Compositional Synthesis of Live and Bounded Free Choice Petri Nets [1]

Javier Esparza
Institut für Informatik, Universität Hildesheim
Samelsonplatz 1, D-3200 Hildesheim (FRG)
e-mail:esparza@infhil.uucp

Manuel Silva
Depto. Ingeniería Eléctrica e Informática
Universidad de Zaragoza
C/ María de Luna 3, E-50015 Zaragoza (Spain)
e-mail:silva@etsii.unizar.es

Abstract. The paper defines two notions of composition of concurrent modules modelled by means of Petri nets: *synchronisations* and *fusions*. We study these two notions for the class of Free Choice nets, and characterise the compositions (within this class) that preserve liveness (absence of partial or global deadlocks) and boundedness (absence of overflows in finite stores). The characterisation shows which structures must be avoided in order to preserve the properties.

Keywords. Petri nets, Free Choice nets, compositional synthesis, liveness, boundedness.

1 Introduction

The development of compositional techniques for the analysis and synthesis of concurrent systems is an active field of research. This paper deals with this problem for systems modelled by means of Petri Nets. In particular, our goal is to give, for interesting composition operators, necessary and sufficient conditions on the structure of the net for the preservation of two properties: *liveness* and *boundedness*. Liveness is defined as the absence of partial or global deadlocks (from every reachable state all actions can

[1]This work was partially supported by the DEMON Esprit Basic Research Action 3148 and the Spanish Plan Nacional de Investigación, Grant TIC-0358/89.

be executed again). Boundedness means finiteness of the state space, and can be also interpreted as the absence of overflows in finite stores such as buffers.

However, the obtention of these conditions for general Petri Nets is an exceedingly ambitious goal, because the interplay between nondeterminism - choices - and concurrency makes very difficult to find relationships between the behaviour of a system and the structure of the net that models it. That is why we consider here the subclass of Free Choice nets (FC), in which this interplay is restricted: in FC nets, choices are not influenced by the environment, a concept similar to the internal nondeterminism of TCSP. This subclass has been studied in [BD 90,Hack 72,TV 84] among other papers.

Recently, [ES 90] gave a first complete theory for the *top-down* synthesis of live and bounded FC systems, which was subsequently used in [Espa 90] to derive new properties. In this work, we present a compositional synthesis theory for the class of nets underlying this class of systems: actually, the free choice nets that are structurally live and structurally bounded (SL&SB for short). In other words, we abstract from the initial markings. However, this is not a heavy constraint, since the markings that make these nets live and bounded can be easily calculated.

We start introducing two notions of composition: *synchronisations* and *fusions*. Synchronisations essentially merge transitions: they are closely related to the parallel operator of process algebras. Fusions, on the other hand, essentially merge places. We introduce later the concept of *well formed FC-synchronisations* as those preserving the free choice property (i.e. if the components of the synchronisation are FC so is the final result), and satisfying an additional graph theoretical condition. We show that an FC-synchronisation is SL&SB if and only if it is well formed.

This characterisation in terms of graph theoretical properties can be called "low level", since it is close to the graph structure of nets but difficult to interpret. We show that it is equivalent to a "high level" characterisation, which consist of the absence of two structures in the composed net, called *killing choices* and *synchronic mismatches*. These two structures have a clear and intuitive meaning.

Finally, we use the Duality Theorem of FC nets to derive for fusions similar results to the ones obtained for synchronisations.

Section 2 introduces the concepts of synchronisation and fusion. Sections 3 and 4 present the "low level" and "high level" characterisations of SL&SB FC-synchronisations. In section 5 the correspondent results for fusions are derived.

The basic definitions of net theory relevant for the paper can be found in [Espa 90]. For full proofs the reader is referred to [Espa 90b].

2 Composition of nets: Synchronisations and Fusions

To define synchronisations and fusions, we introduce the notions of *isomorphic* nets and *composition*.

Definition 2.1 *Two nets* $N_a = (P_a, T_a, F_a)$ *and* $N_b = (P_b, T_b, F_b)$ *are* isomorphic *iff there exists a bijection* $h: P_a \cup T_a \cup F_a \to P_b \cup T_b \cup F_b$ *such that:*

$h(P_a) = P_b, h(T_a) = T_b, h(F_a) = F_b$

- $\forall (x,y) \in F_a: h((x,y)) = (h(x), h(y))$ ▪ 2.1

Definition 2.2 *Let* $\{N_1, \ldots, N_k\}$ *be a finite set of nets.* $N = (P, T, F)$ *is a* composition *of* $\{N_1, \ldots, N_k\}$ *iff:*

(a) there exists a set $\{\hat{N}_1, \ldots, \hat{N}_k\}$ *of subnets of* N *such that* $\forall i, 1 \leq i \leq k : N_i$ *is isomorphic to* $\hat{N}_i$

(b) $\cup_{i=1}^{k} \hat{N}_i = N$

The nets $N_1, \ldots, N_k$ *are* components *of* N. ▪ 2.2

The notion of composition is too general: very little can be said about the behaviour of the composition from the behaviours of the components. We consider now particular compositions with a better interpretation.

Definition 2.3 *A composition* N *of* $\{N_1, \ldots, N_k\}$ *(under isomorphisms* $h_1, \ldots h_k$*) is a* synchronisation *iff*

$$\forall i, 1 \leq i \leq k, \ \forall p \in \hat{P}_i: {}^\bullet p \cup p^\bullet \subseteq \hat{T}_i$$

N *is a* fusion *iff*

$$\forall i, 1 \leq i \leq k, \ \forall t \in \hat{T}_i: {}^\bullet t \cup t^\bullet \subseteq \hat{P}_i$$

where the dot notation refers to N. ▪ 2.3

Figure 1 shows a composition, a synchronisation and a fusion of two small nets. The drawing conventions are as follows. In the net composed by other two:

white nodes belong to the first component but not to the second.

shaded nodes belong to the second component but not to the first.

dashed nodes belong to both components.

These conventions are used again in section 4.

Loosely speaking, the isomorphisms of synchronisations "preserve" the environment of places, while the isomorphisms of fusions "preserve" the environment of transitions. This means that the communication between the components is done through transitions in the case of synchronisations, and through places in the case of fusions. The first corresponds to communication by means of rendez-vous, and the second to the case

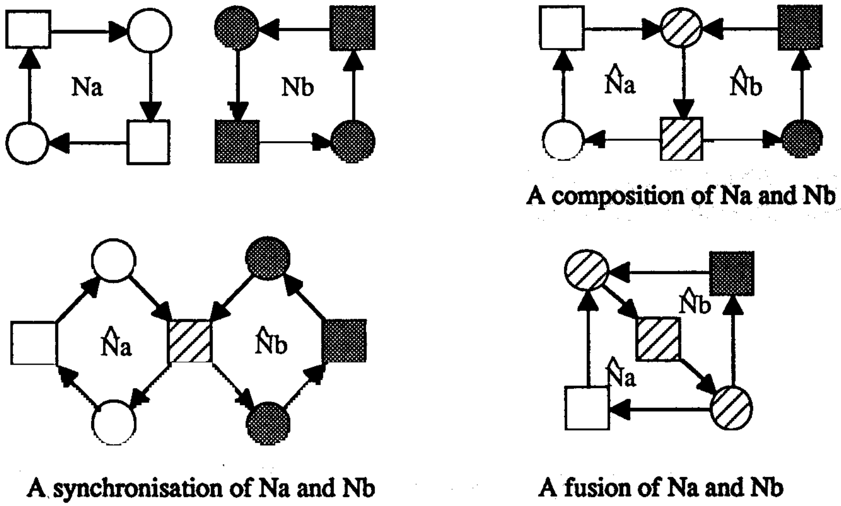


Figure 1: A composition, a synchronisation and a fusion of two small nets.

in which the components share some kind of resource, such as local memory, or share certain states.

In the sequel we consider only compositions of two nets. This is not an important restriction, because any composition of k nets can be done in a stepwise way composing first two nets N_1 and N_2, then composing the obtained net with N_3 and so on, that is, dividing it into $k-1$ compositions of two nets. The definitions are given from this point on for two nets, though theirs extension to the general case is always straightforward. We also change the notation, and denote the two components of the composition by N_a and N_b.

We are interested in the study of synchronisations producing FC nets, that we call *Free Choice Synchronisations.*

Definition 2.4 *A synchronisation N of $\{N_a, N_b\}$ is a* Free Choice synchronisation *(FC-synchronisation for short) iff N is FC.* ∎ 2.4

Free Choice synchronisations admit the following more useful characterisation, which follows easily from the definitions.

Proposition 2.5 *Let N be a synchronisation of $\{N_a, N_b\}$. N is a Free Choice synchronisation iff the two following conditions hold:*

(a) N_a and N_b are FC nets

(b) For every transition t in N: $({}^\bullet t \cap (P_a \setminus P_b) \neq \emptyset \wedge {}^\bullet t \cap (P_b \setminus P_a) \neq \emptyset) \Rightarrow ({}^\bullet t)^\bullet \subseteq \{t\}$.

Proof: It is easy to show that a net is Free Choice iff for all transitions t: $|{}^\bullet t| > 1 \Rightarrow ({}^\bullet t)^\bullet = \{t\}$.

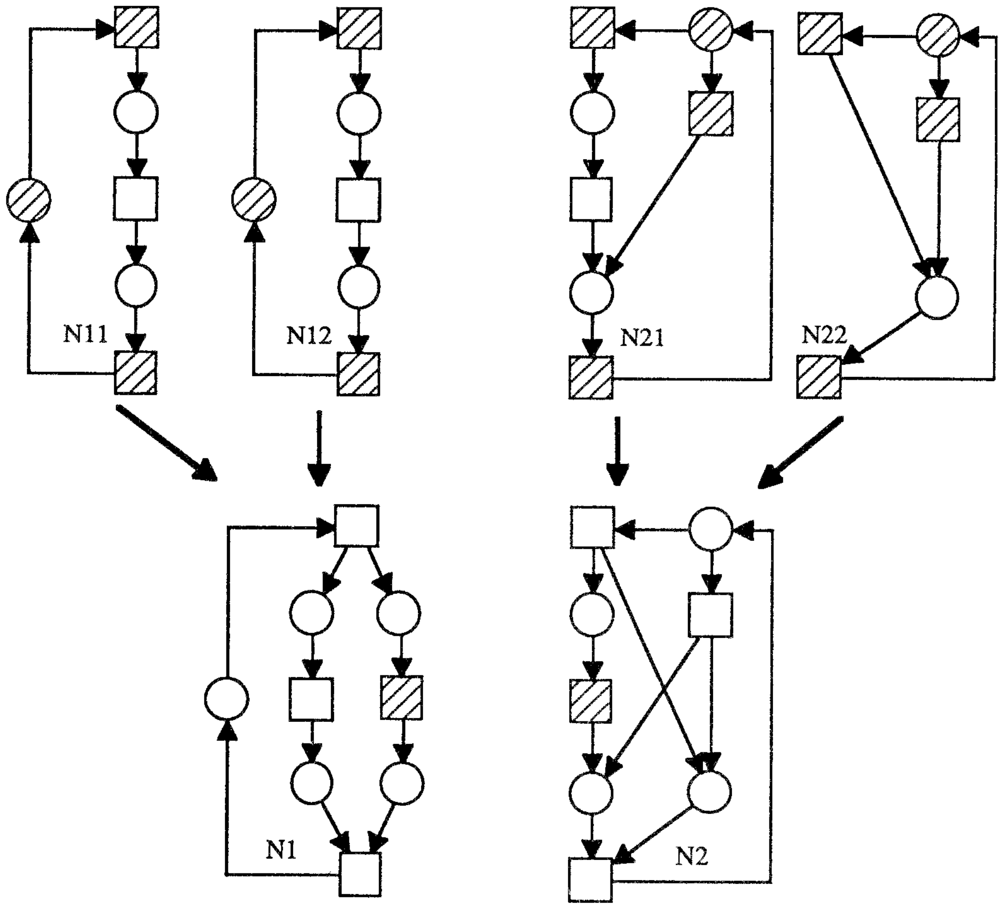


Figure 2: A synchronisation of four nets.

($\Rightarrow$) Assume N is Free Choice. (a) is obvious. To prove (b), notice that $({}^\bullet t \cap (P_a \setminus P_b) \neq \emptyset \wedge {}^\bullet t \cap (P_b \setminus P_a) \neq \emptyset)$ implies $|{}^\bullet t| > 1$.

($\Leftarrow$) Assume (a) and (b) hold. Take a transition t of N such that $|{}^\bullet t| > 1$. If ${}^\bullet t \subseteq P_a$, by the definition of synchronisation, $({}^\bullet t)^\bullet \subseteq T_a$. Since N_a is FC by (a), we have $({}^\bullet t)^\bullet = \{t\}$. Similarly if ${}^\bullet t \subseteq P_b$. If neither ${}^\bullet t \subseteq P_a$ nor ${}^\bullet t \subseteq P_b$, we have again $({}^\bullet t)^\bullet = \{t\}$ by (b). ■ 2.5

Figure 2 shows how an FC net can be constructed stepwisely by means of succesive FC-synchronisations. The four initial nets, N_{11}, N_{12}, N_{21}, N_{22}, are strongly connected state machines. N_{11} and N_{12} are synchronised to yield N_1 (the nodes identified by the isomorphisms are shaded). Analogously, N_{11} and N_{12} yield N_2. Finally, N_1 and N_2 are synchronised to yield N (not shown in the figure).

3 Well Formed Free Choice Synchronisations

Our goal is to characterise in structural terms (i.e. through conditions on the graph structure of the net) the FC-synchronisations of two SL&SB nets that are also SL&SB. In fact, it is easy to show that structural boundedness is given for granted.

Proposition 3.1 *Let N_a, N_b be two SL&SB nets, and N a synchronisation of $\{N_a, N_b\}$. Then N is also structurally bounded.*

Proof: (sketch) Let p be a place of N. Assume w.l.o.g. that $p \in P_a$. Let M be an arbitrary marking of N, and M_a its projection on N_a. It is easy to see that the language of (N, M) projected on the transitions of N_a is a subset of the language of (N_a, M_a). Since N_a is structurally bounded, p is bounded in (N_a, M_a). Due to the language inclusion, p is also bounded in (N, M). Since p and M are arbitrary, the result follows. ∎ 3.1

The difficulty lies in characterising which are the structurally live FC-synchronisations. We show in this section that they are exactly the *well formed* FC-synchronisations. In order to introduce them, we need to define first two structures: handles [ES 89], and T-components [Hack 72].

Definition 3.2 *Let N be a net and $N' \leq N$ a partial subnet of N. An elementary path $(x_1, \ldots, x_r)$ in N, $r \geq 2$, is a* handle *of N' iff $\{x_1, \ldots, x_r\} \cap (P' \cup T') = \{x_1, x_r\}$. It is also said that N'* has *a handle $(x_1, \ldots, x_r)$.* ∎ 3.2

The reason of the name is its graphical appeal, which can be appreciated in figure 3. The reader should not confuse our handles with the ones defined in [GJRT 83] for the study of graph grammars.

The character of a handle is determined by the nature (place or transition) of its first and last nodes. We classify them according to this criterion into four subclasses: *PP-*, *PT-*, *TP-* and *TT-handles* (see figure 3). The meaning is obvious.

The intuition lying behind figure 3 is that, when constructing a system through the iterative addition of handles, PP- and TT-handles are nicer for preserving liveness and boundedness than PT- or TP-handles, which "create problems" that have to be solved.

T-components are structures associated to the infinite behaviours of the net.

Definition 3.3 *Let $N = (P, T, F)$ be a net. A strongly connected T-graph $N_1 = (P_1, T_1, F_1) \subseteq N$ is a T-component of N iff $P_1 = {}^\bullet T_1 = T_1^\bullet$, where the dot notation refers to N.* ∎ 3.3

The basic property of T-components is that an occurrence sequence in which only the transitions of the T-component occur, and they occur exactly once, reproduces the original marking. Therefore, such a sequence can be executed infinitely many times.

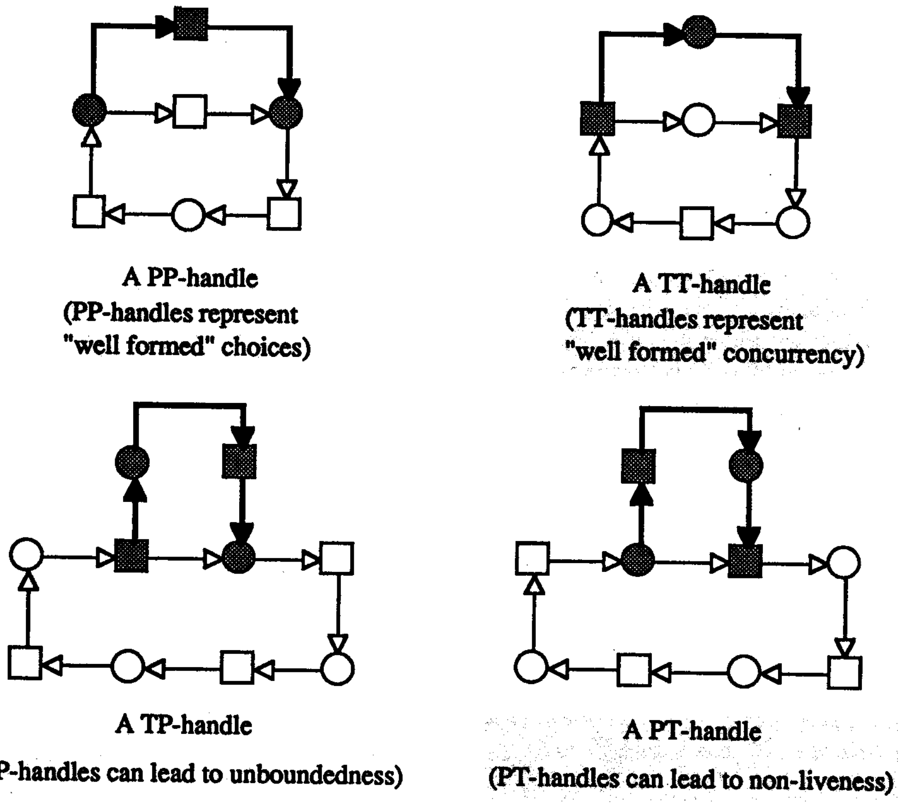


Figure 3: The four classes of handles.

Proposition 3.4 *Let (N, M_0) be a system and $N_1 = (P_1, T_1, F_1)$ a T-component of N. If there exists a sequence σ such that*

$$\vec{\sigma}(t) = \begin{cases} 1 & \textit{if } t \in T_1 \\ 0 & \textit{otherwise} \end{cases}$$

then $M_0[\,\sigma\rangle M_0$. ■ 3.4

We can now define well formed FC-synchronisations.

Definition 3.5 *Let N_a and N_b be two SL&SB nets. N is a* well formed FC-synchronisation *of $\{N_a, N_b\}$ iff no T-component of N_a or N_b has a TP-handle in N.* ■ 3.5

Using the following proposition, it is not difficult to prove that SL&SB FC-synchronisations must be well formed:

Proposition 3.6 *Let N be an FC net and $N' \leq N$ a strongly connected T-graph with a TP-handle in N. Then N is not SL&SB.*

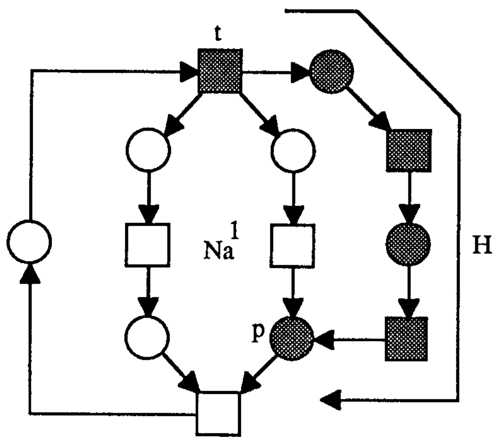


Figure 4: Illustration of the definition of well formed synchronisation.

Proof: (sketch) The result is a slight generalisation of [Dese 86]. It is proven there for the case in which N' is an elementary circuit. It is not difficult to see that whenever N contains a strongly connected T–graph with a TP–handle, it also contains an elementary circuit with the same property. ∎ 3.6

Since a T–component of N_a or N_b is a strongly connected T–graph of N, it follows that a non well formed FC–synchronisation cannot be *SL&SB*. We would like to give an informal argument to make this result plausible. Let N_1^a be a T–component of N_a with a TP–handle $H = (t, \ldots, p)$ in N. The intuitive idea is to use a policy for the occurrence of transitions. Denote by $N_1^a \cup H$ the net composed by N_1^a and H (see figure 4). Let p' be any place in $N_1^a \cup H$. Whenever one of its output transitions is enabled, *all* its output transitions are enabled because the net is Free Choice. The policy consists of always letting the transition in $N_1^a \cup H$ occur. Assume that the system is live. It can be proved that occurrence sequences exist which respect this policy and let t occur arbitrarily many times. These occurrence sequences increase arbitrarily the total number of tokens in the places of $N_1^a \cup H$. Hence, the system is not bounded for these markings, which contradicts proposition 3.1.

Well formedness is not only a necessary condition but also characterises SL&SB FC–synchronisations of SL&SB components:

Theorem 3.7 *Let N be an FC-synchronisation of $\{N_a, N_b\}$, where N_a and N_b are SL&SB. N is SL&SB iff it is well formed.*

Proof: (hint)

(⇒) See above.

(⇐) The proof is long and quite hard. It has two parts. First the result is proven for the particular case in which N_a is a strongly connected P–graph. It is shown that, if N is well formed, then it can be reduced to N_b using the reduction algorithm of [ES 90]. Since this reduction procedure preserves SL&SB and N_b is SL&SB by hypothesis, it follows that N is SL&SB. Using this first result, the general case is proven by means of a graph argument. ∎ 3.7

The reader can check that all the FC-synchronisations performed to obtain the net N of figure 2 are well formed, and that the resulting net is SL&SB.

We finish this section with two results. The first shows that every SL&SB FC net can be obtained through well formed synchronisations of strongly connected P-graphs (i.e. well formed synchronisations are, in some sense, complete).

We need introduce first the notion of P-component of a net.

Definition 3.8 *Let $N = (P, T, F)$ be a net. A strongly connected P-graph $N_1 = (P_1, T_1, F_1) \subseteq N$ is a P-component of N iff $T_1 = {}^\bullet P_1 = P_1^\bullet$, where the dot notation refers to N.* ∎ 3.8

Proposition 3.9 *Let N be an SL&SB FC net. There exists a set $\{N_1, \ldots, N_k\}$ of strongly connected P-graphs and a sequence $\{N^1, \ldots, N^k\}$ of nets such that:*

(1) $N^1 = N_1$

(2) $\forall i, 1 < i \leq (k-1)$: N^{i+1} *is a well formed FC-synchronisation of* $\{N^i, N_i\}$

(3) $N^k = N$.

Proof: (sketch) By a well known result [Hack 72], every node of N belongs to some P–component. The nets N_1 to N_k are chosen isomorphic to some minimal set of P–components that cover the net. This guarantees that N can be obtained by synchronising N_1 to N_k. The result follows then from an important monotonicity property: if N^i is not SL&SB, then N^{i+1} is also not SL&SB. Now, if the synchronisation of $\{N^i, N_i\}$ were not well formed, N^{i+1} would not be SL&SB and, by the monotonicity result, neither would be N, against the hypothesis. ∎ 3.9

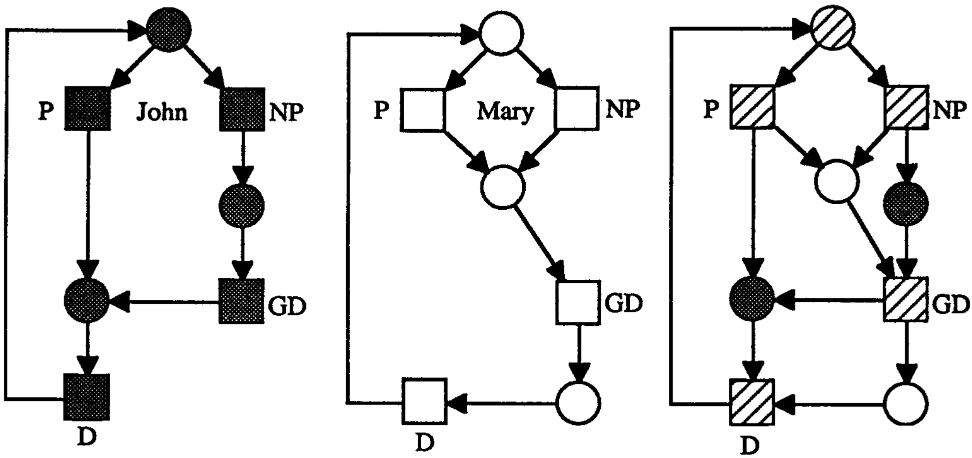
The net N of figure 2 can be obtained by synchronising first N_{11} and N_{12}, and synchronising then the result with N_{21} and N_{22} succesively.

The second result characterises, by means of a simple structural condition, the set of markings that make an SL&SB FC net live and bounded. This shows that by considering the structural problem first we did not impose a strong constraint.

Theorem 3.10 *Let N be an SL&SB FC net. (N, M_0) is live and bounded iff for every P-component $N_1 = (P_1, T_1, F_1)$ of N, at least one place of P_1 is marked at M_0.*

Proof: (hint) Follows from Commoner's theorem [Hack 72] and lemma 6.10 of [BT 87]. ∎ 3.10

The condition of theorem 3.10 can be checked in polynomial time by means of a graph algorithm.



NP: do Not Play tennis
P: Play tennis
GD: Go Dancing
D: have a Drink

Figure 5: The pair of transitions (P, GD) is a synchronic mismatch.

4 High-level characterisation of structurally well-formed synchronisations

The definition of well formed synchronisations has one strong and one weak point. The strong point is its simplicity and suitability for calculations. The weak point, its absence of "meaning". If it is shown that a certain synchronisation is not well formed, the definition sheds no light on which kind of design error was committed. Due to this reason, we characterise here well formed synchronisations from a "high-level" point of view, by means of more complex structures in the graph theoretical sense, but closer to design concepts. In fact, we show that there are only two "bad structures" or structural design errors that may cause an FC-synchronisation to be non well formed.

Synchronic mismatches. In order to introduce this first design error, consider the two nets on the left of figure 5. They model the behaviour of John and Mary, two millionaires of Palm Beach. Every day John decides whether he will play tennis or not. If he does not play tennis, he goes dancing and then has a drink. If he does play tennis, then he is too tired to go dancing and just drinks. After the drink a new day comes and everything starts again.

Also Mary decides every day to play tennis or not. But, since she is in better shape than John, she always goes dancing after, and then has the drink. The question is: if John and Mary get married, and want to play tennis, go dancing and drink together, can the marriage reach a deadlock? The marriage corresponds to the FC-synchronisation on the right of the figure, and it is easy to see that the system can deadlock. The reason is that John can execute the action "do play tennis" an arbitrarily large number of times without executing "go dancing", while Mary cannot. Since the occurrence dependences of these two actions are different for the two components of the synchronisation we say that they do not "match".

To formalize the above problem, let us introduce a *synchronic relation.* Synchronic relations [Silv 87] are used to study dependences between the occurrences of transitions.

Definition 4.1 *Let (N, M_0) be a system with $N = (P, T, F)$ and $t_1, t_2 \in T$. We define the following relations over $T \times T$:*

(1) (t_1, t_2) *is in* k-bounded deviation relation *in* (N, M_0) *iff* $\forall M \in [M_0\rangle$ *and* $\forall \sigma$ *applicable at* M *(i.e.* $M[\sigma\rangle$*):* $\vec{\sigma}(t_2) = 0 \Rightarrow \vec{\sigma}(t_1) \leq k$.

(2) (t_1, t_2) *is in* bounded deviation relation (BD-relation) *in* (N, M_0) *iff* $\exists k \in I\!N$ *such that* (t_1, t_2) *is in* k*-bounded deviation relation.*

Let now $N = (P, T, F)$ *be a net and* $t_1, t_2 \in T$.

(3) (t_1, t_2) *is in* structural BD-relation *in* N *iff* $\forall M_0$: (t_1, t_2) *are in BD-relation.* ▪ 4.1

Definition 4.2 *Let* N *be a synchronisation of* $\{N_a, N_b\}$ *and* $t_i, t_j \in T_a \cap T_b$. (t_i, t_j) *is a* synchronic mismatch *iff it is in structural BD-relation in one and only one of* N_a, N_b.
▪ 4.2

In the case of John and Mary, the pair (P, GD) is in the structural BD-relation of Mary but not in the one of John. The pair is hence a synchronic mismatch.

Proposition 4.3 *Let* N *be an FC-synchronisation of* $\{N_a, N_b\}$*, where both* N_a*,* N_b *are SL&SB. If* N *contains a synchronic mismatch, then* N *is not SL&SB.*

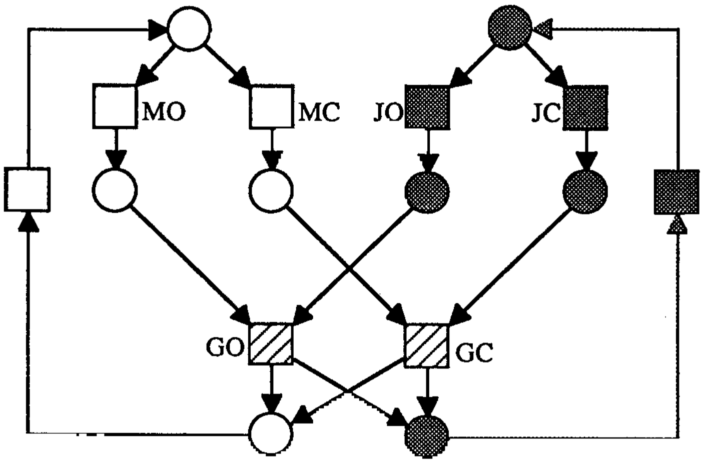
Proof: (sketch) Assume w.l.o.g. that (t_i, t_j) is in the structural BD-relation for N_a but not for N_b. Using a result of [Silv 87], we have:

every T-component of N_a containing t_i contains also t_j

there exists a T-component N_b^1 of N_b that contains t_i but not t_j.

The proof is carried out by showing that N_b^1 has a TP–handle in N. Then, N is not well formed and by theorem 3.7 not SL&SB. It is proved that:

There is an elementary path Π in N_a leading from a transition t of N_b^1 to t_j, such that its only node in N_b^1 is t.
This part is non trivial. See [Espa 90b].



MO / JO: Mary / John decides to go to the Odeon
MC / JC : Mary / John decides to go to the Capitol
GO: John and Mary go to the Odeon
GC: John and Mary go to the Capitol

Figure 6: The two places on the top are killing choices.

- There is an elementary path Π' in N_b leading from t_j to a place p of N_b^1, such that its only node in N_b^1 is p.

  Since N_b is SL&SB, it is strongly connected [Best 87]. This guarantees the existence of an elementary path in N_b leading from t_j to a node of N_b^1, with only its last node in N_b^1. This last node is a place because N_b^1 is a T–component of N_b.

The TP–handle can be extracted from the concatenation of Π and Π'. ■ 4.3

Killing choices. In order to introduce the second error, let us go back to John and Mary. They have changed of hobbies, and like now to go to the cinema every day. There are two cinemas for millionaires in Palm Beach, the "Odeon" and the "Capitol". John decides each day which of the two cinemas he wants to go to, and so does Mary.

John and Mary want to get married and go to the cinema together, but both want to decide, without consulting the other, which of the two cinemas they will go to. The corresponding synchronisation is shown in figure 6. Notice that the net contains no synchronic mismatches, but nevertheless leads to a deadlock for any marking. The deadlock is produced by the fact that the choices of John and Mary are *private*, but *concern the partner*. It is intuitively reasonable that these choices lead to non liveness for any marking. We call them *killing choices*.

Definition 4.4 *Let N be a FC-synchronisation of $\{N_a = (P_a, T_a, F_a),\ N_b = (P_b, T_b, F_b)\}$. A place $p \in P_a$ is a* killing choice *of N_a iff the following three conditions hold:*

(a) $p \notin P_b$

(b) There exists a T-component N_a^1 of N_a containing p and a transition $t_i \in T_a \cap T_b$.

(c) There exists an elementary path $B = (p, \dots, t_j)$, $t_j \in T_a \cap T_b$, such that p is the only node of N_a^1 in B.

A killing choice of N_b is defined analogously. N contains a killing choice *iff it contains a killing choice of N_a or a killing choice of N_b.* ∎ 4.4

Notice that p is a place with more than one output transition, because it has at least one output transition in the T-component and another one out of it. In fact, N_a can decide freely at p whether the tokens are kept in the T-component or are taken out of it. The reader can check that the two top places of the net of figure 6 are killing choices.

We obtain the following result:

Proposition 4.5 *Let N_a and N_b be two SL&SB FC nets and N be an FC-synchronisation of $\{N_a, N_b\}$. If N contains a killing choice, then N is not SL&SB.*

Proof: (sketch) Assume w.l.o.g. that N contains a killing choice p of N_a. By definition, there exists a T-component N_a^1 of N_a containing p and t_i, but not t_j (where t_i, $t_j \in T_a \cap T_b$). The definition of killing choice does not impose further requirements on t_i , t_j. Nevertheless, it is inmediate to see the following:

- t_i can be chosen such that there exists an elementary path $\Pi = (t_i, \dots, p)$ of N_a^1 whose only node in N_b is t_i.
- t_j can be chosen such that the only node of the path B in N_b is t_j (where B is the path required by the definition of killing choice).

As N_b is SL&SB, a well known result states that there exists a T–component of N_b containg t_i [Best 87]. Consider two cases:

Case 1. Every T-component of N_b containing t_i contains t_j.

In this case, N contains a synchronic mismatch and by proposition 4.3 it is not well formed.

Case 2. There exists a T-component N_b^1 of N_b that contains t_i but not t_j.

In this case, the concatenation of Π and B is an elementary path leading from N_b^1 to t_j whose only node in N_b^1 is t_i. Since N_b is SL&SB, it is strongly connected [Best 87]. Therefore there exists a path B' in N_b from t_j to N_b^1 whose only node in N_b^1 is the last one. This last node is a place because N_b^1 is a T-component of N_b. A TP-handle of N_b^1 can be extracted from the concatenation of Π, B and B'.

∎ 4.5

The completeness theorem. Killing choices and synchronic mismatches are structures that correspond to our intuitions of bad designs in the construction of a concurrent system. It is not surprising that they lead to deadlocks. The stronger result we present is that, loosely speaking, these are the only two possible errors. More precisely, all FC-synchronisations which are not SL&SB contain killing choices and/or synchronic mismatches:

Theorem 4.6 *Let N_a and N_b two SL&SB FC nets and N an FC-synchronisation of $\{N_a, N_b\}$. N is SL&SB iff it contains no synchronic mismatch and no killing choice.*

Proof: ($\Rightarrow$) Use propositions 4.3, 4.5.

($\Leftarrow$) If N is not well formed, we can assume w.l.o.g. that N_a^1 is a T-component of N_a with a TP-handle $H = (t, \ldots, p)$. It is possible to prove that H can be chosen as the concatenation of two paths Π_1 and B, where $\Pi_1 = (t, \ldots, t')$ is a handle of N_a and B is a path of N_a.

Consider now two cases:

Case 1. Every T-component of N_b containing t contains also t'.

Then (t, t') is a synchronic mismatch because t' is not a transition of N_a^1.

Case 2. There exists a T-component $N_b^1 = (P_b^1, T_b^1; F_b^1)$ containing t but not t'.

Let p' be the last node of Π_1 that belongs to N_b^1 (p' must be a place because N_b^1 is a T-component of N_b). The subpath $\Pi_1' = (p', \ldots, t')$ of Π_1 leads from N_b^1 to $t' \in T_a \cap T_b$ and its only node in N_b^1 is p'. Moreover, $p' \notin P_a$ because Π_1 is a handle of N_a. Then p' is a killing choice of N_b. ∎ 4.6

5 Fusions

Given a net N, N^{-d} denotes the reverse dual net of N. The following relationship between synchronisations and fusions follows easily from the definitions:

Proposition 5.1 *N is an FC-synchronisation of $\{N_a, N_b\}$ iff N^{-d} is an FC-fusion of $\{N_a^{-1}, N_b^{-1}\}$.* ∎ 5.1

Making use of this property and of the Duality theorem for FC nets, we can obtain for fusions similar results to the ones obtained for synchronisations. The Duality theorem states the following:

Theorem 5.2 *[Hack 72] Let N be a net. N is SL&SB FC iff N^{-d} is SL&SB FC.* ∎ 5.2

In order to check if an FC-fusion N of two SL&SB FC nets N_a, N_b is SL&SB as well, we just consider the reverse-dual net N^{-d}, which by proposition 5.1 is an FC-synchronisation. We can then check whether this FC-synchronisation is well formed. By theorem 3.7, this is the case exactly when N^{-d} is SL&SB and, by the Duality theorem, exactly when N is SL&SB.

It is possible to mimic our presentation of the results for synchronisations. An FC-fusion is defined to be *well formed* iff the FC-synchronisation of the reverse-dual components is well formed. Also the design errors can be introduced in the same way: an FC-fusion of two nets has a *killing joint* (respectively, a *fusion mismatch*) iff the FC-synchronisation of of the reverse-dual nets has a killing choice (respectively, a synchronic mismatch). We obtain the dual theorems corresponding to our two main results for synchronisations:

Theorem 5.3 *Let N be an FC-fusion of $\{N_a, N_b\}$ N is SL&SB iff it is well formed.* ■ 5.3

Theorem 5.4 *Let N_a and N_b be two SL&SB FC nets and N an FC-fusion of $\{N_a, N_b\}$. N is SL&SB iff it contains no fusion mismatch and no killing joint.* ■ 5.4

6 Conclusions

We have introduced two composition operators for Petri Nets. For the class of Free Choice nets, we have characterised by means of compositional structural conditions when these operators preserve SL&SB. We have interpreted this characterisation in terms of two design errors. These errors are close to the intuition, and suggest what to change in order to obtain a correct system.

Acknowledgements

We thank three anonymous referees for pointing out some mistakes and for helpful comments.

References

[BD 90] BEST, E.; DESEL, J.: *Partial Order Behaviour and Structure of Petri Nets.* Formal Aspects of Computing Vol.2 No.2, 123–138.

[Best 87] BEST, E.: *Structure Theory of Petri Nets: the Free Choice Hiatus.* Advanced Course on Petri Nets / Brauer, Reisig, Rozenberg (eds.), LNCS 254 and 255, pp. 168–205.

[BT 87] BEST, E.; THIAGARAJAN, P.S.: *Some Classes of Live and Safe Petri Nets.* Concurrency and Nets / Voss, K.; Genrich, H.J., Rozenberg, G. (eds.). — Berlin: Springer-Verlag, pp. 71–94.

[Dese 86] DESEL, J.: *A structural property of Free-choice systems.* Newsletter of the GI Special Interest Group in Petri Nets and Related System Models, No. 25, pp.16–20.

[Espa 90b] ESPARZA, J.: *Structure Theory of Free Choice nets.* Ph. D. Thesis, Departamento de Ingeniería Eléctrica e Informática, Universidad de Zaragoza, June.

[Espa 90] ESPARZA, J.: *Synthesis Rules for Petri Nets, and How They Lead to New Results.* CONCUR'90 / Baeten, Klop, (eds.), LNCS 458, pp.182–198.

[ES 91] ESPARZA, J.; SILVA, M.: *Handles in Petri Nets.* Hildesheimer Informatik Fachbericht, 3-91.

[ES 90] ESPARZA, J.; SILVA, M.: *Top-down Synthesis of Live and Bounded Free Choice nets.* Proceedings of the XIth. International Conference on Application and Theory of Petri nets. Paris, June, pp. 63-83. To appear in Advances in Petri Nets 91.

[GJRT 83] GENRICH, H.J.; JANNSENS, D.; ROSENBERG, G.; THIAGARAJAN, P.S.: *Petri Nets and Their Relation to Graph Grammars.* 2nd Int. Workshop on Graph Grammars and their Application to Computer Science. LNCS 153, pp. 115–129.

[Hack 72] HACK, M.H.T.: *Analysis of Production Schemata by Petri Nets.* Cambridge, Mass.: MIT, Dept. Electrical Engineering, MS Thesis. Corrected June 1974

[Silv 87] SILVA, M.: *Towards a Synchrony Theory for P/T Nets.* Concurrency and Nets / Voss, K.; Genrich, H.J., Rozenberg, G. (eds.). — Berlin: Springer-Verlag, pp. 71–94.

[TV 84] THIAGARAJAN, P.S.; VOSS, K.: *A Fresh look at free Choice Nets.* Information and Control, Vol. 61, No. 2, May, pp. 85–113.