Mathematical Structures in Computer Science (2020), **30**, pp. 710–735
doi:10.1017/S0960129520000122

CAMBRIDGE UNIVERSITY PRESS

PAPER

Rewriting with generalized nominal unification†

Yunus Kutz and Manfred Schmidt-Schauß*

Goethe-University, Frankfurt am Main, Germany
*Corresponding author. Email: schauss@ki.informatik.uni-frankfurt.de

(Received 15 March 2019; revised 20 April 2020; accepted 21 April 2020; first published online 22 May 2020)

Abstract

We consider matching, rewriting, critical pairs and the Knuth–Bendix confluence test on rewrite rules in a nominal setting extended by atom-variables. We utilize atom-variables instead of atoms to formulate and rewrite rules on constrained expressions, which is an improvement of expressiveness over previous approaches. Nominal unification and nominal matching are correspondingly extended. Rewriting is performed using nominal matching, and computing critical pairs is done using nominal unification. We determine the complexity of several problems in a quantified freshness logic. In particular we show that nominal matching is Π_2^p-complete. We prove that the adapted Knuth–Bendix confluence test is applicable to a nominal rewrite system with atom-variables, and thus that there is a decidable test whether confluence of the ground instance of the abstract rewrite system holds. We apply the nominal Knuth–Bendix confluence criterion to the theory of monads and compute a convergent nominal rewrite system modulo alpha-equivalence.

Keywords: Nominal unification; nominal rewriting; Knuth–Bendix confluence criterion; atom-variables; confluence

1. Introduction

The goal of this paper is to demonstrate the expressive power of nominal modelling with atom-variables (Schmidt-Schauß et al. 2019) also, in applications. Therefore, we investigate rewriting matching and critical pairs a la Knuth–Bendix (Knuth and Bendix 1970) in a higher-order language with alpha-equivalence and nominal modelling, where in the nominal unification and matching algorithm also atom-variables are permitted in addition to expression-variables and where the rewriting is done using a corresponding form of nominal matching with atom-variables. Previous approaches (Aoto and Kikuchi 2016; Ayala-Rincón et al. 2016; Fernández and Rubio 2012; Kikuchi et al. 2017; Suzuki et al. 2016) to nominal rewriting and checking local confluence in order to apply the Knuth–Bendix confluence check usually proceed as follows: Rewrite rules are formulated such that atoms represent names, and in order to make the formulation independent of atom names, equivariance of the rewriting relation is implicitly assumed. This is the same as using atom-variables together with the implicit (extra) assumption that different atom-variables can only be instantiated with different atoms. Examples for tools are Aoto and Kikuchi (2016) for confluence tests, and Ayala-Rincón et al. (2019*a*,b) for certifications of algorithms for an extension with a commutative theory. Our approach to use unrestricted atom-variables omits this distinct-name assumption and makes reasoning more flexible, has a high potential of making less case distinctions and in this way improves upon the previous approaches. The advantage is that the

†Manfred Schmidt-Schauß is supported by the Deutsche Forschungsgemeinschaft (DFG) under grant SCHM 986/11-1.

© The Author(s), 2020. Published by Cambridge University Press

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

process of trying all possible equality relations between the used atoms (which is necessary in the previous approaches and has to be done in every single rewriting step) can be turned into a computation by using our unification and matching algorithm, and that in the case of good luck, the computation results in a unique answer.

Nominal techniques (Pitts 2016, 2013) support machine-oriented reasoning on the syntactic level for higher-order languages and support reasoning modulo α-equivalence. An algorithm for nominal unification was first described in Urban et al. (2003), which outputs unique most general unifiers. More efficient algorithms are given in Calvès and Fernández (2008) and Levy and Villaret (2010), exhibiting a quadratic algorithm. The approach is also used in higher-order logic programming (Cheney 2004, 2010) and in automated theorem provers like nominal Isabelle (Urban 2008; Urban and Kaliszyk 2012). Nominal unification with atoms was generalized by permitting also atom-variables (Schmidt-Schauß et al. 2019) where also in the generalization, unique most general unifiers are computed, while the decision problem is NP-complete.

We illustrate our nominal modelling and nominal rewriting by two examples. A first simple example is the reduction rule (cpcx) in the concurrent calculus Concurrent Haskell with Futures (CHF) (Sabel and Schmidt-Schauß 2011, 2012) or in other functional programming calculi. It permits rewriting a sub-expression using the rule

$$(\texttt{let}\ y = c\ x_1 \ldots x_n\ \texttt{in}\ s) \to (\texttt{let}\ y = c\ x_1 \ldots x_n\ \texttt{in}\ s'),$$

where s' is the expression s where one free occurrence of the variable y is replaced by $(c\ x_1 \ldots x_n)$. This rule can be applied as a correct transformation even if the variables x_i are not pairwise different, which is in contrast to usual nominal rewriting using atoms instead of atom-variables, since a single unifier in our proposed algorithm covers all possibilities of equal/unequal variables x_i.

As an extended example[1] to illustrate our ideas, we define a capture free substitution via rewriting. We will use the following naming scheme: X and S are used for atom- and expression-variables, respectively, and lowercase letters for ground expressions: i.e., atoms, i.e. variable names, expressions and function symbols. We represent the operation $t[s/y]$ as a nominal rewrite system, which goes through the structure of t and rewrites depending on the validity of freshness constraints.

We write $t[s/y]$ as $subst(t, y, s)$. The rewrite rules in the abstract language with variables are:

(1) $subst(X, X, S) \to S$.
(2) $subst(app(S_1, S_2), X, S) \to app(subst(S_1, X, S), subst(S_2, X, S))$
(3) $X\#Y, X\#S \vdash subst((\lambda X.S_1), Y, S) \to \lambda X.subst(S_1, Y, S)$.
(4) $X\#Y \vdash subst(X, Y, S) \to X$.

Our Definition 4.2 of the rewriting relation is intended to be a rewrite relation on $\sim_\alpha$-equivalence classes, as usual for applications in programming languages. From Definition 4.2 of the rewriting relation on ground expression, it follows that alpha-renamings are automatically included. Thus, a rewrite relation like:

$$subst(s_1, x, s) \to subst(s_1', x, s), \text{ where } s_1 \sim_\alpha s_1'$$

holds by definition. This allows us to omit explicit renamings from the rewrite rule set for the capture-free substitution.

To illustrate the effect of closing the relation under α-equivalence, we consider the NL_a expression $subst(\lambda x.z, z, (app(x, z)))$. There is no (usual) rewrite step on it since x occurs free in $(app(x, z))$. However, a renaming (as allowed in our definition of rewrite) helps to enable the desired rewrite:

$$subst(\lambda x.z, z, app(x, z)) \sim_\alpha subst(\lambda x'.z, z, app(x, z))$$
$$\downarrow$$
$$\lambda x'.subst(z, z, app(x, z))$$

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

where the latter rewrite step is valid, since the condition $x'\#z, x'\#app(x,z)$ holds. Note that the result is unique under α-equivalence and thus independent of the new (fresh) name x'. By closing and rewriting under α-equivalence, the rewrite step

$$subst(\lambda x.z, z, app(x,z)) \to \lambda x'.subst(z, z, app(x,z))$$

becomes valid as well, and the required renaming is handled implicitly rather than explicitly. The defined relation of capture-free substitution is confluent (and terminating) module α-equivalence, as can be checked via a critical-pair analysis.

Our motivation to study nominal rewriting is to improve automated reasoning methods in higher-order programming languages. For example, program transformations using binders can often be defined by nominal rewriting rules. The advantageous feature is that a single nominal rewriting step is unique and can be computed in polynomial time. Checking the correctness of the rewrite step is in the polynomial hierarchy. The contrast is second-order rewriting which is usually undecidable and not unique.

The *results* of this paper are as follows. We define a logic quantified freshness logic (QFL) over nominal constraints and equations in Section 3 and determine the complexity of validity of freshness and equivalence formulas which is later used to determine the complexity of matching (Corollary 3.14). We describe a nominal matching algorithm in Section 4 and give a definition of nominal rewriting of expressions under constraints and with atom-variables in Section 4.1.

The complexity of nominal matching with atom-variables due to the complexity of constraint satisfiability is proved to be Π_2^p-complete (Theorem 4.10).

A variant of the Knuth–Bendix confluence test under atom-variables is described in Section 4 and proved correct for detecting confluence on the induced rewriting system on ground expressions (Theorem 4.19). We compute the completion and prove a confluence result modulo α-equivalence for the (completed) rewrite rules of the monad theory (Theorem 5.4), which is more general than previous ones and demonstrates the power of our method.

The structure of the paper is as follows. In Section 2 the languages of nominal expressions are described. Section 3 describes the QFL for quantified freshness constraints and α-equivalence. Section 4 is a presentation and adaptation of rewrite rules and the Knuth–Bendix confluence test. In Section 5 we apply nominal matching, rewriting and nominal confluence test with atom-variables to the theory of monads. In Section 6 we give a comparison to the classical nominal rewriting framework introduced by Fernández et al. (2004). We conclude in Section 7.

2. Nominal Terms

We first introduce some notation (Schmidt-Schauß et al. 2019).

Let $\mathcal{F}$ be a set of function symbols $f \in \mathcal{F}$, s.t. each f has a fixed arity $ar(f) \geq 0$. Let $\mathcal{A}t$ be *the set of atoms* ranged over by a, b, c. The ground language NL_a is defined by the grammar:

$$e ::= a \mid (f\ e_1 \ldots e_{ar(f)}) \mid \lambda a.e$$

where e is a nonterminal for expressions, a a nonterminal for atoms, and λ is a binder for atoms. Constraints are of the form $a\#e$. The basic constraint $a\#e$ is valid if a does not occur freely in e and a set of constraints ∇ is valid if all constraints are valid. When speaking about NL_a-expressions, we use as convention that different letters a, b stand for different atoms a and b and the same letter always indicates the same atom in the relevant context.

Constructs of the form $(a\ b)$ will denote a *swapping* of the two atoms a, b in an expression e.

We will use the following definition of α-equivalence on NL_a:

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Definition 2.1. *Syntactic α-equivalence $\sim$ in NL_a is inductively defined:*

$$\frac{}{a \sim a} \quad \frac{\forall i : e_i \sim e'_i}{(f\ e_1 \ldots e_{ar(f)}) \sim (f\ e'_1 \ldots e'_{ar(f)})} \quad \frac{e \sim e'}{\lambda a.e \sim \lambda a.e'} \quad \frac{a\#e' \wedge e \sim (a\ b)\cdot e'}{\lambda a.e \sim \lambda b.e'}$$

Note that $\sim$ is identical to the equivalence relation generated by α-equivalence by renaming binders, which can be proved in a simple way by arguing on the (binding-)structure of expressions (using deBruijn-indices) and hence $\sim$ is an equivalence relation on NL_a. It is also a congruence on NL_a, i.e., for any context C, we have $e_1 \sim e_2$ implies $C[e_1] \sim C[e_2]$.

We introduce two further languages, where we also permit permutations and atom- and expression-variables.

Definition 2.2. *Let $\mathcal{S}$ be the set of expression-variables ranged over by S, T and let $\mathcal{A}$ be the set of atom-variables ranged over by A, B. The grammar of the nominal language NL_{aAS} with atoms, atom-variables and expression-variables is:*

$$\begin{aligned} e &::= W \mid \pi\cdot S \mid (f\ e_1 \ldots e_{ar(f)}) \mid \lambda W.e \\ \pi &::= \varnothing \mid (W\ W')\cdot\pi' \\ W &::= \pi\cdot a \mid \pi\cdot A \end{aligned}$$

where e is a nonterminal for expressions, π is a permutation, and W a nonterminal for suspensions. The symbol $\varnothing$ denotes the identity permutation, which we may omit in the notation.

For an expression e any ambiguity about which language the expression should belong to, is resolved by the context at hand.

The language $NL_{AS} \subset NL_{aAS}$ is defined by:

$$\begin{aligned} e &::= V \mid \pi\cdot S \mid (f\ e_1 \ldots e_{ar(f)}) \mid \lambda V.e \\ \pi &::= \varnothing \mid (V\ V')\cdot\pi' \\ V &::= \pi\cdot A \end{aligned}$$

where V is a nonterminal for suspensions of an atom-variable.

Note that we permit nested permutation expressions. For example, the expression $((\pi\cdot A)\ (\pi'\cdot A'))$ is a single nested swapping. The inverse π^{-1} of a permutation $\pi = sw_1\cdot\ldots\cdot sw_n$ with swappings sw_i is the expression $sw_n\cdot\ldots\cdot sw_1$. The set $AtVar(e)$ are the atom-variables contained in e, $ExVar(e)$ the expression-variables contained in e and $Var(e) = AtVar(e) \cup ExVar(e)$. Furthermore, $FVar(e)$ denotes the set of free variables in e, i.e. all expression-variables and all atom-variables which are not bound. These notations will also be used for other syntactic objects.

The languages of interest in this paper are NL_a and NL_{AS}. The ground language of NL_{AS} is NL_a, i.e. expressions s of NL_{AS} can be instantiated to ground expressions by ground substitutions that replace atom-variables by atoms and expression-variables by ground expressions. The language NL_{aAS} serves as an intermediate language during the interpretation of NL_{AS} terms.

3. A Quantified Logic of Freshness Constraints

The logic *QFL* is the background logic for the analysis of the formalism in this paper. It is used to make statements such as correctness, completeness and complexity about matching algorithms and equivalence of constrained expressions.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Definition 3.1. *The formulas of QFL are defined as follows, where e denotes NL_{aAS}-expressions, W atom-variable suspensions as in NL_{aAS}, and logical operations are as usual.*

$$\Phi := Q_1 X_1 \ldots Q_k X_k.\varphi \qquad \text{where } Q_i \in \{\forall, \exists\}, \text{ and } X := A \mid S,$$
$$\varphi := W_i \# e \mid e \sim e \mid \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi$$

Since we use NL_{aAS} there are permutations permitted in the language of QFL. We assume that the simplification and application of ground permutations are done if possible. Thus, we can assume that ground expressions e are represented as NL_a-expressions.

Validity of closed formulas is defined as follows:

$\exists A\Phi$	*iff* $\Phi[a/A]$ *for some* $a \in \mathcal{A}t$;	$\neg\varphi$	*iff* φ *is not valid;*
$\exists X\Phi$	*iff* $\Phi[e/X]$ *for some* $e \in NL_a$;	$\varphi_1 \vee \varphi_2$	*iff* φ_1 *or* φ_2;
$\forall A\Phi$	*iff* $\Phi[a/A]$ *for all* $a \in \mathcal{A}t$;	$\varphi_1 \wedge \varphi_2$	*iff* φ_1 *and* φ_2;
$\forall X\Phi$	*iff* $\Phi[e/X]$ *for all* $e \in NL_a$;	$a\#e$	*iff* $a\#e$ *holds in* NL_a;
$\top$	*is always true;*	$e_1 \sim e_2$	*iff* $e_1 \sim e_2$ *holds in* NL_a

For simplicity we will sometimes use the notation $V =_{\#} V'$ instead of $V\#\lambda V'.V$, since the constraint is valid if and only if V and V' are mapped to the same atom.

Note that unlike in first-order logic, *QFL* has an implicit fixed domain, NL_a. Note also that equality in NL_a is α-equivalence implying that relations on NL_a cannot distinguish between α-equivalent terms. Similar to the first order we define a variant of equality where its semantics is α-equivalence, which is necessary, since α-equality of non-ground expressions is not as straightforward as equality in the first-order case.

A set of quantifier-free formulas of the form $W\#e$ is called a *freshness environment* or *freshness constraint*. These sets are interpreted as conjunctions of their elements. Furthermore, for a free variable X (either an expression-variable S or an atom-variable A) in a formula φ, we say that an expression e or an atom a is an interpretation of X if we consider the formulas $\varphi[e/X]$ or $\varphi[a/X]$ in the context at hand. The semantics of a formula $\exists X.\Phi$ is then equivalent to the existence of an interpretation of X s.t. Φ holds. Analogously, the formula $\forall X.\Phi$ holds if for all interpretations of X the formula Φ holds.

Definition 3.2. *Let φ be a quantifier-free formula. If there is a ground substitution γ into NL_a, such that $\varphi\gamma$ is closed and valid, then we say γ is* solution *of φ and φ is* satisfiable.

The nominal unification algorithm in Schmidt-Schauß et al. (2019) for the language NL_{AS} is unitary and computes a most-general unifier (∇, σ) if one exists at all. The set ∇ consists of constraints. This computation can be performed in polynomial time, ignoring the satisfiability check of ∇. The satisfiability of ∇, i.e. the existence of a ground substitution under which all constraints in ∇ become valid, was shown to be NP-complete.

This final satisfiability question can be written as the existential formula $\exists\overline{X}.\nabla$, where $\overline{X} = Var(\nabla)$. The previously shown complexity is in line with the results of this paper (e.g. Theorem 3.9).

Definition 3.3. *Let Δ_1, Δ_2 be two freshness environments s.t. $\Delta_1 \subseteq \Delta_2$ and let $\overline{X_1} = Var(\Delta_1), \overline{X_2} = Var(\Delta_2) \setminus \overline{X_1}$. Then a QFL-formula of the form :*

$$\forall\overline{X_1}\exists\overline{X_2}.(\Delta_1 \implies \Delta_2)$$

is called a continuation check *of Δ_1 to Δ_2. If the formula holds, we say Δ_1 can be* extended *to Δ_2.*

Corollary 3.4. *Let Δ_1, Δ_2 be two freshness environments. Then Δ_1 can be extended to Δ_2 iff every solution of Δ_1 can be extended to a solution of Δ_2.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

$$\text{(M1)}\ \frac{(\Gamma \uplus \{e \sim e\}, \nabla)}{(\Gamma, \nabla)} \qquad \text{(M2)}\ \frac{(\Gamma \uplus \{\pi_1 \cdot S \sim \pi_2 \cdot S\}, \nabla)}{(\Gamma, \nabla \cup \{A \# \lambda \pi_1^{-1}\pi_2 A.S \mid A \in AtVar(\pi_1, \pi_2)\})}$$

$$\text{(M3)}\ \frac{(\Gamma \uplus \{\pi_1 \cdot A \sim \pi_2 \cdot B\}, \nabla)}{(\Gamma, \nabla \cup \{\pi_1 \cdot A =_{\#} \pi_2 \cdot B\})} \qquad \text{(M4)}\ \frac{(\Gamma \uplus \{(f\ e_1 \ldots e_{ar(f)}) \sim (f\ e'_1 \ldots e'_{ar(f)})\}, \nabla)}{(\Gamma \cup \{e_1 \sim e'_1, \ldots, e_{ar(f)} \sim e'_{ar(f)}\}, \nabla)}$$

$$\text{(M5)}\ \frac{(\Gamma \uplus \{\lambda \pi_1 \cdot A_1.e_1 \sim \lambda \pi_2 \cdot A_2.e_2\}, \nabla)}{(\Gamma \cup \{e_1 \sim ((\pi_1 \cdot A_1)\ (\pi_2 \cdot A_2)) \cdot e_2\}, \nabla \cup \{\pi_1 \cdot A_1 \# \lambda \pi_2 \cdot A_2.e_2\})}$$

$$\text{(M6)}\ \frac{(\Gamma \uplus \{e_1 \sim e_2\}, \nabla)}{(\varnothing, \{\neg \top\} \cup \nabla)}\ \text{If the case of } e_1 \sim e_2 \text{ is not covered by the other rules.}$$

Figure 1. Rules of `EqToCons`

3.1 Decision procedures and complexity analysis

We provide decision algorithms for special forms and quantification of equality $e_1 \sim e_2$, under constraints and for freshness extensions.

For equality the idea is as follows: We transform equations (at positive occurrences in the formulas) into a freshness constraint which is equivalent to the equation, i.e. $\forall \overline{X}.(\Delta \implies e_1 \sim e_2)$ iff $\forall \overline{X}.(\Delta \implies \nabla)$, and then use results for equality-free constraints.

Definition 3.5. *For two NL_{aAS}-expressions e_1, e_2 the algorithm `EqToCons` starts with the pair $(\{e_1 \sim e_2\}, \varnothing)$ and applies the rules in Figure 1. If it terminates with $\Gamma = \varnothing$, then the output is ∇.*

Lemma 3.6. *Let the equation $e_1 \sim e_2$ and the freshness environment Δ be the input of the algorithm `EqToCons`. If Δ is satisfiable, then it produces a freshness environment ∇ in polynomial time s.t. $\forall \overline{X}.(\Delta \implies e_1 \sim e_2)$ iff $\forall \overline{X}.(\Delta \implies \nabla)$ and only fails if $\forall \overline{X}.(\Delta \implies e_1 \sim e_2)$ is false.*

Proof. It is easy to verify that the rules (M1) ... (M5) retain exactly the set of solutions. The rule (M6) fires, if the top symbols of the expressions e_1, e_2 are different. If one or two are variables or suspensions, then only the (M2) and the (M3)-cases can occur in case there is a solution. Other possibilities prevent solutions, for example, $X_1 \sim X_2$ for $X_1 \neq X_2$ is not solvable, since both are universally quantified and there are sufficiently many different NL_a-expressions, in particular infinitely many different atoms. Note also that (M2) is correct, since every atom A occurring in the permutations π_1, π_2 contributes the constraint $A \# \lambda \pi_1^{-1}\pi_2 A.S$, which informally means: If A is changed by $\pi_1^{-1}\pi_2$, then A is fresh for S. More detailed arguments can be derived from Schmidt-Schauß et al. (2019), since the rules assure equivalence on ground substitutions.

The complexity follows from the following observations: First note that every rule strictly decreases the size of Γ by at least 1. So there is at most a linear number of rule applications before termination. The only rule which can increase the size of the data structure and in particular the size of permutations is (M5). This increase of the total size is bounded by 1 in depth and 1 in the number of swappings per rule application. Hence, the size of all permutations is bound polynomial in the input size. It follows that every rule runs in polynomial time in the input size, yielding a polynomial time algorithm. In particular, the rule (M2) contributes only polynomial time, because the maximal size of any permutations and the number of atoms is polynomially bounded in the input size. □

Now we define the algorithm that decides *QFL*-formulas containing $\sim$-literals

Definition 3.7. *The algorithm `CheckEq` decides QFL($\sim$) formulas of the form:*

$$\forall \overline{X} : (\Delta \implies e_1 \sim e_2)$$

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

as follows:

(1) *Apply* `EqToCons` *to* $e_1 \sim e_2$ *resulting in* ∇.
(2) *Check the formula* $\forall\overline{X} : (\Delta \implies \nabla)$ *for validity.*

Proposition 3.8. *There is a polynomial time transformation from QFL-formulas without equations* $e_1 \sim e_2$ *to QBL maintaining validity such that the quantifier schema in the form* $\forall^*\exists^* \ldots$ *or* $\exists^*\forall^* \ldots$ *remains the same and the complete quantifier prefix increases only quadratically.*

Proof. Let $\varphi = Q_1\overline{X_1} \ldots Q_k\overline{X_k}.\varphi'$ be a *QFL*-formula where m is the number of atom-variables and l the number of expression-variables. To decide the validity of φ it is sufficient to take $NL_{a,m}$, which is NL_a, but there are only m atoms $M = \{a_1, \ldots, a_m\}$. The justification is that there are only m atom-variables, and no atoms in the formula; hence m atoms are sufficient for the interpretation of atom-variables. Every permutation π will be interpreted as permutation over M, and suspensions $\pi \cdot A$ will also be interpreted by some atom in M. This holds for all interpretations. Without loss of generality we can assume that for every interpretation the same set of atoms is chosen. An NL_a-interpretation of nominal terms e may contain more atoms, but only the atoms from M that occur in e are relevant for the truth-value of single freshness constraint. Hence it is sufficient to interpret expression-variables S as a subset of M and then compute the freshness constraints. Now we can use this interpretation to argue on the complexity. Every interpretation of φ is of at most quadratic size in m. In addition, the check of validity of φ' under the interpretation can be done in polynomial time. Hence the complexity of the set of freshness formulas with a fixed quantifier prefix $\forall^*\exists^* \ldots$ is in the corresponding complexity class for QBF-formulas with the same quantifier prefix.

The number of necessary variables corresponds to the size of the interpretation of variables as bit-strings, which is $\leq m$, hence a corresponding QBF formula has at most a quadratic number of quantifiers. □

Proposition 3.8 implies the following theorem.

Theorem 3.9. *QFL-formulas without equations* $e_1 \sim e_2$ *are in the complexity class in the polynomial hierarchy as indicated by the quantifier prefix interpreted as QBF quantifier prefix.*

Lemma 3.6 and Theorem 3.9 imply:

Corollary 3.10. *The validity check of QFL-formulas* $\forall\overline{X} : (\Delta \implies e_1 \sim e_2)$ *and* $\forall\overline{V} : (\Delta \implies \nabla)$ *is in* coNP. *The validity check for formulas of the form* $\forall\overline{X_1}\exists\overline{X_2} : (\Delta \implies \nabla)$ *is in* Π_2^p.

3.2 Hardness of the validity check

To demonstrate the hardness of *QFL*-formulas we encode quantified Boolean formulas, in fact quantified 3-CNF, into *QFL* formulas. This is sufficient to show hardness results (Papadimitriou 1994).

The following constructions are used in our proofs below:
There are two atom-variables – `True` and `False`. For a Boolean formula with the variables $\{x_1, \ldots, x_n\}$, the set $\{A_1, \ldots, A_n\}$ defines the respective atom-variables and the set of (different) atom-variables $\{\overline{A_1}, \ldots, \overline{A_n}\}$ their respective negation. Therefore, we define the following constraints:

(1) $\Delta_1 = \{A_i \# \lambda\texttt{True}.\lambda\texttt{False}.A_i \mid 1 \leq i \leq n\}$
(2) $\Delta_2 = \{A_i \# \overline{A_i}\} \cup \{\overline{A_i} \# \lambda\texttt{True}.\lambda\texttt{False}.\overline{A_i} \mid 1 \leq i \leq n\}$

The constraints Δ_1, Δ_2 ensure that the atom-variables behave like Boolean variables.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Now one needs to encode any given 3-CNF formula. For every clause $l_1 \vee l_2 \vee l_3$ the literal l_i is A_j or $\overline{A_j}$ for some j. Let L_i be either A_j or $\overline{A_j}$ depending on l_i. The constraint $\texttt{True\#}\lambda L_1.\lambda L_2.\lambda L_3.\texttt{True}$ encodes that the clause must be true. For a clause set $\{C_1, \ldots, C_k\}$ define

$$\nabla = \{\texttt{True\#}\lambda L_1^i.\lambda L_2^i.\lambda L_3^i.\texttt{True} \mid 1 \leq i \leq k\}$$

with the construction described as above.

Theorem 3.11. *Decidability of validity of QFL-formulas of the form* $\forall \overline{X}.(\Delta \implies \nabla)$ *and* $\forall \overline{X}.(\Delta \implies e_1 \sim e_2)$ *is* coNP*-hard.*

Proof. Let φ be a universally quantified 3-CNF formula with variables $\{x_1, \ldots, x_n\}$.
Let $\{A_1, \ldots, A_n\}, \{\overline{A_1}, \ldots, \overline{A_n}\}, \Delta_1, \Delta_2, \nabla$ be constructed as described above. Then φ is valid iff

$$\forall \texttt{True}, \texttt{False}, A_1, \ldots, A_n \overline{A_1}, \ldots, \overline{A_n}.(\{\texttt{True\#False}\} \cup \Delta_1 \cup \Delta_2 \implies \nabla)$$

is valid. Hence the class of formulas in the first claim is coNP-hard (Papadimitriou 1994).

For the second claim, we construct e_1, e_2 that reduce to ∇ using `EqToCons`, and hence are equivalent to ∇.

Let $\texttt{True\#}\lambda L_1^i.\lambda L_2^i.\lambda L_3^i.\texttt{True}$ be any constraint in ∇. Let $e_1^i = \lambda \texttt{True}.(\texttt{True}\ \ L_1^i) \cdot (\lambda L_2^i.\lambda L_3^i.\texttt{True})$ and $e_2^i = \lambda L_1^i.\lambda L_2^i.\lambda L_3^i.\texttt{True}$. Then `EqToCons` reduces $e_1^i \sim e_2^i$ to the required constraint. Furthermore $f\ e_1^1\ \ldots e_1^k \sim f\ e_2^1\ \ldots e_2^k$ reduces to ∇. Hence the second claim of the theorem holds. □

Corollary 3.12. *Decidability of validity of QFL-formulas of the form* $\forall \overline{X}.(\Delta \implies \nabla)$ *and* $\forall \overline{X}.(\Delta \implies e_1 \sim e_2)$ *is* coNP*-complete.*

Theorem 3.13. *Decidability of validity of QFL-formulas of the form* $\forall \overline{X_1} \exists \overline{X_2} : (\Delta \implies \nabla)$ *is* Π_2^p*-hard.*

Proof. Let $\varphi = \forall x_1, \ldots, x_k \exists x_{k+1} \ldots x_n.\varphi'$ be a QBF with φ' being a 3-CNF.
Let $\{A_1, \ldots, A_n\}, \{\overline{A_1}, \ldots, \overline{A_n}\}, \Delta_1, \Delta_2, \nabla$ be constructed as described above. Then φ is valid iff

$$\forall \texttt{True}, \texttt{False}, A_1, \ldots, A_k \exists A_{k+1}, \ldots, A_n, \overline{A_1}, \ldots, \overline{A_n}.(\{\texttt{True\#False}\} \implies \Delta_1 \cup \Delta_2 \cup \nabla)$$

is valid. Hence Π_2^p-hardness follows Papadimitriou (1994). □

Corollary 3.14. *Decidability of validity of QFL-formulas of the form* $\forall \overline{X_1} \exists \overline{X_2} : (\Delta \implies \nabla)$ *is* Π_2^p*-complete.*

4. Nominal Rewriting

In this section we define the operations of rewriting, matching and unification for nominal expressions. In order to reason about terms in NL_a on a meta level we define this on pairs (Δ, e), called *constrained expressions*. The advantage is that it leads to a decidable criterion for confluence on the ground level. As a slight disadvantage, it complicates the algorithms and reasoning. For example, the notion of equivalence of constrained expressions would permit several variants. We will use a variant that supports the joining of critical pairs.

In the following we develop and explain nominal matching, nominal unification, nominal rewrite and nominal Knuth–Bendix confluence check.

4.1 Nominal rewriting, unification and matching

We start by defining constraint expressions, which will be the targets to be rewritten.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Definition 4.1. *Let ∇ be a freshness constraint and e be an expression in NL_{AS}. Then the pair (∇, e) is called a* constrained expression. *The semantics $Sem(\nabla, e)$ is defined as the set $\{e\rho \mid e\rho \in NL_a$ and $\nabla\rho$ is ground and valid$\}$.*

Now we define rewrite rules, which are used in two ways: to rewrite constrained NL_{AS}-expressions, as well as (unconstrained) NL_a-expressions. First we define ground rewriting, and after some preparations we define general rewriting in Definition 4.14. We only consider the so-called *uniform* rewriting, which means that no new unbound names are introduced by rewriting.

Definition 4.2. *A* (nominal) rewrite rule *is of the form $R = (\nabla \vdash l \to r)$, where ∇ is a freshness context and l, r are expressions of NL_{AS}, and $FVar(r) \subseteq FVar(l)$. Let $\mathcal{R} = \{R_1, \ldots, R_n\}$ be a* rewrite system *consisting of a set of rewrite rules.*

The induced (semantical) rewrite relation on NL_a is defined as:

$$\xrightarrow{\mathcal{R},NL_a,\epsilon} = \{(s,t) \mid (\nabla_i \vdash l_i \to r_i) \in \mathcal{R}, C \text{ is any } NL_a\text{-context}, \gamma \text{ is a ground substitution}, dom(\gamma) = Var(R_i), \nabla_i\gamma \text{ is valid}, l_i\gamma \sim s, r_i\gamma \sim t\}.$$

$$\xrightarrow{\mathcal{R},NL_a} = \{(C[s], C[t]) \mid s \xrightarrow{\mathcal{R},NL_a,\epsilon} t\}.$$

The equational theory $=_{\mathcal{R},NL_a}$ on NL_a generated by $\mathcal{R}$ is the equivalence closure of $\xrightarrow{\mathcal{R},NL_a}$.

An example for a rule that fits the definition is the following version of the η-expansion rule: $\{B\#A\} \vdash A \to \lambda B.A\ B$, since B is bound by the lambda on the right-hand side. We permit also rules with a non-deterministic behaviour. For example, non-determinism is generated by the rule $\{A\#\lambda B.\lambda C.A\} \vdash A \to \lambda B.\lambda C.A$, which permits a rewrite to two different expressions that are not α-equivalent.

Another effect shows up in the rule $\{A\#\lambda B.\lambda C.A, A\#\lambda C.\lambda D.A\} \vdash A \to \lambda B.C$, which is not valid according to our Definition 4.2, since a free atom is introduced. However, the rule is equivalent to $\{A\#\lambda B.\lambda C.A, A\#\lambda C.\lambda D.A\} \vdash A \to \lambda B.A$, which is permitted.

Definition 4.3. *A binary relation Q on NL_a is called* equivariant, *if $(s_1, s_2) \in Q$ iff $\pi.(s_1, s_2) \in Q$ for any atom-permutation π.*

Proposition 4.4. *For any rewrite system $\mathcal{R}$, the rewrite relation $\xrightarrow{R,NL_a}$ as well as the equational theory $=_{\mathcal{R},NL_a}$ are equivariant.*

Proof. This simply holds, since the atom names are not mentioned in $\mathcal{R}$ and any ground substitution can be used. □

As a corollary, we obtain, for example, that $=_{\mathcal{R},NL_a}$ either makes all atoms equal or makes all atoms different.

Unification is classically defined as an algorithm to make terms equal via a substitution, or in the nominal case a substitution and freshness environment (Levy and Villaret 2010; Schmidt-Schauß et al. 2019; Urban et al. 2004).

Definition 4.5. *Let $P = (\Delta, \Gamma)$ be a unification problem consisting of a freshness constraint and a set Γ of equations $s_i \doteq t_i$ between NL_{AS}-expressions. Then (∇, σ) is a* nominal unifier *if for every ρ such that $P\sigma\rho$ is ground and $\nabla\rho$ is valid, $s_i\sigma\rho \sim t_i\sigma\rho$ holds for all equations in Γ and $\Delta\sigma\rho$ holds.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

$$\text{(M1)}\ \frac{(\Gamma \uplus \{e \preceq e\}, \nabla, \theta)}{(\Gamma, \nabla, \theta)} \qquad \text{(M2)}\ \frac{(\Gamma \uplus \{\pi \cdot S \preceq e\}, \nabla, \theta), S \in V_1}{(\Gamma[(\pi^{-1} \cdot e)/S], \nabla[(\pi^{-1} \cdot e)/S], \theta \cup \{S \mapsto (\pi^{-1} \cdot e)\})}$$

$$\text{(M3)}\ \frac{(\Gamma \uplus \{\pi_1 \cdot S \preceq \pi_2 \cdot S\}, \nabla), S \in V_2}{(\Gamma, \nabla \cup \{A \# \lambda\pi_1^{-1}\pi_2 A.S \mid A \in AtVar(\pi_1, \pi_2)\})} \qquad \text{(M4)}\ \frac{(\Gamma \uplus \{\pi_1 \cdot A \preceq \pi_2 \cdot B\}, \nabla, \theta)}{(\Gamma, \nabla \cup \{A =_{\#} \pi_1^{-1} \cdot \pi_2 \cdot B\}, \theta)}$$

$$\text{(M4)}\ \frac{(\Gamma \uplus \{(f\ e_1 \dots e_{ar(f)}) \preceq (f\ e'_1 \dots e'_{ar(f)})\}, \nabla, \theta)}{(\Gamma \uplus \{e_1 \preceq e'_1, \dots, e_{ar(f)} \preceq e'_{ar(f)}\}, \nabla, \theta)}$$

$$\text{(M5)}\ \frac{(\Gamma \uplus \{\lambda\pi_1 \cdot A_1.e_1 \preceq \lambda\pi_2 \cdot A_2.e_2\}, \nabla, \theta)}{(\Gamma \uplus \{((\pi_1 \cdot A_1)\ (\pi_2 \cdot A_2)) \cdot e_1 \preceq e_2\}, \nabla \cup \{(A_1 \# \pi_1^{-1} \cdot (\lambda\pi_2 \cdot A_2.e_2))\}, \theta)}$$

Figure 2. Rules of *NomMatchAS*

Furthermore, (∇, σ) *is a* most general unifier *if for all ground solutions* ρ *of* P *there is a ground substitution* γ *s.t.* $\nabla\sigma\gamma$ *is valid and* $(\sigma \circ \gamma)(X) \sim \rho(X)$ *for all* $X \in Var(P)$.

A matcher of a matching problem $l \preceq r$ is usually defined as a unifier which does not instantiate (or further restrict) the right-hand side by applying a substitution to it. Again, we need to slightly adapt the previous definitions.

Definition 4.6. *[Matching] Let* $(\Delta_1, s), (\Delta_2, t)$ *be two constrained expressions that are variable disjoint, i.e.* $V_1 \cap V_2 = \varnothing$ *for* $V_1 = Var(\Delta_1, s)$ *and* $V_2 = Var(\Delta_2, t)$. *A* matcher *of the matching problem* $(\Delta_1, s) \preceq (\Delta_2, t)$ *is a pair* (∇, θ) *of a constraint and a substitution as follows:*

- *The right-hand side is not restricted, i.e.* $dom(\theta) \subseteq V_1$ *and every solution of* Δ_2 *can be extended to a solution of* $\nabla \cup \Delta_1\theta$. *This corresponds to the formula*

$$\forall V_2 \exists V_1 : (\Delta_2 \implies \nabla \cup \Delta_1\theta)$$

.

- *It is a unifier of* $(\Delta_1 \cup \Delta_2, \{s \doteq t\})$.

We call the tuple a most general matcher *if it is a matcher and a most general unifier of* $(\Delta_1 \cup \Delta_2, \{s \doteq t\})$.

When matching is used for rewriting, the disjoint variable condition can be easily fulfilled by completely renaming the rewrite rule. Here we use the equivalence of a rewrite rule with its renamed variants.

We provide an algorithm which computes a most general matcher based on the most general unifier algorithm of Schmidt-Schauß et al. (2019).

Definition 4.7. (Matching algorithm). *The input of the algorithm NomMatchAS is a matching-problem* $(\Delta_1, s) \preceq (\Delta_2, t)$ *with* $V_1 = Var(\Delta_1, s)$, $V_2 = Var(\Delta_2, t)$, *where* $V_1 \cap V_2 = \varnothing$. *The matching algorithm operates on a triple consisting of a set of equations, a freshness environment and a substitution. The matching algorithm starts with* $(\{s \preceq t\}, \varnothing, \varnothing)$.
In its first phase it performs the rules in Figure 2 until the triple is of the form $(\varnothing, \nabla, \theta,)$, *i.e.* Γ *is empty. If the process gets stuck, then there is no match.*
Afterwards the second matching condition needs to be checked, i.e. the validity of the formula

$$\forall V_2 \exists V_1 : (\Delta_2 \implies \nabla \cup \Delta_1\theta)$$

must hold.

The output of the algorithm is $(\Delta_2 \cup \nabla \cup \Delta_1\theta, \theta)$.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Example 4.8. These examples help to understand the meaning and effects of the definition and algorithm of nominal matching.

- $(\varnothing, f(S,S)) \preceq (\varnothing, f(S_1,S_2))$. This problem is not solvable, since S_1 and S_2 cannot be made equal.
- $(\varnothing, f(A,A)) \preceq (\varnothing, f(A_1,A_2))$. In this case the algorithm computes $\nabla = (\{A =_\# A_1, A =_\# A_2\}, \theta = \varnothing$. The final check $\forall A_1, A_2 \exists A : (\varnothing \implies \nabla)$ fails. