Reversible Occurrence Nets

Hernán Melgratti Daniel Dávalos

August 27, 2026

Introduction

Petri nets constitute a foundational model of concurrency, which makes their reversible counterparts particularly relevant. Reversible Petri nets have been used to investigate the relationships between different models of concurrency, such as process calculi and event structures. In this paper, we address the problem of mechanizing the theory of reversible Petri nets with causally consistent reversibility. Specifically, we present a full mechanization of reversible Occurrence Petri nets in the Lean proof assistant. We formally verify that this model satisfies causal-dependent reversibility by mechanizing the so-called parabolic lemma.

About this document

This is a document with the formal statements about the Lean repository `github.com/DanielDavalos93/reversible-occ-nets`, and the blueprint `DanielDavalos93.github.io/reversible-occ-nets` which contains: blueprint pdf, blueprint web, dependency graph and the web documentation (Lean style).

Contents

1 Petri nets **3**

2 Occurrence nets **5**

3 Reversible occurrence nets **7**
3.1 Transition type and reversible nets 7
3.2 Trace equivalence 8

4 Parabolic **10**
4.1 Swapping lemma 10
4.2 Parabolic lemma 10

Chapter 1

Petri nets

Definition 1 (Net)**.** A *net* N is a tuple $N = (\alpha, \beta, \bullet_, _\bullet)$, where α is a nonempty set of places, β is the set of transitions, and $\bullet_, _\bullet : \beta \to \mathbb{N}^\alpha$ assign source and target to each transition. We consider only nets in which every transition both consumes and produces, i.e., $\bullet t \neq \emptyset$ and $t\bullet \neq \emptyset$ for all $t \in \beta$.

Definition 2 (Preset for places.)**.** A *preset for places* is a function that take a net N, a place p and return the set $\{t \mid p \in t\bullet\}$, where the postset function is defined in Definition 1.

Definition 3 (Preset for transitions.)**.** A *preset for transitions* is a function that take a net N, a transition t and return the multiset $\bullet t$.

Definition 4 (Postset for places.)**.** A *postset for places* is a function that take a net N, a place p and return the set $\{t | p \in \bullet t\}$, where the preset function is defined in Definition 1.

Definition 5 (Postset for transitions.)**.** A *postset for transitions* is a function that take a net N, a transition t and return the multiset $t\bullet$.

The notation for preset of places or transition are written as $\bullet_{\{\{N\}\}} t$, but in this file we'll use only the short notation $\bullet t$.

Definition 6 (Minimal)**.** This definition say if the multiset doesn't have any transition before.

Definition 7 (Is minimal)**.** A set s is *initial* in a net N if $s \subseteq minimal(N)$.

Definition 8 (Maximal)**.** This definition say if the multiset doesn't have any transition after.

Definition 9 (Is maximal)**.** A set s is *maximal* in a net N if $s \subseteq maximal(N)$.

Definition 10 (Enabled transition)**.** Given a net N and a multiset m, a verificator of enabled transition is a function $\mathsf{is_enabled} : N \to \mathsf{Multiset} \to \beta \to \mathsf{Prop}$ that verifies if $m \leq \bullet t$. We denote $\mathsf{is_enabled\ N\ m\ t}$ as $m[[t]]_{\{\{N\}\}}$. [1]

Definition 11. Given a net N, a transition t and a prove that t is enabled at m, the function $\mathsf{marking_after_firing\ N\ m\ e}$ returns the multiset applied at m on t, which is $m - \bullet t + t\bullet$.

Definition 12 (Firing)**.** Given a net N, $\mathsf{is_firing} : \mathsf{N} \to \mathsf{Multiset}\ \alpha \to \mathsf{h} \to \mathsf{Multiset}\ \alpha \to \mathsf{Prop}$ checks if a firing on a multiset m by t is equal to another multiset m', i.e., if $m[[t\rangle = m'$. We denote this only by $m[[t\rangle m'$

[1] In this documentation we avoid the subscript notation, and instead we write only $m[[t]]$.

Theorem 13. *Let N be a net, t a transition and m a multiset, then $m[[t\rangle\rangle(m - \bullet t + t\bullet)$.*

Proof. It is immediate by Definition 12 and Definition 11. □

Definition 14 (Firing sequence)**.** `firing_sequence N m ls m'` is the concatenation of sequences, where ls is the sequence of transitions, m is the initial marking (Definition 7) and m' the final marking of the sequence. We denote for $s = \varepsilon$ for a empty sequence, in Lean this is an empty list, we denote for ';' the concatenation of lists. Therefore, a firing sequence is defined inductively as

- Empty. $m[[\varepsilon\rangle\rangle m$
- Inductive step. For a sequence $t; s$ where t is a transition and s is a transition sequence, $m[[t; s\rangle\rangle m'$ is a firing sequence if there is m'' such that $m[[t\rangle m''$ is firing and $m''[[s\rangle\rangle m'$ is a firing sequence.

