Parallel Closure Theorem for Left-Linear Nominal Rewriting Systems

Kentaro Kikuchi[1], Takahito Aoto[2], and Yoshihito Toyama[1]

[1] RIEC, Tohoku University, Sendai, Japan
{ kentaro, toyama }@nue.riec.tohoku.ac.jp
[2] Faculty of Engineering, Niigata University, Niigata, Japan
aoto@ie.niigata-u.ac.jp

Abstract. Nominal rewriting has been introduced as an extension of first-order term rewriting by a binding mechanism based on the nominal approach. In this paper, we extend Huet's parallel closure theorem and its generalisation on confluence of left-linear term rewriting systems to the case of nominal rewriting. The proof of the theorem follows a previous inductive confluence proof for orthogonal uniform nominal rewriting systems, but the presence of critical pairs requires a much more delicate argument. The results include confluence of left-linear uniform nominal rewriting systems that are not α-stable and thus are not represented by any systems in traditional higher-order rewriting frameworks.

1 Introduction

Variable binding is ubiquitous in many expressive formal systems such as systems of predicate logics, λ-calculi, process calculi, etc. Every language containing variable binding needs to deal with α-equivalence. Intuitively α-equivalence may be dealt with implicitly, but much effort is required in formal treatment. To overcome the difficulty, many studies have been made in the literature (e.g. [5, 18]), among which the nominal approach [9, 17] is a novel one—unlike other approaches, it incorporates permutations and freshness conditions on variables (atoms) as basic ingredients.

To deal with equational logics containing variable binding, various rewriting frameworks have been proposed (e.g. [12, 13]). *Nominal rewriting* [8] has been introduced as a new rewriting framework based on the nominal approach. A distinctive feature of nominal rewriting is that α-conversion and capture-avoiding substitution are not relegated to the meta-level—they are explicitly dealt with at the object-level. In contrast, previous rewriting frameworks as in [12, 13] employ some meta-level calculus (e.g. the simply-typed λ-calculus) and accomplish α-conversion and capture-avoiding substitution via the meta-level calculus.

Confluence and *critical pairs* are fundamental notions for systematic treatment of equational reasoning based on rewriting. Some basic confluence results such as Rosen's criterion (orthogonal systems are confluent) and Knuth-Bendix's criterion (terminating systems with joinable critical pairs are confluent) have been extended to the case of nominal rewriting [3, 8, 19, 20].

In the present paper, we are concerned with Huet's criterion [10] (left-linear systems with parallel closed critical pairs are confluent, which is known as the parallel closure theorem) in the setting of nominal rewriting. We are also aiming to obtain its generalisation analysing overlaps at the root as in the case of term rewriting [21]. These results extend the previous results of Rosen's criterion in the nominal rewriting setting [3, 8, 19], and include confluence of, in particular, weakly orthogonal nominal rewriting systems, i.e. left-linear nominal rewriting systems in which all critical pairs are α-equivalent.

The difficulties in proving confluence properties of nominal rewriting systems, compared to the case of ordinary term rewriting, are threefold. First, rewriting is performed via matching modulo α-equivalence, so that a redex is not necessarily an instance of the LHS of a rule but a term that is α-equivalent to it. This causes, among others, similar difficulties in proving the critical pair lemma to those for E-critical pairs [11]. Secondly, rewrite rules have freshness contexts (or constraints), and accordingly, critical pairs are also accompanied with freshness contexts. This is analogous to the case of term rewriting with certain constraints (e.g. [7]). Thirdly, as a characteristic feature of nominal rewriting, rewrite steps involve permutations, or, in terms of [8], the set of rewrite rules is closed under equivariance. Therefore, to keep finiteness of the representations, critical pairs need to be parametrised by permutations.

Due to these difficulties, it is not obvious in nominal rewriting that a peak with rewriting at a non-variable position of one of the rules is an instance of a critical pair. This property is necessary in the proof of Lemma 13, where we construct required permutations and substitutions using some lemmas and the property of the most general unifier occurring in the critical pair.

The parallel closure theorem for left-linear nominal rewriting systems has not been shown for years, while confluence by orthogonality and the critical pair lemma has already been discussed in [3, 8, 19, 20]: [3, 8, 19] deal with left-linear systems without critical pairs, and [20] deals with terminating or left-and-right-linear systems. We give an example of a nominal rewriting system whose confluence is shown by our criterion but cannot be shown by any of the criteria given in the previous papers (see Example 1). Moreover, in the present paper, we do not particularly assume α-stability [19] of nominal rewriting systems. This is in contrast to [3, 19, 20] where confluence criteria are considered only for α-stable rewriting systems. We give an example of a nominal rewriting system that is not α-stable and that is shown to be confluent by our criterion (see Example 2).

The structure of our confluence proof follows the so-called inductive method for first-order orthogonal term rewriting systems as explained, e.g. in Chapter 9 of [4, pp. 208–211], but much more complicated than the first-order case by the above-mentioned difficulties. Our confluence proof also shows that such an inductive method can be adapted to cases with critical pairs.

The paper is organised as follows. In Section 2, we recall basic notions of nominal rewriting and critical pairs. In Section 3, we prove confluence for some classes of nominal rewriting systems via the parallel closure theorem and its generalisation. In Section 4, we conclude with discussion on related work.

2 Nominal rewriting

Nominal rewriting [8] is a framework that extends first-order term rewriting by a binding mechanism. In this section, we recall basic definitions on nominal terms and nominal rewriting, following [19, 20]. For further descriptions and examples, see [8, 19, 20].

2.1 Nominal terms

A *nominal signature* Σ is a set of *function symbols* ranged over by $f, g, \ldots$. We fix a countably infinite set $\mathcal{X}$ of *variables* ranged over by $X, Y, Z, \ldots$, and a countably infinite set $\mathcal{A}$ of *atoms* ranged over by $a, b, c, \ldots$, and assume that Σ, $\mathcal{X}$ and $\mathcal{A}$ are pairwise disjoint. Unless otherwise stated, different meta-variables for objects in Σ, $\mathcal{X}$ or $\mathcal{A}$ denote different objects. A *swapping* is a pair of atoms, written $(a\ b)$. *Permutations* π are bijections on $\mathcal{A}$ such that the set of atoms for which $a \neq \pi(a)$ is finite. Permutations are represented by lists of swappings applied in the right-to-left order. For example, $((b\ c)(a\ b))(a) = c$, $((b\ c)(a\ b))(b) = a$, $((b\ c)(a\ b))(c) = b$. We write Id for the identity permutation, π^{-1} for the inverse of π, and $\pi \circ \pi'$ for the composition of π' and π, i.e., $(\pi \circ \pi')(a) = \pi(\pi'(a))$.

Nominal terms, or simply *terms*, are generated by the grammar

$$t, s ::= a \mid \pi{\cdot}X \mid [a]t \mid f\ t \mid \langle t_1, \ldots, t_n \rangle$$

and called, respectively, atoms, moderated variables, abstractions, function applications and tuples. We abbreviate $\mathit{Id}{\cdot}X$ as X if there is no ambiguity. $f\ \langle\,\rangle$ is abbreviated as f, and referred to as a *constant*. An abstraction $[a]t$ is intended to represent t with a bound. We write $V(t)(\subseteq \mathcal{X})$ for the set of variables occurring in t. A *linear* term is a term in which any variable occurs at most once.

Positions are finite sequences of positive integers. The empty sequence is denoted by ε. For positions p, q, we write $p \preceq q$ if there exists a position o such that $q = po$. We write $p \parallel q$ for $p \not\preceq q$ and $q \not\preceq p$. The set of positions in a term t, denoted by $\mathit{Pos}(t)$, is defined as follows: $\mathit{Pos}(a) = \mathit{Pos}(\pi{\cdot}X) = \{\varepsilon\}$; $\mathit{Pos}([a]t) = \mathit{Pos}(f\ t) = \{1p \mid p \in \mathit{Pos}(t)\} \cup \{\varepsilon\}$; $\mathit{Pos}(\langle t_1, \ldots, t_n \rangle) = \bigcup_i \{ip \mid p \in \mathit{Pos}(t_i)\} \cup \{\varepsilon\}$. The subterm of t at a position $p \in \mathit{Pos}(t)$ is written as $t|_p$. We write $s \subseteq t$ if s is a subterm occurrence of t, and write $s \subset t$ if $s \subseteq t$ and $s \neq t$. A position $p \in \mathit{Pos}(t)$ is a *variable position* in t if $t|_p$ is a moderated variable. The set of variable positions in t is denoted by $\mathit{Pos}_{\mathcal{X}}(t)$. The size $|t|$ of a term t is defined as the number of elements in $\mathit{Pos}(t)$.

Next, two kinds of permutation actions $\pi{\cdot}t$ and t^π, which operate on terms extending a permutation on atoms, are defined as follows:

$$\begin{array}{rlrl}
\pi{\cdot}a &= \pi(a) & a^\pi &= \pi(a) \\
\pi{\cdot}(\pi'{\cdot}X) &= (\pi \circ \pi'){\cdot}X & (\pi'{\cdot}X)^\pi &= (\pi \circ \pi' \circ \pi^{-1}){\cdot}X \\
\pi{\cdot}([a]t) &= [\pi{\cdot}a](\pi{\cdot}t) & ([a]t)^\pi &= [a^\pi]t^\pi \\
\pi{\cdot}(f\ t) &= f\ \pi{\cdot}t & (f\ t)^\pi &= f\ t^\pi \\
\pi{\cdot}\langle t_1, \ldots, t_n \rangle &= \langle \pi{\cdot}t_1, \ldots, \pi{\cdot}t_n \rangle & \langle t_1, \ldots, t_n \rangle^\pi &= \langle t_1^\pi, \ldots, t_n^\pi \rangle
\end{array}$$

The difference between the two consists in the clause for moderated variables. In particular, when $\pi' = Id$, π is suspended before X in the first action as $\pi\cdot(Id\cdot X) = (\pi \circ Id)\cdot X = \pi\cdot X$, while in the second action π has no effect as $(Id\cdot X)^\pi = (\pi \circ Id \circ \pi^{-1})\cdot X = Id\cdot X$. Note also that the permutation actions do not change the set of positions, i.e. $Pos(\pi\cdot t) = Pos(t^\pi) = Pos(t)$.

A *context* is a term in which a distinguished constant $\Box$ occurs. Contexts having precisely one $\Box$ are written as $C[\,]$. The term obtained from a context C by replacing each $\Box$ at positions p_i by terms t_i is written as $C[t_1, \ldots, t_n]_{p_1,\ldots,p_n}$ or simply $C[t_1, \ldots, t_n]$. Similarly, the term obtained from a term s by replacing each subterm at positions p_i by terms t_i is written as $s[t_1, \ldots, t_n]_{p_1,\ldots,p_n}$.

A *substitution* σ is a map from variables to terms. Substitutions act on variables, without avoiding capture of atoms, where substituting $\sigma(X)$ for X of a moderated variable $\pi\cdot X$ induces a permutation action $\pi\cdot(\sigma(X))$. The application of a substitution σ on a term t is written as $t\sigma$. For a permutation π and a substitution σ, we define the substitution $\pi\cdot\sigma$ by $(\pi\cdot\sigma)(X) = \pi\cdot(\sigma(X))$.

The following properties hold.

Proposition 1. *$\pi\cdot(\pi'\cdot t) = (\pi \circ \pi')\cdot t$ and $(t^\pi)^{\pi'} = t^{\pi' \circ \pi}$.*

Proposition 2 ([8, 22]). *$\pi\cdot(t\sigma) = (\pi\cdot t)\sigma$.*

Lemma 1. *$\pi\cdot(t\sigma) = t^\pi(\pi\cdot\sigma)$.*

2.2 Freshness constraints and α-equivalence

A pair $a\#t$ of an atom a and a term t is called a *freshness constraint*. A finite set $\nabla \subseteq \{a\#X \mid a \in \mathcal{A}, X \in \mathcal{X}\}$ is called a *freshness context*. For a freshness context ∇, we define $V(\nabla) = \{X \in \mathcal{X} \mid \exists a.\ a\#X \in \nabla\}$, $\nabla^\pi = \{a^\pi\#X \mid a\#X \in \nabla\}$ and $\nabla\sigma = \{a\#\sigma(X) \mid a\#X \in \nabla\}$.

The rules in Figure 1 define the relation $\nabla \vdash a\#t$, which means that $a\#t$ is satisfied under the freshness context ∇.

$$\frac{}{\nabla \vdash a\#b} \qquad \frac{\nabla \vdash a\#t}{\nabla \vdash a\#f\ t} \qquad \frac{\nabla \vdash a\#t_1 \quad \cdots \quad \nabla \vdash a\#t_n}{\nabla \vdash a\#\langle t_1, \ldots, t_n\rangle}$$

$$\frac{}{\nabla \vdash a\#[a]t} \qquad \frac{\nabla \vdash a\#t}{\nabla \vdash a\#[b]t} \qquad \frac{\pi^{-1}\cdot a\#X \in \nabla}{\nabla \vdash a\#\pi\cdot X}$$

Fig. 1. Rules for freshness constraints

The rules in Figure 2 define the relation $\nabla \vdash t \approx_\alpha s$, which means that t is α-equivalent to s under the freshness context ∇. $ds(\pi, \pi')$ in the last rule denotes the set $\{a \in \mathcal{A} \mid \pi\cdot a \neq \pi'\cdot a\}$. Note that if $\nabla \vdash t \approx_\alpha s$ then $Pos(t) = Pos(s)$.

The following properties are shown in [8, 22].

Proposition 3. *1. $\nabla \vdash a\#t$ if and only if $\nabla \vdash \pi\cdot a\#\pi\cdot t$.*
2. $\nabla \vdash t \approx_\alpha s$ if and only if $\nabla \vdash \pi\cdot t \approx_\alpha \pi\cdot s$.
3. If $\nabla \vdash a\#t$ and $\nabla \vdash t \approx_\alpha s$ then $\nabla \vdash a\#s$.
4. $\forall a \in ds(\pi, \pi').\ \nabla \vdash a\#t$ if and only if $\nabla \vdash \pi\cdot t \approx_\alpha \pi'\cdot t$.

$$\frac{}{\nabla \vdash a \approx_\alpha a} \qquad \frac{\nabla \vdash t \approx_\alpha s}{\nabla \vdash f\ t \approx_\alpha f\ s} \qquad \frac{\nabla \vdash t_1 \approx_\alpha s_1 \quad \cdots \quad \nabla \vdash t_n \approx_\alpha s_n}{\nabla \vdash \langle t_1, \ldots, t_n \rangle \approx_\alpha \langle s_1, \ldots, s_n \rangle}$$

$$\frac{\nabla \vdash t \approx_\alpha s}{\nabla \vdash [a]t \approx_\alpha [a]s} \qquad \frac{\nabla \vdash (a\ b)\cdot t \approx_\alpha s \quad \nabla \vdash b\#t}{\nabla \vdash [a]t \approx_\alpha [b]s} \qquad \frac{\forall a \in ds(\pi, \pi').\ a\#X \in \nabla}{\nabla \vdash \pi\cdot X \approx_\alpha \pi'\cdot X}$$

Fig. 2. Rules for α-equivalence

Proposition 4. *For any freshness context ∇, the binary relation $\nabla \vdash - \approx_\alpha -$ is a congruence (i.e. an equivalence relation that is closed under any context).*

In the sequel, $\vdash$ is extended to mean to hold for all members of a set (or a sequence) on the RHS.

2.3 Nominal rewriting systems

Nominal rewrite rules and nominal rewriting systems are defined as follows.

Definition 1 (Nominal rewrite rule). A *nominal rewrite rule*, or simply *rewrite rule*, is a triple of a freshness context ∇ and terms l and r such that $V(\nabla) \cup V(r) \subseteq V(l)$ and l is not a moderated variable. We write $\nabla \vdash l \to r$ for a rewrite rule, and identify rewrite rules modulo renaming of variables. A rewrite rule $\nabla \vdash l \to r$ is *left-linear* if l is linear. For a rewrite rule $R = \nabla \vdash l \to r$ and a permutation π, we define R^π as $\nabla^\pi \vdash l^\pi \to r^\pi$.

Definition 2 (Nominal rewriting system). A *nominal rewriting system*, or simply *rewriting system*, is a finite set of rewrite rules. A rewriting system is *left-linear* if so are all its rewrite rules.

Definition 3 (Rewrite relation). Let $R = \nabla \vdash l \to r$ be a rewrite rule. For a freshness context Δ and terms s and t, the *rewrite relation* is defined by

$$\Delta \vdash s \to_{\langle R,\pi,p,\sigma\rangle} t \overset{\text{def}}{\iff} \Delta \vdash \nabla^\pi\sigma,\ s = C[s']_p,\ \Delta \vdash s' \approx_\alpha l^\pi\sigma,\ t = C[r^\pi\sigma]_p$$

where $V(l) \cap (V(\Delta) \cup V(s)) = \emptyset$. We write $\Delta \vdash s \xrightarrow{p}_R t$ if there exist π and σ such that $\Delta \vdash s \to_{\langle R,\pi,p,\sigma\rangle} t$. We write $\Delta \vdash s \to_{\langle R,\pi\rangle} t$ if there exist p and σ such that $\Delta \vdash s \to_{\langle R,\pi,p,\sigma\rangle} t$. We write $\Delta \vdash s \to_R t$ if there exists π such that $\Delta \vdash s \to_{\langle R,\pi\rangle} t$. For a rewriting system $\mathcal{R}$, we write $\Delta \vdash s \to_{\mathcal{R}} t$ if there exists $R \in \mathcal{R}$ such that $\Delta \vdash s \to_R t$.

Lemma 2. *If $\Delta \vdash s \to_{\langle R,\pi,p,\sigma\rangle} t$ then $\Delta \vdash \tau\cdot s \to_{\langle R,\tau\circ\pi,p,\tau\cdot\sigma\rangle} \tau\cdot t$.*

In the following, a binary relation $\Delta \vdash - \bowtie -$ ($\bowtie$ is $\to_R$, $\approx_\alpha$, etc.) with a fixed freshness context Δ is called the relation $\bowtie$ under Δ or simply the relation $\bowtie$ if there is no ambiguity. If a relation $\bowtie$ is written using $\to$ then the inverse is written using $\leftarrow$. Also, we write $\bowtie^=$ for the reflexive closure and $\bowtie^*$ for the reflexive transitive closure. We use $\circ$ for the composition of relations. We write $\Delta \vdash s_1 \bowtie_1 s_2 \bowtie_2 \ldots \bowtie_{n-1} s_n$ for $\Delta \vdash s_i \bowtie_i s_{i+1}$ $(1 \le i < n)$.

2.4 Basic critical pairs

In this subsection, we define our notion of critical pairs, following [20].

First, we recall unification of nominal terms. Let P be a set of equations and freshness constraints $\{s_1 \approx t_1, \ldots, s_m \approx t_m, a_1 \# u_1, \ldots, a_n \# u_n\}$ (where a_i and a_j may denote the same atom). Then, P is *unifiable* if there exist a freshness context Γ and a substitution θ such that $\Gamma \vdash s_1\theta \approx_\alpha t_1\theta, \ldots, s_m\theta \approx_\alpha t_m\theta, a_1 \# u_1\theta, \ldots, a_n \# u_n\theta$; the pair $\langle \Gamma, \theta \rangle$ is called a *unifier* of P. It is shown in [22] that the unification problem for nominal terms is decidable. Moreover, if P is unifiable then there exists a *most general unifier* (*mgu* for short) of P, where an mgu of P is a unifier $\langle \Gamma, \theta \rangle$ of P such that for any unifier $\langle \Delta, \sigma \rangle$ of P, there exists a substitution δ such that $\Delta \vdash \Gamma\delta$ and $\Delta \vdash X\theta\delta \approx_\alpha X\sigma$ for any variable X.

Definition 4 (Basic critical pair). Let $R_i = \nabla_i \vdash l_i \to r_i$ $(i = 1, 2)$ be rewrite rules. We assume w.l.o.g. $V(l_1) \cap V(l_2) = \emptyset$. Let $\nabla_1 \cup \nabla_2^\pi \cup \{l_1 \approx l_2^\pi|_p\}$ be unifiable for some permutation π and a non-variable position p such that $l_2 = L[l_2|_p]_p$, and let $\langle \Gamma, \theta \rangle$ be an mgu. Then, $\Gamma \vdash \langle L^\pi\theta[r_1\theta]_p, r_2^\pi\theta \rangle$ is called a *basic critical pair* (*BCP* for short) of R_1 and R_2. $BCP(R_1, R_2)$ denotes the set of all BCPs of R_1 and R_2, and $BCP(\mathcal{R})$ denotes the set $\bigcup_{R_i, R_j \in \mathcal{R}} BCP(R_i, R_j)$.

We remark that any BCP $\Gamma \vdash \langle L^\pi\theta[r_1\theta]_p, r_2^\pi\theta \rangle$ of R_1 and R_2 forms a peak, i.e., we have $\Gamma \vdash L^\pi\theta[r_1\theta]_p \leftarrow_{\langle R_1, Id, p, \theta \rangle} L^\pi\theta[l_2^\pi|_p\theta]_p = (L[l_2|_p]_p)^\pi\theta = l_2^\pi\theta \to_{\langle R_2, \pi, \varepsilon, \theta \rangle} r_2^\pi\theta$.

2.5 Uniform rewrite rules

In the rest of the paper, we are concerned with confluence properties for particular classes of nominal rewriting systems. For this, we restrict rewriting systems by some conditions. First we consider the uniformity condition [8]. Intuitively, uniformity means that if an atom a is not free in s and s rewrites to t then a is not free in t.

Definition 5 (Uniformity). A rewrite rule $\nabla \vdash l \to r$ is *uniform* if for any atom a and any freshness context Δ, $\Delta \vdash \nabla$ and $\Delta \vdash a \# l$ imply $\Delta \vdash a \# r$. A rewriting system is *uniform* if so are all its rewrite rules.

The following properties of uniform rewrite rules are important and will be used in the sequel.

Proposition 5 ([8]). *Suppose $\Delta \vdash s \to_R t$ for a uniform rewrite rule R. Then, $\Delta \vdash a \# s$ implies $\Delta \vdash a \# t$.*

Lemma 3. *Let $\nabla \vdash l \to r$ be a uniform rewrite rule, and let $\Delta \vdash C[l^\pi\sigma]_p \approx_\alpha \hat{C}[u]_p$. Then there exists a permutation $\hat{\pi}$ such that $\Delta \vdash l^\pi\sigma \approx_\alpha \hat{\pi}\cdot u$ and $\Delta \vdash C[r^\pi\sigma]_p \approx_\alpha \hat{C}[\hat{\pi}^{-1}\cdot(r^\pi\sigma)]_p$.*

Proof. We prove the following generalised statement: if $\Delta \vdash \tau\cdot(C_1[u]_p) \approx_\alpha C_2[v]_p$ then there exists a permutation π satisfying

1. $\Delta \vdash (\pi \circ \tau){\cdot}u \approx_\alpha v$.
2. Let u' and v' be terms such that (i) $\forall a \in \mathcal{A}.\ \Delta \vdash a\#u \Longrightarrow \Delta \vdash a\#u'$, and (ii) $\Delta \vdash (\pi \circ \tau){\cdot}u' \approx_\alpha v'$. Then $\Delta \vdash \tau{\cdot}(C_1[u']_p) \approx_\alpha C_2[v']_p$. ((i) is equivalent to $\forall a \in \mathcal{A}.\ \Delta \vdash a\#v \Longrightarrow \Delta \vdash a\#v'$ under 1 and (ii).)

The lemma is obtained as a special case of this where $\tau = Id$, $C_1 = \hat{C}$, $C_2 = C$, $\pi = \hat{\pi}$, $v = l^\pi\sigma$, $v' = r^\pi\sigma$ and $u' = \hat{\pi}^{-1}{\cdot}(r^\pi\sigma)$. The proof of the above statement is by induction on the context $C_1[\,]$. ☐

Lemma 4. *Let R be a uniform rewrite rule. If $\Delta \vdash s' \approx_\alpha s \rightarrow_{\langle R,\pi,p,\sigma\rangle} t$, then there exist π', σ', t' such that $\Delta \vdash s' \rightarrow_{\langle R,\pi',p,\sigma'\rangle} t' \approx_\alpha t$.*

Proof. Noting that $\Delta \vdash s \approx_\alpha s'$ implies $Pos(s) = Pos(s')$, we obtain the lemma from Lemma 3 by taking $\pi' = \hat{\pi}^{-1} \circ \pi$ and $\sigma' = \hat{\pi}^{-1}{\cdot}\sigma$. ☐

3 Confluence of left-linear nominal rewriting systems

In this section, we study confluence properties of left-linear nominal rewriting systems. Specifically, we prove a version of Huet's parallel closure theorem [10] in the setting of nominal rewriting. Huet's parallel closure theorem states that all left-linear parallel closed term rewriting systems are confluent, where a term rewriting system is parallel closed if all its critical pairs are joinable in one-step parallel reduction from left to right. (It is important to note that critical pairs are ordered.) We also prove a generalisation of the theorem, analysing overlaps at the root as in the case of term rewriting [21].

First we introduce, for precise treatment of α-equivalence, confluence properties modulo the equivalence relation $\approx_\alpha$ in terms of abstract reduction systems [14].

Definition 6. Let $\mathcal{R}$ be a nominal rewriting system.

1. s and t are *joinable modulo* $\approx_\alpha$ under a freshness context Δ, denoted by $\Delta \vdash s \downarrow_{\approx_\alpha} t$, iff $\Delta \vdash s\ (\rightarrow^*_{\mathcal{R}} \circ \approx_\alpha \circ \leftarrow^*_{\mathcal{R}})\ t$.
2. $\rightarrow_{\mathcal{R}}$ is *confluent modulo* $\approx_\alpha$ iff $\Delta \vdash s\ (\leftarrow^*_{\mathcal{R}} \circ \rightarrow^*_{\mathcal{R}})\ t$ implies $\Delta \vdash s \downarrow_{\approx_\alpha} t$.
3. $\rightarrow_{\mathcal{R}}$ is *Church-Rosser modulo* $\approx_\alpha$ iff $\Delta \vdash s\ (\leftarrow_{\mathcal{R}} \cup \rightarrow_{\mathcal{R}} \cup \approx_\alpha)^*\ t$ implies $\Delta \vdash s \downarrow_{\approx_\alpha} t$.
4. $\rightarrow_{\mathcal{R}}$ is *strongly locally confluent modulo* $\approx_\alpha$ iff $\Delta \vdash s\ (\leftarrow_{\mathcal{R}} \circ \rightarrow_{\mathcal{R}})\ t$ implies $\Delta \vdash s\ (\rightarrow^{=}_{\mathcal{R}} \circ \approx_\alpha \circ \leftarrow^*_{\mathcal{R}})\ t$.
5. $\rightarrow_{\mathcal{R}}$ is *strongly compatible with* $\approx_\alpha$ iff $\Delta \vdash s\ (\approx_\alpha \circ \rightarrow_{\mathcal{R}})\ t$ implies $\Delta \vdash s\ (\rightarrow^{=}_{\mathcal{R}} \circ \approx_\alpha)\ t$.

It is known that Church-Rosser modulo an equivalence relation $\sim$ is a stronger property than confluence modulo $\sim$ [14]. So in the rest of this section we aim to show Church-Rosser modulo $\approx_\alpha$ for some class of left-linear uniform nominal rewriting systems through the theorems that can be seen as extensions of Huet's parallel closure theorem [10] and its generalisation [21].

3.1 Parallel reduction

A key notion for proving confluence of left-linear rewriting systems is parallel reduction. Here we define it inductively, using a particular kind of contexts.

Definition 7. The *grammatical contexts*, ranged over by G, are the contexts defined by

$$G ::= a \mid \pi{\cdot}X \mid [a]\Box \mid f\ \Box \mid \langle \Box_1, \ldots, \Box_n \rangle$$

Let $\mathcal{R}$ be a nominal rewriting system. For a given freshness context Δ, we define the relation $\Delta \vdash - \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} -$ inductively by the following rules:

$$\frac{\Delta \vdash s_1 \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t_1 \quad \cdots \quad \Delta \vdash s_n \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t_n}{\Delta \vdash G[s_1, \ldots, s_n] \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} G[t_1, \ldots, t_n]}\ (\mathsf{C}) \qquad \frac{\Delta \vdash s \rightarrow_{\langle R, \pi, \varepsilon, \sigma \rangle} t \quad R \in \mathcal{R}}{\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t}\ (\mathsf{B})$$

where $n\,(\geq 0)$ depends on the form of G. We define $\Delta \vdash \sigma \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} \delta$ by $\forall X \in \mathcal{X}.\ \Delta \vdash X\sigma \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} X\delta$.

The relation $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ can also be defined by $\Delta \vdash C[s_1, \ldots, s_n]_{p_1, \ldots, p_n} \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} C[t_1, \ldots, t_n]_{p_1, \ldots, p_n}$ for some context C, where $\Delta \vdash s_i \rightarrow_{R_i} t_i$ for some $R_i \in \mathcal{R}$, and $p_i \parallel p_j$ for $i \neq j$. In that case, we write $\Delta \vdash s \stackrel{P}{\mathrel{+\!\!\!\!\!\rightarrow}}_{\mathcal{R}} t$ where $P = \{p_1, \ldots, p_n\}$ (P is uniquely determined from the derivation of $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$).

Lemma 5. *1. $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s$.*
2. If $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then $\Delta \vdash C[s] \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} C[t]$.
3. If $\Delta \vdash s \rightarrow_{\langle R, \pi, p, \sigma \rangle} t$ and $R \in \mathcal{R}$ then $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$.
4. If $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then $\Delta \vdash s \rightarrow^*_{\mathcal{R}} t$.

Proof. 1. By induction on s.
2. By induction on the context $C[\,]$.
3. By 2 and the rule (B).
4. By induction on the derivation of $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$. □

Lemma 6. *If $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then $\Delta \vdash \pi{\cdot}s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} \pi{\cdot}t$.*

Proof. By induction on the derivation of $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$. If the last applied rule in the derivation is (B), then we use Lemma 2. □

Lemma 7. *If $\Delta \vdash \sigma \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} \delta$ then $\Delta \vdash s\sigma \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s\delta$.*

Proof. By induction on s. If $s = \pi{\cdot}X$, then we use Lemma 6. □

Lemma 8. *Let $\mathcal{R}$ be a uniform nominal rewriting system. If $\Delta \vdash a\#s$ and $\Delta \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then $\Delta \vdash a\#t$.*

Proof. By Proposition 5 and Lemma 5(4). □

We define the notions in Definition 6 for $\mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}}$ as well. Our aim is to prove strong local confluence modulo $\approx_\alpha$ (Theorems 1 and 2), which together with strong compatibility with $\approx_\alpha$ (Lemma 9) yields Church-Rosser modulo $\approx_\alpha$ of $\mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}}$ (and hence of $\rightarrow_{\mathcal{R}}$).

Lemma 9 (Strong compatibility with $\approx_\alpha$). *Let $\mathcal{R}$ be a uniform rewriting system. If $\Delta \vdash s' \approx_\alpha s \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then there exists t' such that $\Delta \vdash s' \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t' \approx_\alpha t$.*

Proof. By induction on the derivation of $\Delta \vdash s \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t$. If the last applied rule in the derivation is (B), then the claim follows by Lemma 4. Among the other cases, we treat the case where $G = [a]\Box$. Then the last part of the derivation has the form

$$\frac{\Delta \vdash s_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t_1}{\Delta \vdash [a]s_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} [a]t_1}\ (\mathsf{C})$$

where $[a]s_1 = s$ and $[a]t_1 = t$. Now we have two cases.

(a) $s' = [a]s'_1$ and $\Delta \vdash [a]s'_1 \approx_\alpha [a]s_1$.
Then $\Delta \vdash s'_1 \approx_\alpha s_1$, and so by the induction hypothesis, there exists t'_1 such that $\Delta \vdash s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t'_1 \approx_\alpha t_1$. Hence we have $\Delta \vdash [a]s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} [a]t'_1 \approx_\alpha [a]t_1$.

(b) $s' = [b]s'_1$ and $\Delta \vdash [b]s'_1 \approx_\alpha [a]s_1$.
Then $\Delta \vdash s_1 \approx_\alpha (a\ b)\cdot s'_1$ and $\Delta \vdash a\#s'_1$. So by the induction hypothesis, there exists t'_1 such that $\Delta \vdash (a\ b)\cdot s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t'_1 \approx_\alpha t_1$. By taking $\pi = (a\ b)$ in Lemma 6, we have $\Delta \vdash s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} (a\ b)\cdot t'_1$, and by Lemma 8, we have $\Delta \vdash a\#(a\ b)\cdot t'_1$. Hence, we obtain the following derivations, from which the claim follows.

$$\frac{\Delta \vdash t'_1 \approx_\alpha t_1 \qquad \Delta \vdash a\#(a\ b)\cdot t'_1}{\Delta \vdash [b](a\ b)\cdot t'_1 \approx_\alpha [a]t_1} \quad \text{and} \quad \frac{\Delta \vdash s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} (a\ b)\cdot t'_1}{\Delta \vdash [b]s'_1 \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} [b](a\ b)\cdot t'_1}\ (\mathsf{C})$$

The cases where $G \neq [a]\Box$ are simpler. $\Box$

A key lemma to the parallel closure theorem is Lemma 11, which corresponds to Lemma 9.3.10 of [4] in the first-order case. Here we employ a version of the statement that can be adapted to cases where critical pairs exist. First we show a lemma to address the separated case of moderated variables.

Lemma 10. *Let $\mathcal{R}$ be a uniform rewriting system. Then, if $\Delta \vdash \nabla\sigma$, $\Delta \vdash s \approx_\alpha \pi\cdot X\sigma$ and $\Delta \vdash s \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t$ then there exists δ such that $\Delta \vdash \nabla\delta$, $\Delta \vdash t \approx_\alpha \pi\cdot X\delta$, $\Delta \vdash \sigma \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} \delta$ and for any $Y \neq X$, $Y\sigma = Y\delta$.*

Proof. From $\Delta \vdash s \approx_\alpha \pi\cdot X\sigma$, we have $\Delta \vdash \pi^{-1}\cdot s \approx_\alpha X\sigma$, and from $\Delta \vdash s \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t$, we have $\Delta \vdash \pi^{-1}\cdot s \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} \pi^{-1}\cdot t$ by Lemma 6. Hence by Lemma 9, there exists t' such that $\Delta \vdash X\sigma \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} t' \approx_\alpha \pi^{-1}\cdot t$. We take δ defined by $X\delta = t'$ and $Y\delta = Y\sigma$ for any $Y \neq X$. Then we have $\Delta \vdash t \approx_\alpha \pi\cdot X\delta$ and $\Delta \vdash \sigma \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} \delta$. Since $\mathcal{R}$ is uniform, it follows from Lemma 8 that if $\Delta \vdash a\#X\sigma$ then $\Delta \vdash a\#t'(= X\delta)$. Hence, from $\Delta \vdash \nabla\sigma$, we have $\Delta \vdash \nabla\delta$. $\Box$

Lemma 11. *Let $\mathcal{R}$ be a uniform rewriting system. Then, for any linear term l, if $\Delta \vdash \nabla^\pi\sigma$, $\Delta \vdash s \approx_\alpha l\sigma$ and $\Delta \vdash s \overset{P}{\mathrel{-\!\!\!+\!\!\!\!\rightarrow}}_{\mathcal{R}} t$ where $\forall p \in P.\, \exists o \in Pos_{\mathcal{X}}(l).\, o \preceq p$ then there exists δ such that $\Delta \vdash \nabla^\pi\delta$, $\Delta \vdash t \approx_\alpha l\delta$, $\Delta \vdash \sigma \mathrel{-\!\!\!+\!\!\!\!\rightarrow}_{\mathcal{R}} \delta$ and for any $X \notin V(l)$, $X\sigma = X\delta$.*

Proof. By induction on l. The case where l is a moderated variable $\pi \cdot X$ follows from Lemma 10. For the other cases, since $\forall p \in P. \exists o \in Pos_{\mathcal{X}}(l).\, o \preceq p$, the last rule used in the derivation of $\Delta \vdash s \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t$ must be (C). We proceed by case analysis according to the form of l. Here we consider the cases where $l = \langle l_1, \ldots, l_n \rangle$ and $l = [a]l_1$.

1. $l = \langle l_1, \ldots, l_n \rangle$. Since $\Delta \vdash s \approx_\alpha l\sigma$, s is of the form $\langle s_1, \ldots, s_n \rangle$. Then the last part of the derivation of $\Delta \vdash s \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t$ has the form
$$\frac{\Delta \vdash s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t_1 \quad \ldots \quad \Delta \vdash s_n \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t_n}{\Delta \vdash \langle s_1, \ldots, s_n \rangle \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} \langle t_1, \ldots, t_n \rangle}\ (\mathsf{C})$$
and for each $i \in \{1, \ldots, n\}$, $\Delta \vdash s_i \approx_\alpha l_i\sigma$. By the induction hypothesis, there exist δ_i's such that $\Delta \vdash \nabla^\pi \delta_i$, $\Delta \vdash t_i \approx_\alpha l_i\delta_i$, $\Delta \vdash \sigma \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} \delta_i$ and $\forall X \notin V(l_i).\, X\sigma = X\delta_i$. Since l is linear, we can take δ such that if $X \in V(l_i)$ then $X\delta = X\delta_i$ and if $X \notin V(l)$ then $X\delta = X\sigma$. It is easy to check that this δ satisfies the required condition.
2. $l = [a]l_1$. Since $\Delta \vdash s \approx_\alpha [a]l_1\sigma$, we have two cases.
   (a) $s = [a]s_1$. Then $\Delta \vdash s_1 \approx_\alpha l_1\sigma$, and the last part of the derivation of $\Delta \vdash s \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t$ has the form
   $$\frac{\Delta \vdash s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t_1}{\Delta \vdash [a]s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} [a]t_1}\ (\mathsf{C})$$
   Then by the induction hypothesis, there exists δ such that $\Delta \vdash \nabla^\pi \delta$, $\Delta \vdash t_1 \approx_\alpha l_1\delta$, $\Delta \vdash \sigma \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} \delta$ and $\forall X \notin V(l_1).\, X\sigma = X\delta$. By $\Delta \vdash t_1 \approx_\alpha l_1\delta$, we have $\Delta \vdash [a]t_1 \approx_\alpha [a]l_1\delta$. Since $V(l_1) = V(l)$, we have $\forall X \notin V(l).\, X\sigma = X\delta$. Thus we see that the claim holds.
   (b) $s = [b]s_1$. Then $\Delta \vdash (b\ a) \cdot s_1 \approx_\alpha l_1\sigma$, $\Delta \vdash a \# s_1$, and the last part of the derivation of $\Delta \vdash s \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t$ has the form
   $$\frac{\Delta \vdash s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t_1}{\Delta \vdash [b]s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} [b]t_1}\ (\mathsf{C})$$
   From $\Delta \vdash s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} t_1$, we have $\Delta \vdash (b\ a) \cdot s_1 \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} (b\ a) \cdot t_1$ by Lemma 6. Since $\mathcal{R}$ is uniform, it also follows $\Delta \vdash a \# t_1$ by Lemma 8. Hence $\Delta \vdash b \# (b\ a) \cdot t_1$. Thus, by the induction hypothesis, there exists δ such that $\Delta \vdash \nabla^\pi \delta$, $\Delta \vdash (b\ a) \cdot t_1 \approx_\alpha l_1\delta$, $\Delta \vdash \sigma \twoheadrightarrow\!\!\!\!\!+\!\!\!\!+_{\mathcal{R}} \delta$ and $\forall X \notin V(l_1).\, X\sigma = X\delta$. Then from $\Delta \vdash (b\ a) \cdot t_1 \approx_\alpha l_1\delta$ and $\Delta \vdash a \# t_1$, it follows that $\Delta \vdash [b]t_1 \approx_\alpha [a]l_1\delta$. Since $V(l_1) = V(l)$, we see that the claim holds. □

3.2 Confluence of left-linear parallel closed rewriting systems

In this subsection, we prove the main theorems of the paper: the parallel closure theorem (Theorem 1) and its generalisation (Theorem 2).

First, we state a lemma concerning substitutions.

Lemma 12 ([8]). *Let σ and σ' be substitutions such that $\forall X \in \mathcal{X}.\, \Delta \vdash X\sigma \approx_\alpha X\sigma'$. Then $\Delta \vdash t\sigma \approx_\alpha t\sigma'$ for any term t.*

The following can be seen as a critical pair lemma for left-linear systems.

Lemma 13. *Let $\mathcal{R}$ be a left-linear uniform rewriting system and let $R \in \mathcal{R}$. If $\Delta \vdash s_1 \xleftarrow{\varepsilon}_R s \xrightarrow{P}\!\!\!\!\!\!\!\!+\!\!\!\!+\;_{\mathcal{R}} s_2$ then one of the following holds:*

1. *There exists a term t such that $\Delta \vdash s_1 \twoheadrightarrow_{\mathcal{R}} t \leftarrow_R s_2$.*
2. *There exist $p \in P$, $R' \in \mathcal{R}$, $\Gamma \vdash \langle u, v\rangle \in BCP(R', R)$, s', π and θ such that $\Delta \vdash s \xrightarrow{p}_{R'} s' \xrightarrow{P\setminus\{p\}}_{\mathcal{R}} s_2$, $\Delta \vdash \Gamma^\pi\theta$, $\Delta \vdash s' \approx_\alpha u^\pi\theta$ and $\Delta \vdash s_1 \approx_\alpha v^\pi\theta$.*

Proof. Let $R = \nabla \vdash l \to r \in \mathcal{R}$, and suppose $\Delta \vdash s_1 \leftarrow_{\langle R,\pi,\varepsilon,\sigma\rangle} s \xrightarrow{P}_{\mathcal{R}} s_2$. Then by the definition of rewrite relation, we have $\Delta \vdash \nabla^\pi\sigma$, $\Delta \vdash s \approx_\alpha l^\pi\sigma$ and $s_1 = r^\pi\sigma$. Now we distinguish two cases.

– Case $\forall p \in P.\, \exists o \in Pos_{\mathcal{X}}(l).\, o \preceq p$.
Then by Lemma 11, there exists δ such that $\Delta \vdash \nabla^\pi\delta$, $\Delta \vdash s_2 \approx_\alpha l^\pi\delta$ and $\Delta \vdash \sigma \twoheadrightarrow_{\mathcal{R}} \delta$. Hence we have $\Delta \vdash s_2 \to_{\langle R,\pi,\varepsilon,\delta\rangle} r^\pi\delta$, and by Lemma 7, $\Delta \vdash r^\pi\sigma \twoheadrightarrow_{\mathcal{R}} r^\pi\delta$. Thus, part 1 of the claim holds.

– Case $\exists p \in P.\, \neg\exists o \in Pos_{\mathcal{X}}(l).\, o \preceq p$.
Then $p \in Pos(l) \setminus Pos_{\mathcal{X}}(l)$, and $\Delta \vdash s \to_{\langle R',\pi',p,\sigma'\rangle} s' \xrightarrow{P\setminus\{p\}}_{\mathcal{R}} s_2$ for some $R' = \nabla' \vdash l' \to r' \in \mathcal{R}$, π', σ' and s'. Let L be the context with $l = L[l|_p]_p$. First we show claim I: the set $\nabla' \cup \nabla^{\breve{\pi}} \cup \{l' \approx l^{\breve{\pi}}|_p\}$ is unifiable for some $\breve{\pi}$.

(Proof of claim I) By the definition of rewrite steps, we have $\Delta \vdash \nabla'^{\pi'}\sigma', \nabla^\pi\sigma,\ s|_p \approx_\alpha l'^{\pi'}\sigma', s \approx_\alpha l^\pi\sigma$. Thus, $\Delta \vdash s[l'^{\pi'}\sigma']_p \approx_\alpha s[s|_p]_p = s \approx_\alpha l^\pi\sigma$. Hence, $\Delta \vdash s[l'^{\pi'}\sigma']_p \approx_\alpha L^\pi\sigma[l^\pi|_p\sigma]_p$. Now, by Lemma 3, there exists $\hat{\pi}$ such that

$$\Delta \vdash l'^{\pi'}\sigma' \approx_\alpha \hat{\pi}\cdot(l^\pi|_p\sigma) \tag{3.1}$$

$$\Delta \vdash s[r'^{\pi'}\sigma']_p \approx_\alpha L^\pi\sigma[\hat{\pi}^{-1}\cdot(r'^{\pi'}\sigma')]_p \tag{3.2}$$

From $\Delta \vdash \nabla'^{\pi'}\sigma', \nabla^\pi\sigma$ and (3.1), we have

$$\Delta \vdash \nabla'(\pi'^{-1}\cdot\sigma'), \nabla^{\pi'^{-1}\circ\hat{\pi}\circ\pi}((\pi'^{-1}\circ\hat{\pi})\cdot\sigma)$$

$$\Delta \vdash l'(\pi'^{-1}\cdot\sigma') \approx_\alpha l^{\pi'^{-1}\circ\hat{\pi}\circ\pi}|_p((\pi'^{-1}\circ\hat{\pi})\cdot\sigma) \tag{3.3}$$

Now, let $\breve{\pi} = \pi'^{-1}\circ\hat{\pi}\circ\pi$ and let $\breve{\sigma}$ be the substitution such that $\breve{\sigma}(X) = (\pi'^{-1}\cdot\sigma')(X)$ for $X \in V(l')$, $\breve{\sigma}(X) = ((\pi'^{-1}\circ\hat{\pi})\cdot\sigma)(X)$ for $X \in V(l)$, and $\breve{\sigma}(X) = X$ otherwise, where we assume w.l.o.g. $V(l') \cap V(l) = \emptyset$. Then, the statement (3.3) equals $\Delta \vdash \nabla'\breve{\sigma}, \nabla^{\breve{\pi}}\breve{\sigma}, l'\breve{\sigma} \approx_\alpha l^{\breve{\pi}}|_p\breve{\sigma}$.

(End of the proof of claim I)

Thus, $\nabla' \cup \nabla^{\breve{\pi}} \cup \{l' \approx l^{\breve{\pi}}|_p\}$ is unifiable. Hence we have $\Gamma \vdash \langle L^{\breve{\pi}}\theta[r'\theta]_p, r^{\breve{\pi}}\theta\rangle \in BCP(R', R)$ where $\langle \Gamma, \theta\rangle$ is an mgu and so there is a substitution δ such that

$$\Delta \vdash \Gamma\delta \tag{3.4}$$

$$\forall X \in \mathcal{X}.\, \Delta \vdash X\theta\delta \approx_\alpha X\breve{\sigma} \tag{3.5}$$

Let $u = L^{\breve{\pi}}\theta[r'\theta]_p$ and $v = r^{\breve{\pi}}\theta$. In the following, we show claim II: with the BCP $\Gamma \vdash \langle u, v\rangle$, part 2 of the statement of the lemma holds.

(Proof of claim II) From the property (3.5) and Lemma 12, we have $\Delta \vdash r^{\breve{\pi}}\theta\delta \approx_\alpha r^{\breve{\pi}}\breve{\sigma}$. Hence $\Delta \vdash v\delta \approx_\alpha r^{\pi'^{-1}\circ\hat{\pi}\circ\pi}((\pi'^{-1}\circ\hat{\pi})\cdot\sigma)$, which means $\Delta \vdash v^{\hat{\pi}^{-1}\circ\pi'}((\hat{\pi}^{-1}\circ\pi')\cdot\delta) \approx_\alpha r^\pi\sigma$. Now, let $\hat{\pi}' = \hat{\pi}^{-1}\circ\pi'$ and $\delta' = (\hat{\pi}^{-1}\circ\pi')\cdot\delta$. Then we have $\Delta \vdash v^{\hat{\pi}'}\delta' \approx_\alpha r^\pi\sigma = s_1$. Also, from the property (3.4), we have $\Delta \vdash \Gamma^{\hat{\pi}'}\delta'$. It only remains to show $\Delta \vdash u^{\hat{\pi}'}\delta' \approx_\alpha s'$. Again, from the property (3.5) and Lemma 12, we have $\Delta \vdash L^{\breve{\pi}}[r']_p\theta\delta \approx_\alpha L^{\breve{\pi}}[r']_p\breve{\sigma}$. Hence $\Delta \vdash u\delta \approx_\alpha L^{\breve{\pi}}[r']_p\breve{\sigma} = L^{\breve{\pi}}\breve{\sigma}[r'\breve{\sigma}]_p = L^{\pi'^{-1}\circ\hat{\pi}\circ\pi}((\pi'^{-1}\circ\hat{\pi})\cdot\sigma)[r'(\pi'^{-1}\cdot\sigma')]_p$. Equivalently, $\Delta \vdash u^{\hat{\pi}^{-1}\circ\pi'}((\hat{\pi}^{-1}\circ\pi')\cdot\delta) \approx_\alpha L^\pi\sigma[\hat{\pi}^{-1}\cdot(r'^{\pi'}\sigma')]_p$. From this and (3.2), we have $\Delta \vdash u^{\hat{\pi}^{-1}\circ\pi'}((\hat{\pi}^{-1}\circ\pi')\cdot\delta) \approx_\alpha s[r'^{\pi'}\sigma']_p$, which means $\Delta \vdash u^{\hat{\pi}'}\delta' \approx_\alpha s[r'^{\pi'}\sigma']_p = s'$. (End of the proof of claim II)

□

Before proceeding to Theorem 1, we state one more lemma.

Lemma 14. *1. If $\Gamma \vdash s \approx_\alpha t$ and $\Delta \vdash \Gamma^\pi\theta$ then $\Delta \vdash s^\pi\theta \approx_\alpha t^\pi\theta$.*
2. If $\Gamma \vdash s \to_R t$ and $\Delta \vdash \Gamma^\pi\theta$ then $\Delta \vdash s^\pi\theta \to_R t^\pi\theta$.
3. If $\Gamma \vdash s \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t$ and $\Delta \vdash \Gamma^\pi\theta$ then $\Delta \vdash s^\pi\theta \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t^\pi\theta$.

Now we show the parallel closure theorem which states that $\mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}}$ is strongly locally confluent modulo $\approx_\alpha$ for a class of left-linear nominal rewriting systems.

Definition 8. A nominal rewriting system $\mathcal{R}$ is *parallel closed* if for any $\Gamma \vdash \langle u, v\rangle \in BCP(\mathcal{R})$, $\Gamma \vdash u\ (\mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}}\circ \approx_\alpha)\ v$. A nominal rewriting system $\mathcal{R}$ is *weakly orthogonal* if it is left-linear and for any $\Gamma \vdash \langle u, v\rangle \in BCP(\mathcal{R})$, $\Gamma \vdash u \approx_\alpha v$.

Theorem 1 (Parallel closure theorem). *Let $\mathcal{R}$ be a left-linear parallel closed uniform rewriting system. If $\Delta \vdash t \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t_1$ and $\Delta \vdash t \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t_2$ then there exist t'_1 and t'_2 such that $\Delta \vdash t_1 \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t'_1$, $\Delta \vdash t_2 \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} t'_2$ and $\Delta \vdash t'_1 \approx_\alpha t'_2$.*

Proof. Suppose $\Delta \vdash t \xrightarrow{P_1}\!\!\!\!\!\!+_{\mathcal{R}} t_1$ and $\Delta \vdash t \xrightarrow{P_2}\!\!\!\!\!\!+_{\mathcal{R}} t_2$ where $P_1 = \{p_{11}, \ldots, p_{1m}\}$ and $P_2 = \{p_{21}, \ldots, p_{2n}\}$. We set subterm occurrences $\alpha_i = t|_{p_{1i}} (1 \le i \le m)$ and $\beta_j = t|_{p_{2j}} (1 \le j \le n)$, and let $Red_{in} = \{\alpha_i \mid \exists\beta_j.\, \alpha_i \subset \beta_j\} \cup \{\beta_j \mid \exists\alpha_i.\, \beta_j \subseteq \alpha_i\}$ and $Red_{out} = \{\alpha_i \mid \forall\beta_j.\, \alpha_i \not\subseteq \beta_j\} \cup \{\beta_j \mid \forall\alpha_i.\, \beta_j \not\subseteq \alpha_i\}$. We define $|Red_{in}|$ as $\sum_{\gamma\in Red_{in}}|\gamma|$. The proof of the claim is by induction on $|Red_{in}|$.

- Case $|Red_{in}| = 0$.
  Then we can write $t = C[s_{11}, \ldots, s_{1m}, s_{21}, \ldots, s_{2n}]_{p_{11},\ldots,p_{1m},p_{21},\ldots,p_{2n}}$, $t_1 = C[s'_{11}, \ldots, s'_{1m}, s_{21}, \ldots, s_{2n}]$ and $t_2 = C[s_{11}, \ldots, s_{1m}, s'_{21}, \ldots, s'_{2n}]$ where C is some context, $\Delta \vdash s_{1i} \to_R s'_{1i} (1 \le i \le m)$ and $\Delta \vdash s_{2j} \to_R s'_{2j} (1 \le j \le n)$. Hence, the claim follows by taking $t'_1 = t'_2 = C[s'_{11}, \ldots, s'_{1m}, s'_{21}, \ldots, s'_{2n}]$.
- Case $|Red_{in}| > 0$.
  Suppose $Red_{out} = \{s_1, \ldots, s_h\}$. Then we can write $t = C[s_1, \ldots, s_h]$, $t_1 = C[s_{11}, \ldots, s_{h1}]$ and $t_2 = C[s_{12}, \ldots, s_{h2}]$ where for each k with $1 \le k \le h$, $\Delta \vdash s_k \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s_{k1}$, $\Delta \vdash s_k \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s_{k2}$ and one of them is at the root. Now, to prove the claim, it is sufficient to show that for each k with $1 \le k \le h$, there exist s'_{k1} and s'_{k2} such that $\Delta \vdash s_{k1} \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s'_{k1}$, $\Delta \vdash s_{k2} \mathrel{+\!\!\!\!\!\rightarrow}_{\mathcal{R}} s'_{k2}$ and $\Delta \vdash s'_{k1} \approx_\alpha s'_{k2}$.

Let $1 \leq k \leq h$, and suppose $\Delta \vdash s_k \overset{\{\varepsilon\}}{\twoheadrightarrow}_{\mathcal{R}} s_{k1}$ and $\Delta \vdash s_k \overset{P}{\twoheadrightarrow}_{\mathcal{R}} s_{k2}$. (The symmetric case is proved similarly.) Then there exists $R \in \mathcal{R}$ such that $\Delta \vdash s_k \xrightarrow{\varepsilon}_R s_{k1}$. Hence by Lemma 13, one of the following holds:

1. There exists a term $\hat{s}_k$ such that $\Delta \vdash s_{k1} \twoheadrightarrow_{\mathcal{R}} \hat{s}_k \leftarrow_R s_{k2}$.
2. There exist $p \in P$, $R' \in \mathcal{R}$, $\Gamma \vdash \langle u, v\rangle \in BCP(R', R)$, s'_k, π and θ such that $\Delta \vdash s_k \xrightarrow{p}_{R'} s'_k \overset{P\setminus\{p\}}{\twoheadrightarrow}_{\mathcal{R}} s_{k2}$, $\Delta \vdash \Gamma^\pi\theta$, $\Delta \vdash s'_k \approx_\alpha u^\pi\theta$ and $\Delta \vdash s_{k1} \approx_\alpha v^\pi\theta$.

If part 1 holds then the requirement is satisfied. So we treat the case where part 2 holds. Since $\mathcal{R}$ is parallel closed, there exists w such that $\Gamma \vdash u \twoheadrightarrow_{\mathcal{R}} w \approx_\alpha v$. Then by Lemma 14(1) and (3), we have $\Delta \vdash u^\pi\theta \twoheadrightarrow_{\mathcal{R}} w^\pi\theta \approx_\alpha v^\pi\theta \approx_\alpha s_{k1}$. Hence by Lemma 9, there exists $\hat{s}_{k1}$ such that $\Delta \vdash s'_k \twoheadrightarrow_{\mathcal{R}} \hat{s}_{k1} \approx_\alpha w^\pi\theta \approx_\alpha s_{k1}$.
In the following, we intend to apply the induction hypothesis to the parallel peak $\Delta \vdash s'_k \overset{Q}{\twoheadrightarrow}_{\mathcal{R}} \hat{s}_{k1}$ and $\Delta \vdash s'_k \overset{P\setminus\{p\}}{\twoheadrightarrow}_{\mathcal{R}} s_{k2}$.
Let $P \setminus \{p\} = \{p_1, \ldots, p_{n'-1}\}$ $(n' \geq 1)$. We are now considering a case where $s_k = \alpha_i$ for some i $(1 \leq i \leq m)$, and a set of occurrences $\{\beta_{j_1}, \ldots, \beta_{j_{n'}}\}$ as $\{\beta_j \mid \beta_j \subseteq \alpha_i\}$. Then, clearly $\sum_{l=1}^{n'} |\beta_{j_l}| \leq |Red_{in}|$. We also have $s_k|_p = \beta_{j_{l'}}$ for some l' $(1 \leq l' \leq n')$, and $\{s_k|_{p_1}, \ldots, s_k|_{p_{n'-1}}\} = \{s'_k|_{p_1}, \ldots, s'_k|_{p_{n'-1}}\} = \{\beta_{j_1}, \ldots, \beta_{j_{n'}}\} \setminus \{\beta_{j_{l'}}\}$. Now let $Q = \{q_1, \ldots, q_{m'}\}$. Let $\gamma_{i'} = s'_k|_{q_{i'}} (1 \leq i' \leq m')$ and $\rho_{j'} = s'_k|_{p_{j'}} (1 \leq j' \leq n'-1)$, and let $Red'_{in} = \{\gamma_{i'} \mid \exists\rho_{j'}.\, \gamma_{i'} \subset \rho_{j'}\} \cup \{\rho_{j'} \mid \exists\gamma_{i'}.\, \rho_{j'} \subseteq \gamma_{i'}\}$. Then, $|Red'_{in}| \leq \sum_{j'=1}^{n'-1} |\rho_{j'}| < \sum_{j'=1}^{n'-1} |\rho_{j'}| + |\beta_{j_{l'}}| = \sum_{l=1}^{n'} |\beta_{j_l}|$. Hence we can apply the induction hypothesis to the parallel peak $\Delta \vdash s'_k \overset{Q}{\twoheadrightarrow}_{\mathcal{R}} \hat{s}_{k1}$ and $\Delta \vdash s'_k \overset{P\setminus\{p\}}{\twoheadrightarrow}_{\mathcal{R}} s_{k2}$, and obtain $\hat{s}'_{k1}$ and s'_{k2} such that $\Delta \vdash \hat{s}_{k1} \twoheadrightarrow_{\mathcal{R}} \hat{s}'_{k1}$, $\Delta \vdash s_{k2} \twoheadrightarrow_{\mathcal{R}} s'_{k2}$ and $\Delta \vdash \hat{s}'_{k1} \approx_\alpha s'_{k2}$. Since $\Delta \vdash \hat{s}_{k1} \approx_\alpha s_{k1}$, we have, by Lemma 9, some s'_{k1} such that $\Delta \vdash s_{k1} \twoheadrightarrow_{\mathcal{R}} s'_{k1} \approx_\alpha \hat{s}'_{k1} \approx_\alpha s'_{k2}$ as required. □

We are now ready to show that $\rightarrow_{\mathcal{R}}$ is Church-Rosser modulo $\approx_\alpha$.

Corollary 1 (Church-Rosser modulo $\approx_\alpha$). *If $\mathcal{R}$ is a left-linear parallel closed uniform rewriting system, then $\rightarrow_{\mathcal{R}}$ is Church-Rosser modulo $\approx_\alpha$. In particular, if $\mathcal{R}$ is a weakly orthogonal uniform rewriting system, then $\rightarrow_{\mathcal{R}}$ is Church-Rosser modulo $\approx_\alpha$.*

Proof. By Lemma 9, $\twoheadrightarrow_{\mathcal{R}}$ is strongly compatible with $\approx_\alpha$, and by Theorem 1, $\twoheadrightarrow_{\mathcal{R}}$ is strongly locally confluent modulo $\approx_\alpha$. Hence by the results in [14] (see also [15, Section 2.5]), $\twoheadrightarrow_{\mathcal{R}}$ is Church-Rosser modulo $\approx_\alpha$. Since $\rightarrow_{\mathcal{R}} \subseteq \twoheadrightarrow_{\mathcal{R}} \subseteq \rightarrow^*_{\mathcal{R}}$ by Lemma 5, we see that $\rightarrow_{\mathcal{R}}$ is Church-Rosser modulo $\approx_\alpha$. □

As in the first-order term rewriting case [21], we can generalise the above result by analysing overlaps at the root in the proof of Theorem 1.

Theorem 2. *Suppose that $\mathcal{R}$ is a left-linear uniform rewriting system. Then, $\mathcal{R}$ is Church-Rosser modulo $\approx_\alpha$ if $\Gamma \vdash u\ (\twoheadrightarrow_{\mathcal{R}} \circ \approx_\alpha)\ v$ for any $\Gamma \vdash \langle u, v\rangle \in BCP_{in}(\mathcal{R})$ and $\Gamma \vdash u\ (\twoheadrightarrow_{\mathcal{R}} \circ \approx_\alpha \circ \leftarrow^*_{\mathcal{R}})\ v$ for any $\Gamma \vdash \langle u, v\rangle \in BCP_{out}(\mathcal{R})$,* *where $BCP_{in}(\mathcal{R})$ and $BCP_{out}(\mathcal{R})$ denote the sets of BCPs of $\mathcal{R}$ such that $p \neq \varepsilon$ and $p = \varepsilon$ in the definition of BCP (Definition 4), respectively.*

Proof. To show that $\twoheadrightarrow\!\!\!\!\!+\!\!\!\to_{\mathcal{R}}$ is strongly locally confluent modulo $\approx_\alpha$, we prove a modified statement of Theorem 1 with $\Delta \vdash t_2 \to^*_{\mathcal{R}} t'_2$ instead of $\Delta \vdash t_2 \twoheadrightarrow\!\!\!\!\!+\!\!\!\to_{\mathcal{R}} t'_2$. The proof proceeds in a similar way to that of Theorem 1. In the case where $\Gamma \vdash \langle u, v\rangle \in BCP(R', R)$ in part 2 is at the root, we use the assumption on $BCP_{out}(\mathcal{R})$. $\square$

We demonstrate Theorem 2 on two examples.

Example 1. Consider a nominal signature with function symbols f and g. Let $\mathcal{R}_1$ be the following left-linear uniform rewriting system:

$$\mathcal{R}_1 = \begin{cases} \vdash \mathsf{f}\ \langle [a]X, Y\rangle \to \mathsf{f}\ \langle [a]X, [a]X\rangle & \text{(1-1)} \\ \vdash \mathsf{f}\ \langle [a]a, Y\rangle \to \mathsf{g} & \text{(1-2)} \end{cases}$$

In the following, we write down all patterns of the BCPs of $\mathcal{R}_1$ and check whether $\mathcal{R}_1$ satisfies the condition of Theorem 2.

First, consider BCPs induced by overlaps of (1-1) on its renamed variant, which arise from the unification problem $\{\mathsf{f}\ \langle [a]X, Y\rangle \approx (\mathsf{f}\ \langle [a]Z, W\rangle)^\pi|_\varepsilon(= \mathsf{f}\ \langle [\pi(a)]Z, W\rangle)\}$. If $\pi(a) = a$, then the BCP is $\vdash \langle \mathsf{f}\ \langle [a]Z, [a]Z\rangle,\ \mathsf{f}\ \langle [a]Z, [a]Z\rangle\rangle$, for which $\vdash \mathsf{f}\ \langle [a]Z, [a]Z\rangle \approx_\alpha \mathsf{f}\ \langle [a]Z, [a]Z\rangle$ holds. If $\pi(a) = b$, then the problem $\{\mathsf{f}\ \langle [a]X, Y\rangle \approx \mathsf{f}\ \langle [b]Z, W\rangle\}$ has an mgu $\langle\{a\#Z\},\ \{X := (a\ b){\cdot}Z,\ Y := W\}\rangle$. Hence, the BCP in this case is $a\#Z \vdash \langle \mathsf{f}\ \langle [a](a\ b){\cdot}Z, [a](a\ b){\cdot}Z\rangle,\ \mathsf{f}\ \langle [b]Z, [b]Z\rangle\rangle$, for which we have $a\#Z \vdash \mathsf{f}\ \langle [a](a\ b){\cdot}Z, [a](a\ b){\cdot}Z\rangle \approx_\alpha \mathsf{f}\ \langle [b]Z, [b]Z\rangle$.

The BCP induced by overlaps of (1-2) on its renamed variant is only $\vdash \langle \mathsf{g}, \mathsf{g}\rangle$, for which we have $\vdash \mathsf{g} \approx_\alpha \mathsf{g}$.

Next we consider BCPs induced by overlaps of (1-1) on (1-2) and vice versa. The former arise from the unification problem $\{\mathsf{f}\ \langle [a]X, Y\rangle \approx (\mathsf{f}\ \langle [a]a, Z\rangle)^\pi|_\varepsilon(= \mathsf{f}\ \langle [\pi(a)]\pi(a), Z\rangle)\}$. In either case of $\pi(a) = a$ and $\pi(a) = b$, the BCP is $\vdash \langle \mathsf{f}\ \langle [a]a, [a]a\rangle,\ \mathsf{g}\rangle$, for which we have $\vdash \mathsf{f}\ \langle [a]a, [a]a\rangle \twoheadrightarrow\!\!\!\!\!+\!\!\!\to_{\mathcal{R}_1} \mathsf{g}$. BCPs induced by overlaps of (1-2) on (1-1) arise from the unification problem $\{\mathsf{f}\ \langle [a]a, Y\rangle \approx (\mathsf{f}\ \langle [a]X, Z\rangle)^\pi|_\varepsilon(= \mathsf{f}\ \langle [\pi(a)]X, Z\rangle)\}$. If $\pi(a) = a$, then the problem has an mgu $\langle\emptyset,\ \{X := a,\ Y := Z\}\rangle$. Hence, the BCP in this case is $\vdash \langle \mathsf{g},\ \mathsf{f}\ \langle [a]a, [a]a\rangle\rangle$, for which we have $\vdash \mathsf{g} \leftarrow^*_{\mathcal{R}_1} \mathsf{f}\ \langle [a]a, [a]a\rangle$. If $\pi(a) = b$, then the problem has an mgu $\langle\emptyset,\ \{X := b,\ Y := Z\}\rangle$. Hence, the BCP in this case is $\vdash \langle \mathsf{g},\ \mathsf{f}\ \langle [b]b, [b]b\rangle\rangle$, for which we have $\vdash \mathsf{g} \leftarrow^*_{\mathcal{R}_1} \mathsf{f}\ \langle [b]b, [b]b\rangle$.

We have seen that $\mathcal{R}_1$ satisfies the condition of Theorem 2. Thus we conclude that $\mathcal{R}_1$ is Church-Rosser modulo $\approx_\alpha$. $\square$

The reader may wonder why the case analyses according to permutations in the above example are necessary. This is because there exist rewriting systems where choice of bound atoms in the same two rewrite rules can vary joinability of the induced critical pairs (cf. [20, Example 12]). That means that one has to check all combinations of atoms in the rules to guarantee confluence properties of nominal rewriting systems.

The next example demonstrates that our results can also be applied to nominal rewriting systems that are not α-stable [19] (i.e., applying the same rewrite step to two α-equivalent terms may result in terms that are not α-equivalent). A typical example of a non-α-stable rewriting system is found in [19, Example 19] (unconditional eta-expansion). See also [3, Example 4.3].

Example 2. Consider a nominal signature with function symbols f and g. Let $\mathcal{R}_2$ be the following left-linear uniform rewriting system:

$$\mathcal{R}_2 = \begin{cases} \vdash \mathsf{f}\ X \to \mathsf{f}\ [a]\langle X, X\rangle & \text{(2-1)} \\ \vdash [a]X \to \mathsf{g} & \text{(2-2)} \end{cases}$$

Since $\mathcal{R}_2$ is not α-stable, the confluence criterion by orthogonality in [19] cannot be applied. In the following, we write down all patterns of the BCPs of $\mathcal{R}_2$ and check whether $\mathcal{R}_2$ satisfies the condition of Theorem 2.

First, consider BCPs induced by overlaps of (2-1) on its renamed variant, which arise from the unification problem $\{\mathsf{f}\ X \approx (\mathsf{f}\ Y)^\pi|_\varepsilon (= \mathsf{f}\ Y)\}$. If $\pi(a) = a$, then the BCP is $\vdash \langle \mathsf{f}\ [a]\langle Y, Y\rangle, \mathsf{f}\ [a]\langle Y, Y\rangle\rangle$, for which we have $\vdash \mathsf{f}\ [a]\langle Y, Y\rangle \approx_\alpha \mathsf{f}\ [a]\langle Y, Y\rangle$. If $\pi(a) = b$, then the BCP is $\vdash \langle \mathsf{f}\ [a]\langle Y, Y\rangle, \mathsf{f}\ [b]\langle Y, Y\rangle\rangle$, for which we have $\vdash \mathsf{f}\ [a]\langle Y, Y\rangle \to_{\mathcal{R}_2} \mathsf{f}\ \mathsf{g} \leftarrow_{\mathcal{R}_2} \mathsf{f}\ [b]\langle Y, Y\rangle$.

Next we consider BCPs induced by overlaps of (2-2) on its renamed variant, which arise from the unification problem $\{[a]X \approx ([a]Y)^\pi|_\varepsilon (= [\pi(a)]Y)\}$. If $\pi(a) = a$, then the BCP is $\vdash \langle \mathsf{g}, \mathsf{g}\rangle$, for which we have $\vdash \mathsf{g} \approx_\alpha \mathsf{g}$. If $\pi(a) = b$, then the problem $\{[a]X \approx [b]Y\}$ has an mgu $\langle\{a\#Y\}, \{X := (a\ b){\cdot}Y\}\rangle$. Hence, the BCP in this case is $a\#Y \vdash \langle \mathsf{g}, \mathsf{g}\rangle$, for which we have $a\#Y \vdash \mathsf{g} \approx_\alpha \mathsf{g}$.

We have seen that $\mathcal{R}_2$ satisfies the condition of Theorem 2. Thus we conclude that $\mathcal{R}_2$ is Church-Rosser modulo $\approx_\alpha$. □

4 Conclusion

We have presented proofs of Church-Rosser modulo $\approx_\alpha$ for some classes of left-linear uniform nominal rewriting systems, extending Huet's parallel closure theorem and its generalisation on confluence of left-linear term rewriting systems. In the presence of critical pairs, the proofs are more delicate than the previous proofs for orthogonal uniform nominal rewriting systems. Our theorems can be applied to nominal rewriting systems that are not α-stable, as we have seen in an example.

In traditional higher-order rewriting frameworks (e.g. [12, 13]), α-equivalent terms are always identified in contrast to the framework of nominal rewriting. This makes effects on confluence in the two approaches rather different. In addition to the difference revealed in [20], we have seen that our results on the parallel closure theorem and its generalisation are incomparable with those in traditional higher-order rewriting formalisms, since nominal rewriting systems that are not α-stable cannot be represented by any systems in traditional rewriting formalisms. Also, it is known that under explicit α-equivalence, confluence of β-reduction in λ-calculus is already quite hard to show (cf. [23]). Up to our knowledge, there are no attempts to accomplish a similar effect in traditional higher-order rewriting frameworks.

On the other hand, it is known that in the case of traditional higher-order rewriting, results on confluence by parallel closed critical pairs can be extended to those by development closed critical pairs [16]. However, a rigorous proof of it becomes more complicated than the parallel case, and in the present paper, we have not tried that extension for the case of nominal rewriting. We expect that the extension is possible but it is not entirely an easy task.

Using the combination of all the methods of [19, 20] and the present paper, we have implemented a confluence prover [1]. We use an equivariant unification algorithm [2, 6] to check whether $\nabla_1 \cup \nabla_2^\pi \cup \{l_1 \approx l_2^\pi|_p\}$ is unifiable for some permutation π, for given $\nabla_1, \nabla_2, l_1, l_2|_p$. However, that is not enough to generate concrete critical pairs and check their joinability, parallel closedness, etc. It is necessary to instantiate atom variables and permutation variables from constraints obtained as the solutions of equivariant unification problems, and this process is not obvious. We refer to [1] for all details of the implementation and experiments.

Acknowledgements. We are grateful to the anonymous referees for valuable comments. This research was supported by JSPS KAKENHI Grant Numbers 15K00003 and 16K00091.

References

1. Aoto, T., Kikuchi, K.: Nominal confluence tool. In: Olivetti, N., Tiwari, A. (eds.) IJCAR 2016. LNCS, vol. 9706, pp. 173–182. Springer-Verlag (2016)
2. Aoto, T., Kikuchi, K.: A rule-based procedure for equivariant nominal unification. In: Proceedings of the 8th HOR (2016)
3. Ayala-Rincón, M., Fernández, M., Gabbay, M.J., Rocha-Oliveira, A.C.: Checking overlaps of nominal rewriting rules. Electronic Notes in Theoretical Computer Science 323, 39–56 (2016)
4. Baader, F., Nipkow, T.: Term Rewriting and All That. Cambridge University Press (1998)
5. de Bruijn, N.G.: Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. Indagationes Mathematicae 34, 381–392 (1972)
6. Cheney, J.: Equivariant unification. J. Autom. Reasoning 45, 267–300 (2010)
7. Comon, H.: Completion of rewritie systems with membership constraints. Part I: deduction rules. Journal of Symbolic Computation 25, 397–419 (1998)
8. Fernández, M., Gabbay, M.J.: Nominal rewriting. Inform. Comput. 205, 917–965 (2007)
9. Gabbay, M.J., Pitts, A.M.: A new approach to abstract syntax with variable binding. Formal Aspects Comput. 13, 341–363 (2002)
10. Huet, G.: Confluent reductions: abstract properties and applications to term rewriting systems. J. ACM 27, 797–821 (1980)
11. Jounnaud, J.P., Kirchner, H.: Completion of a set of rules modulo a set of equations. SIAM J. Comput. 15, 1155–1194 (1986)

12. Klop, J.W., van Oostrom, V., van Raamsdonk, F.: Combinatory reduction systems: introduction and survey. Theoret. Comput. Sci. 121, 279–308 (1993)
13. Mayr, R., Nipkow, T.: Higher-order rewrite systems and their confluence. Theoret. Comput. Sci. 192, 3–29 (1998)
14. Ohlebusch, E.: Church-Rosser theorems for abstract reduction modulo an equivalence relation. In: Proceedings of the 9th RTA. LNCS, vol. 1379, pp. 17–31. Springer-Verlag (1998)
15. Ohlebusch, E.: Advanced Topics in Term Rewriting. Springer-Verlag (2002)
16. van Oostrom, V.: Developing developments. Theoret. Comput. Sci. 175, 159–181 (1997)
17. Pitts, A.M.: Nominal logic, a first order theory of names and binding. Inform. Comput. 186, 165–193 (2003)
18. Pollack, R., Sato, M., Ricciotti, W.: A canonical locally named representation of binding. J. Autom. Reasoning 49, 185–207 (2012)
19. Suzuki, T., Kikuchi, K., Aoto, T., Toyama, Y.: Confluence of orthogonal nominal rewriting systems revisited. In: Proceedings of the 26th RTA. LIPIcs, vol. 36, pp. 301–317 (2015)
20. Suzuki, T., Kikuchi, K., Aoto, T., Toyama, Y.: Critical pair analysis in nominal rewriting. In: Proceedings of the 7th SCSS. EPiC, vol. 39, pp. 156–168. EasyChair (2016)
21. Toyama, Y.: Commutativity of term rewriting systems. In: Fuchi, K., Kott, L. (eds.) Programming of Future Generation Computers II, pp. 393–407. North-Holland (1988)
22. Urban, C., Pitts, A.M., Gabbay, M.J.: Nominal unification. Theoret. Comput. Sci. 323, 473–497 (2004)
23. Vestergaard, R., Brotherston, J.: A formalised first-order confluence proof for the λ-calculus using one-sorted variable names. Inform. Comput. 183, 212–244 (2003)