: the simple protocol

4.1 Description

In this section, the correction lemma is illustrated by a simple protocol example adapted from [7].

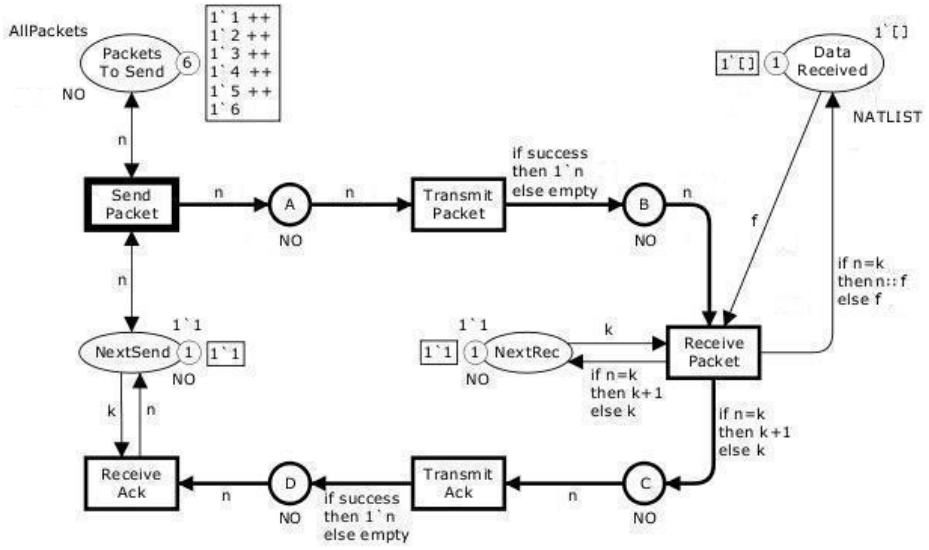

Figure 1: Example of a simple protocol

Figure 1 describes this simple protocol. The left-hand side part models the sender, the right-hand side the receiver while the middle part represents the network. The sender state is modelled by two places: *PacketsToSend* and *NextSend*. The receiver state is modelled by the *DataReceived* place. Places *A*, *B*, *C* and *D* constitute the network.

Note that place *PacketsToSend* is initially marked by six tokens with integer values. The textual inscriptions under a place is called "the colour set" of this place, which represents the available set of token colours. For example, the tokens in place *NextSend* always have an integer value. Here, the colour set `NO` is used to model sequence numbers. The inscription at the right top of place *NextSend* specifies that the initial marking of this place contains a single token with colour (value) 1. Informally, 1‘1 means that the data packet number 1 is to be sent. Finally, we will eventually obtain in place *DataReceived* a list of natural numbers: $[6,5,4,3,2,1]$. Let us note that arc expressions yield token values together with their multiplicity. However, when the multiplicity is 1, it is omitted, thus n denotes 1‘n.

This example is refined by associating additional information with tokens (while the net structure in terms of places and transitions is unchanged). The refined net is presented in Figure 2.

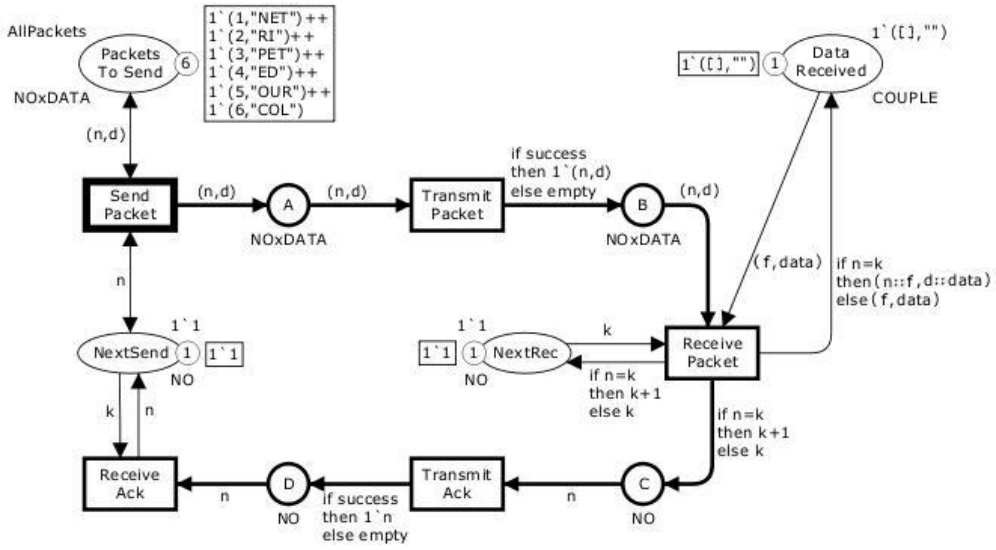

Figure 2: Refined protocol example

The colour sets of places *PacketsToSend*, *A*, *B* and *DataReceived* are extended from `NO` to `NO`×`DATA` which is defined as the cartesian product of the sets describing types `NO` and `DATA`. Note that here some places are not refined, e.g. *NextSend* is still of type `NO`.

The type refinement achieved in Figure 2 not only changes the type of tokens and places but also modifies the arcs expressions accordingly. Note that there exists a subtyping relation between e.g. (x) and $(x,1)$.

4.2 Formalisation and proof in Coq

The simple protocol example is now formalised. Tokens carry complex information, and several functions are required to certify the system. In this example, the arc expressions are of four possible types (all with an integer multiplicity).

nat $*$	(nat)
	(nat $*$ string)
	(list nat)
	(list nat $*$ string)

In Coq, these kinds of arcs are defined by an inductive type:

```
Definition nat_Tuple := list nat.

Inductive arc_type : Type :=
  |bi_types: nat*nat -> arc_type
  |tri_types: nat*(nat*string) -> arc_type
  |bi_n_tuples: nat*nat_Tuple -> arc_type
  |tri_tuples: nat*(nat_Tuple*string) -> arc_type.
```

Then, places and transitions are indexed by natural numbers:

```
Record Place : Type := mkPlace
        { Pr : nat }.

Record Transition : Type := mkTransition
        { Tr : nat }.
```

We now present an excerpt of the definitions of places, transitions and arcs for our example. Sets of places, transitions or arcs (both the untyped arc, i.e. the edge in the graph, and the arc expression) are represented by lists:

```
Definition P1_PackToSend := mkPlace 1.
...
Definition list_P:= P1_PackToSend::P2_A::P3_B::P4_NextRec::
                    P5_DataRec::P6_C::P7_D::P8_NextSend::nil.

Definition T1_SendPack := mkTransition 1.
...
Definition list_T:= T1_SendPack::T2_TransPack::T3_RecPack::
                    T4_TransAck::T5_RecAck::nil.

Definition uAP1T1 := (P1_PackToSend,T1_SendPack).
...
Definition AP1T1 := (P1_PackToSend,T1_SendPack,bi_types (1,1)).
...
Definition list_APT := AP1T1::AP2T2::AP3T3::AP4T3::AP5T3::
                       AP6T4::AP7T5::AP8T5::AP8T1::nil.
Definition list_ATP := AT1P2 ::AT2P3::AT3P4::AT3P5::AT3P6::
                       AT4P7::AT5P8::AT1P8::nil.
Definition list_ATP := uAT1P2...
...
Definition list_APT' := A'P1T1::A'P2T2::A'P3T3::A'P4T3::A'P5T3::A'P6T4::
                        A'P7T5::A'P8T5::A'P8T1::nil.
Definition list_ATP' := A'T1P2 ::A'T2P3::A'T3P4::A'T3P5::A'T3P6::
                        A'T4P7::A'T5P8::A'T1P8::nil.
```

The most interesting aspect of type refinement is due to arc expressions. Type refinement can be seen as a relation between types, which is subtyping. For example, the following table presents subtyping relations involved in our refinement of the simple protocol (note that the first line is unchanged by the refinement, and this still needs to be checked):

ARC EXPRESSIONS	EXAMPLE OF ARC VALUES	VALUE TYPE	COQ `arc_type`
if n=k then k+1 else k	1‘6	nat*nat	`bi_types`
n (n, d)	1‘6 1‘(6, ”COL”)	nat*nat nat*(nat*string)	`bi_types` `tri_types`
if n=k then n::f else f if n=k then (n::f, d::data) else (f, data)	1‘[6] 1‘([6], ”COL”)	nat*list nat nat*(list nat*string)	`bi_n_tuples` `tri_tuples`
f (f, data)	1‘[6]) 1‘(6, ”COL”)	nat*list nat nat*(list nat*string)	`bi_n_tuples` `tri_tuples`

The subtyping relation must be formalised for this example. We begin by defining a function `is_sub` which gives a relation between types of `arc_type`. This relation is then extended to tuples (`is_sub_tupl_apt`) and lists of tuples (`is_sub_l_apt`) for describing arcs from places to transitions. Similar extensions are defined for arcs from transitions to places.

```
Definition is_sub (subtyp:arc_type)(typ:arc_type) : Prop :=
  match subtyp, typ with
  | (bi_types _), (bi_types _) => True
  | (tri_types _), (bi_types _) => True
  | (tri_tuples _), (bi_n_tuples _) => True
  | _, _ => False
  end.

Definition is_sub_tupl_apt (subtupl: Place * Transition * arc_type)
           (tupl: Place * Transition * arc_type) : Prop :=
           (is_sub (snd subtupl) (snd tupl)).

Fixpoint is_sub_l_apt (subl: list (Place * Transition * arc_type))
         (l: list (Place * Transition * arc_type)) {struct subl} : Prop :=
    match subl, l with
     | nil, nil => True
     | (cons a tla), (cons b tlb) =>
             (is_sub_tupl_apt a b) /\ (is_sub_l_apt tla tlb)
     | _, _ => False
    end.
```

The type refinement correctness lemma can now be written, with the help of lemma 3.2 (where, for the sake of readability, we indicate in parenthesis to which item the COQ code relates):

```
Lemma type_colour_refined:
      eqlist Place list_P list_P' /\                        (1.)
      eqlist Transition list_T list_T' /\                   (1.)
      eqlist (Place*Transition) list_uAPT list_uAPT' /\     (1.)
      eqlist (Transition*Place) list_uATP list_uATP' /\     (1.)
      eqlist (list (nat*nat)) list_MP (hd_list list_MP')/\ (2.)
      is_sub_l_apt list_APT' list_APT /\                    (3.)
      is_sub_l_atp list_ATP' list_ATP.                      (3.)
```

where `eqlist` is an equality between lists and $l = l'$ is equivalent to $l \subseteq l'$ and $l' \subseteq l$, `list_MP` and `list_MP'` define the initial markings, and function `hd_list` is defined as follows:

```
Fixpoint hd_list_couple (l:list (nat*(nat*string))):=
     match l with
       | nil=>nil
       |(a,(b,c))::tl=>(a,b)::(hd_list_couple tl)
     end.

Fixpoint hd_list (l:list (list (nat*(nat*string)))):=
      match l with
        |nil=>nil
        |a::tl=>(hd_list_couple a)::(hd_list tl)
      end.
```

Thanks to our simple and general formalisation, the formal correctness proof is almost automatic.

```
Proof.
repeat split;unfold incl;tauto.
Qed.
```

Note that this simple formalisation was obtained after carefully studying different possibilities for encoding Petri net elements in COQ. These are detailed in [4]. Moreover, the proof could be simplified using powerful constructs such as the `split` tactic, which is particularly well-suited for our purposes. This tactic applies to inductive types with a single constructor, which is the case for the `/\` operator in the lemma `type_colour_refined`.

When the proof fails, it still gives valuable information w.r.t. the refinement to be proven: either the lists representing the net graph elements (places, transitions, or edges) do not match, and the refinement relation does not hold ; or the error occurs when examining arc expressions. It may then be the case that refinement does not hold, but also that the type refinement between the supposedly refined and abstract arc expression cannot be automatically proven.

The full development is available at `http://www-lipn.univ-paris13.fr/~mayero/CPNCoq/Jensen_protocol_NFM.v`.

5 Conclusion

When modelling and validating critical systems, one often proceeds in a step-by-step fashion: a first abstract model is designed and validated ; it is then refined so as to take into account additional details ; and this process is repeated as many times as necessary. In order to guarantee that the behaviour of the system is preserved by refinement, it should obey some rules. Three kinds of refinements of coloured Petri nets were formally defined in [9]. Our aim here was to show that the proof of refinement — i.e. that a refined net actually is a refinement of an abstract net — can be automated using theorem-proving techniques, thus avoiding error-prone and lengthy manual proofs.

Previous work focussed on two kinds of refinements: node refinement and subnet refinement, while the third one was scarcely mentioned. This paper has shown that when restricting coloured Petri nets to an appropriate subclass, type refinement can also be handled.

This work confirms that our choices of formalisation, made in [4], are suitable. The prerequisite to the refinements is the formalisation of a given Petri net. This formalisation is probably the most tedious part of our work and requires a significant automation. Since the refinement issues we tackle are meant to be integrated within a step-by-step modelling process, the refined net should be designed by the user starting from the abstract net. Therefore, places and transitions that are in both nets should remain exactly the same and can be identified by their name. Hence, we do not address the problem of proving that a net is a refinement of another one, starting from arbitrary nets.

The possibility to easily integrate automation at a later stage was a key issue in the work presented in this paper. For example, as seen in section 4, to define all the places, all the transitions and all the arcs manually is certainly not efficient, especially if the net has more than 50 places/transitions.

We plan to solve this problem using an interface to PNML (Petri Net Markup Language, [2]). PNML is currently being standardised within ISO/IEC 15909-2. It aims at becoming the common language for Petri nets tools, e.g. CPN-AMI [1], CPN-Tools [6] or other tools supporting Petri nets. Such files can be directly translated into COQ to generate the places, transitions and arcs.

We think that our method scales up rather well. Indeed, the proof is generic and does not change with the nets considered. The only modifications are sub-typing relations and type definitions. Moreover, when proceeding step-by-step, refinements are applied one at a time. Therefore, the nets to be considered are only slightly different.

To complete this work, we should consider refinement as part of a modular design process. In such a framework, a type refinement can affect several modules which could be checked separately for refinement, and one must ensure that type refinement has been applied consistently in all modules.

Acknowledgments Implementation of this work in COQ was achieved with the help of Yibei Yu, a trainee supervised by the authors.

References

[1] CPN-AMI*: Home Page*. `http://www-src.lip6.fr/logiciels/mars/CPNAMI/`.

[2] J. Billington, S. Christensen, K. van Hee, E. Kindler, O. Kummer, L. Petrucci, R. Post, C. Stehno, and M. Weber. The Petri Net Markup Language: Concepts, technology and tools. In *Proc. 24th Int. Conf. Application and Theory of Petri Nets (ICATPN'2003), Eindhoven, The Netherlands, June 2003*, volume 2679 of *Lecture Notes in Computer Science*, pages 483–505. Springer, 2003.

[3] Luca Cardelli and Peter Wegner. On understanding types, data abstraction, and polymorphism. *ACM Comput. Surv.*, 17(4):471–522, 1985.

[4] Christine Choppy, Micaela Mayero, and Laure Petrucci. Experimenting Formal Proofs of Petri Nets Refinements. *Electr. Notes Theor. Comput. Sci.*, 214:231–254, 2008.

[5] *The Coq proof assistant*. `http://coq.inria.fr`.

[6] *cpntools*. `http://wiki.daimi.au.dk/cpntools/cpntools.wiki`.

[7] Kurt Jensen and Lars M. Kristensen. *Coloured Petri Nets, Modelling and Validation of Concurrent Systems*. Monograph to be published by Springer Verlag, 2008.

[8] Charles Lakos. Composing abstractions of coloured Petri nets. In Nielsen, M. and Simpson, D., editors, *Lecture Notes in Computer Science: 21st International Conference on Application and Theory of Petri Nets (ICATPN 2000), Aarhus, Denmark, June 2000*, volume 1825, pages 323–345. Springer-Verlag, 2000.

[9] Charles Lakos and Glen Lewis. Incremental state space construction of coloured Petri nets. In *Proc. 22nd Int. Conf. Application and Theory of Petri Nets (ICATPN'01), Newcastle, UK, June 2001*, volume 2075 of *Lecture Notes in Computer Science*, pages 263–282. Springer, 2001.

[10] Glen Lewis. *Incremental specification and analysis in the context of coloured Petri nets*. PhD thesis, University of Hobart, Tasmania, 2002.

[11] Barbara Liskov and Jeannette M. Wing. A new definition of the subtype relation. In *ECOOP '93: Proceedings of the 7th European Conference on Object-Oriented Programming*, pages 118–141, London, UK, 1993. Springer-Verlag.

[12] Fernando Orejas, Marisa Navarro, and Ana Sanchez. Algebraic implementation of abstract data types: a survey of concepts and new compositionality results. *Mathematical Structures in Computer Science*, pages 33–67, 1996.