Lemma 15 (Firing deterministic)**.** *For a net N and a transition t enabled at m (where e is a proof that it is enabled), if $m[[t\rangle m'$ and $m[[t\rangle m''$ then $m' = m''$.*

Proof. Immediate by unfolding Definition 12. □

Lemma 16. *For every net N and multisets m, m', $m[[\varepsilon\rangle\rangle m'$ implies $m = m'$.*

Proof. By structural induction on the firing sequence. □

Lemma 17. *Let t be a transition and s a sequence (note that $t; s$ is a sequence), m, m' two multisets and $m[[t; s\rangle\rangle m'$, then there exist a multiset m'' such that $m''[[s\rangle\rangle m$.*

Lemma 18. *Let t be a transition, s a sequence of transitions, m, m' two multisets, and $m[[t; s\rangle\rangle m'$. Then, there exist a multiset m'' such that $m[[t\rangle m''$.*

Lemma 19 (Concat firing sequence)**.** *Let be $m[[s_1\rangle\rangle m'$ and $m'[[s_2\rangle\rangle m''$ two firing sequences. Then $m[[s_1; s_2\rangle\rangle m''$.*

Lemma 20 (Append split of firing sequence)**.** *Let $m[[s_1; s_2\rangle\rangle m'$ be a firing sequences, then there is a multiset m'' such that $m[[s_1\rangle\rangle m''$ and $m''[[s_2\rangle\rangle m'$.*

Proof. By induction on the length of s_1, and by structural induction on the firing sequence for s_2. □

Lemma 21 (Firing sequence deterministic)**.** *Let be $m[[s\rangle\rangle m'$ and $m[[s\rangle\rangle m''$ two firing sequences, then $m' = m''$.*

Definition 22. A *marked net* is a tuple $M = (N, m_0)$, where N is a net (Definition 1) and m_0 is the initial marking.

Definition 23 (Reachable)**.** Given a marked net M and a multiset m, *reachable N m* return all the multisets that can be executed by sequences of firing enabled. We denote a reachable for a marking m of a net N by $N \rightsquigarrow m$.

Definition 24 (Safe)**.** A marked net $M = (N, m_0)$ is *safe* if for every multiset m, $M \quad m$ implies that m has no duplicate.

Theorem 25 (Square lemma)**.** *Let N a net, $m[[t_1\rangle m_1$ and $m[[t_2\rangle m_2$ two firings, and $\bullet t_1 \cap \bullet t_2 = \emptyset$. Then, there is a multiset m' such that $m_1[[t_1\rangle m'$ and $m_2[[t_2\rangle m'$.*

Proof. It is suffices to take $m' = m - \bullet t_1 + t_1 \bullet - \bullet t_2 + t_2\bullet$. To prove that $m_1[[t_1]]$ note that we can have $m_1 = m - \bullet t_1 + t_1\bullet$ after firing, and $\bullet t_2 \leq m - \bullet t_1$. Analousgly with the enabled $m_2[[t_2]]$. □

Chapter 2

Occurrence nets

Definition 26 (Immediate dependency)**.** Let N be a net. The *immediate dependency relation* $<_N \subseteq (\alpha \cup \beta) \times (\alpha \cup \beta)$ is defined by the set

$$\{(x, y) \mid (y \in \beta \wedge x \in \bullet y) \vee (x \in \beta \wedge y \in x\bullet)\} \tag{2.1}$$

Definition 27 (Causal relation)**.** We denote the transitive closure of $<_N$ as the *causal relation* $\prec_N$.

Definition 28. A relation $\preccurlyeq_N$ is *causal preorder* if it is the reflexive-transitive closure of $<_N$ (from Definition 26).

Definition 29. Let N be a net and $a \in \alpha$ a place. If $a \in \mathsf{minimal}(a)$ and $x \neq a$ then $\neg(x \preccurlyeq a)$.

Definition 30. Two different transtions t, t' are in *immediate conflict* if $\bullet t \cap \bullet t \neq \emptyset$. Let's denote this relation as $t \sharp_0 t'$.

Definition 31 (Conflict)**.** Two elements $x, y \in \alpha \cup \beta$ are in *conflict* if there exist two transtions t, t' that $t \preccurlyeq x$, $t' \preccurlyeq y$ and $t \sharp_0 t'$. We denote a conflict relation of x, y as $x \sharp y$.

Definition 32 (Backward conflict)**.** A place a has a *backward conflict* if it is produced by two distinct transitions, i.e., $\exists t_1, t_2, (t_1 \neq t_2) \wedge (a \in t_1\bullet) \wedge (p \in t_2\bullet)$.

Definition 33 (Acyclicity)**.** A net is *acyclic* if its causal relation is irreflexive, i.e., there is no $x \in \alpha \cup \beta$ such that $x \prec_N x$.

Definition 34 (Occurrence net)**.** A marked net (N, m_0) is an *occurrence net* if it satisfies the following statements:

1. N is acyclic;
2. there is no self-conflict, i.e., $\neg(t \sharp t)$ for all transition t;
3. there is no backward conflict;
4. N is 1-safe, i.e., marking is a set;
5. the initial marking is the set of initial places, i.e., m_0 is minimal (Definition 6).

Definition 35 (Marked occurrence net)**.** A marked net (N, m_0) is called *marked ocurrence* if N is occurrence, m_0 has no duplicates and each place $p \in m_0$ implies $p \in \mathsf{minimal}\ N$.

Definition 36 (Concurrency)**.** Two different elements $x, y \in \alpha \cup \beta$ are *concurrent* in N if $\neg(x \preccurlyeq y)$, $\neg(y \preccurlyeq x)$ and $\neg(x \sharp y)$. We denote the concurrency between these elements as x co y.

Definition 37 (Concurrent multiset)**.** A multiset m is concurrent in N if it no has duplicate and

$$\forall x, y \in \alpha, (x \in m) \Rightarrow (y \in m) \Rightarrow x \neq y \Rightarrow x \text{ co } y.$$

We'll denote the concurrency of a multiset m by Concurrent m.

Lemma 38. *Let be N an occurrence net, Concurrent N m and $m' \leq m$, then Concurrent N m'.*

Lemma 39. *Let be N an occurrence net and Concurrent N $(m + t\bullet)$, then Concurrent N $(m + \bullet t)$.*

Lemma 40. *Let N be an occurrence net, t an enabled transition at m and a, b two different places. If Concurrent N m, $m[[t\rangle m'$ is a firing, and $a, b \in m'$, then a co b.*

Lemma 41. *Let N be an occurrence net and t a transition enabled at m. If Concurrent N m and $m[[t\rangle m'$ is a firing, then Concurrent N m'.*

Lemma 42. *Let N be an occurrence net and s a transition sequence. If N is concurrent at m and $m[[s\rangle\!\rangle m'$ is a firing sequence, then Concurrent N m'.*

Proof. The proof procedes by applying structural induction over the length of the sequence s.

For the base case apply the Lemma 16 and is obtained that $m' = m$, so it's concurrent at m' by hypothesis.

For the step case, we can apply the inductive hypothesis over Lemma 41. □

Lemma 43. *Every marked occurrence net (N, m_0) is marking concurrent at m_0.*

Theorem 44. *Every marked occurrence net (N, m_0) is safe.*

Proof. A net is safe if for each multiset m and sequence s, $m_0[[s\rangle\!\rangle m$ implies that m has no duplicate tokens. So, let m be a multiset and s a transition sequence.

We've proved (Lemma 43) that m_0 is concurrent in N, so it's enough to apply the Lemma 42 to the occurrence condition in the hypothesis s, firing sequence $m_0[[s\rangle\!\rangle m$ and use the Lemma 43. □

Chapter 3

Reversible occurrence nets

3.1 Transition type and reversible nets

Definition 45 (Transition Type)**.** Lets define the type $\mathsf{Transition} ::= \mathsf{fwd} \mid \mathsf{bwd}$, where their elements are the forward direction for fwd and backward direction for bwd. Given a type for transition β, we define the set of reversible transitions as pairs $t_r ::= \langle t, \mathsf{fwd}\rangle \mid \langle t, \mathsf{bwd}\rangle$ with $t \in \beta$.

Definition 46 (Opposite)**.** For a transition with type $\mathsf{Transition}$ we define the *opposite* of t_t as

$$opposite(t_t) = \begin{cases} \mathsf{fwd} & \text{if } t_t = \mathsf{bwd} \\ \mathsf{bwd} & \text{if } t_t = \mathsf{fwd} \end{cases}$$

Definition 47. For $b \in \beta$, we'll say that a *transition* $t = (b, \mathsf{fwd})$ *is forward* and let's denote it as $\rhd t$.

Definition 48. For $b \in \beta$, we'll say that a *transition* $t = (b, \mathsf{bwd})$ *is backward* and let's denote it as $\lhd t$.

Definition 49 (Reverse)**.** For a transition with type $t = \langle t_\beta, t_t\rangle \in \beta \times \mathsf{Transition}$, its *reverse* is defined as $\leftharpoondown t := \langle t_\beta, opposite(t_t)\rangle$.

Definition 50. Let s a sequence of transitions with types $\beta \times \mathsf{Transition}$. We denote $\rhd\rhd\, s$ if forall $t \in s$, $\rhd t$; or if $s = \varepsilon$.

Definition 51. Let s a sequence of transitions with types $\beta \times \mathsf{Transition}$. We denote $\lhd\lhd\, s$ if forall $t \in s$, $\lhd t$; or if $s = \varepsilon$.

Theorem 52. *Let s_1, s_2 two transition sequences. Then, $\lhd\lhd s_1; s_2$ if and only if $\lhd\lhd s_1 \wedge \lhd\lhd s_2$.*

Proof. ($\Rightarrow$) Suppose that $s = s_1; s_2$ is a transition sequence with all the transitions backward. By induction over the length of the sequence s_1:

- Empty. If $s_1 = \varepsilon$ we have that $s = \varepsilon; s_2 = s_2$, and by hypothesis $\lhd\lhd s$, then $\lhd\lhd s_2$ and by Def. 51 $\lhd\lhd \varepsilon$ is truth. Therefore, $\lhd\lhd s_1 \wedge \lhd\lhd s_2$.
- Inductive step. If $s_1 = t; s'$ with $\lhd\lhd (s'; s_2)$ implies $\lhd\lhd s' \wedge \lhd\lhd s_2$, then $\lhd\lhd (t; s; s_2)$ implies that $\lhd t$ and therefore $\lhd\lhd (t; s') \wedge \lhd\lhd s_2$.

($\Leftarrow$) By induction over the length on the sequence s_1. □

Theorem 53. *Let s_1, s_2 two transition sequences. Then, $\rhd\rhd s_1; s_2$ if and only if $\rhd\rhd s_1 \wedge \rhd\rhd s_2$.*

Proof. Analousgly to Thm. 52. □

Definition 54 (Inverse)**.** Let be $t, t' \in \beta \times \mathsf{Transition}$. The transition t is *inverse* of t' if $t =\!\!\prec t'$. We denote the inverse of two transitions t, t' –in this order– by $t \prec\!\!\rightharpoonup t'$.

Theorem 55. *Let t, t' be two transitions in $\beta \times \mathsf{Transition}$. Then, $t = t'$ if and only if $\prec t =\!\!\prec t'$.*

Proof. Immediatly by Def. 54. □

Definition 56 (Inverse symmetric)**.** For $t, t' \in \beta \times \mathsf{TransitionType}$, $t \prec\!\!\rightharpoonup t'$ if and only if $t \prec\!\!\rightharpoonup t'$.

Definition 57 (Reversing occurrence nets)**.** A *reversible occurrence net* is a net $N = (\alpha, \beta \uplus \{\prec t \mid t \in \beta\}, \bullet_, _\bullet)$ defined by the following conditions:

1. $(\alpha, \beta, (\bullet_)_{|\beta}, (_\bullet)_{|\beta}$ is an occurrence net, where $f_{|\beta}$ denotes the restriction of the function f to the domain β.
2. For every $t \in \beta$, $\bullet t = (\prec t)\bullet$ and $t\bullet = \bullet(\prec t)$.

Definition 58. For a reversible net R, if $m[[t]]$ and $m[[t\rangle m'$ then there is a transition t', which $t' \prec\!\!\rightharpoonup t$ and $m'[[t']]$.

Lemma 59 (Cancelation)**.** *If $t \prec\!\!\rightharpoonup t'$, $m[[t\rangle m'$ and $m'[[t']]$ then $m'[[t'\rangle m$.*

Proof. □

Definition 60 (Marked reversible occurrence net)**.** A tuple $MO = (R, m_0)$ is *marked reversible occurrence* if R is a reversible net and ($\mathsf{fwd_subnet}$ R, m_0) is marked occurrence, where $\mathsf{fwd_subnet}$ returns the forward subnet of a reversing net.

Lemma 61 (Loop)**.** *Let $t, t' \in \beta \times Transition$ two reversing transitions, i.e., $t \prec\!\!\rightharpoonup t'$. Then,*

$$(\exists e, m[[e\rangle m') \iff (\exists e, m'[[e\rangle m)$$

Theorem 62 (Backtracking)**.** *If $(\exists s, m[[s\rangle\!\rangle m')$ then $(\exists s, m'[[s\rangle\!\rangle m)$.*

Proof. By induction over the length of a sequence s. By applying the Lemma 61 to the step case $t; s$ on s, we can obtain a witness $s; \prec t$ and apply the respective concatenation (Lemma 19) and we have the firing sequence as expected. □

3.2 Trace equivalence

Definition 63 (Transition equivalence)**.** The statement of the lemma requires a formal notion of *equivalent firing sequences*, which is the smallest congruence[1] $\asymp$ on transition sequences closed under the following rules:

(i) $t; t' \asymp t'; t$ if t co t',

(ii) $t; \prec t \asymp \varepsilon$, and

[1] A relation R over sequences is a **congruence** if it is an equivalence relation closed by concatenation, i.e., $s_1 R s_2$ and $s_3 R s_4$ implies $s_1; s_3 R s_2; s_4$ for all s_1, s_2, s_3 and s_4.

(iii) $\leftharpoondown t; t \asymp \varepsilon$.

Definition 64. $s \asymp s$.

Definition 65. $s_1 \asymp s_2 \Longrightarrow s_2 \asymp s_1$.

Definition 66. $s_1 \asymp s_2 \wedge s_2 \asymp s_3 \Longrightarrow s_1 \asymp s_3$.

Theorem 67. $s_1 \asymp s_2 \wedge s_3 \asymp s_4 \Longrightarrow s_1; s_3 \asymp s_2; s_4$.

Proof. By cases over the structural definition 63. □

Chapter 4

Parabolic

4.1 Swapping lemma

Definition 68. Let $t \in \beta$ a transition and s a sequence of transitions of β. We define

$$t \notin^r := \forall t' \in s, \neg(t \leftharpoondown\!\!\rightharpoonup t').$$

Definition 69. Let $t \in \beta$ a transition and s a sequence of transitions of β. We define

$$t\exists^r := \exists t' \in s, (t \leftharpoondown\!\!\rightharpoonup t').$$

Lemma 70. *Let $M = (N, m_0)$ a marked reversible occurrence net, m a marking, t and $'t$ two transitions with $t \bullet \cap \bullet t' = \emptyset$ and $\neg(t \leftharpoondown\!\!\rightharpoonup t')$. If $M \quad m$ and $m[t; t'\rangle m'$, then $m[[t'; t\rangle m'$.*

Lemma 71. *Let $M = (N, m_0)$ a marked reversible occurrence net, m a marking, t and $'t$ two transitions with $\rhd t$ (is forward transition) and $\lhd t'$ (is backward transition). If $M \quad m_0$, $\neg(t \leftharpoondown\!\!\rightharpoonup t')$ and $m[[t; t'\rangle m'$ is a firing sequence, then we can have the swapped firing sequence between the transitions: $m[[t'; t\rangle m'$.*

Lemma 72 (Swapping)**.** *Let $M = (N, m_0)$ a marked reversible occurrence net, m a marking, s a sequence and t a transition with the condition $\lhd \lhd s$ and $\rhd t$. If $M \quad m_0$, $t \notin s$ and $m[[t; s\rangle m'$ is a firing sequence, then we can have the swapped between the transition and all the backward sequence: $m[[s; t\rangle m'$.*

4.2 Parabolic lemma

Lemma 73. *Step of forward case for parabolic.*

Theorem 74 (Parabolic lemma)**.** *Let R be a reversible occurrence net, m a reachable marking, and $m[[\omega\rangle m'$ a firing sequence. Then there exist two sequences of transitions, ω' and ω'', such that ω' consists only of backward transitions, ω'' consists only of forward transitions, $\omega \asymp \omega'; \omega''$, and $m[[\omega'; \omega''\rangle m'$.*

Proof. By applying induction on the firing sequence. The base case when $m' = m$ is immediate. The inductive step applies the property of $\asymp$ and the Lemma 73. □

Appendix - Auxiliar lemmas for multisets

Lemma 75. *If $t \leq s$ then $t + (s - t) = s$.*

Proof. □

Lemma 76. $s + t - u = s - u + t$.

Proof. □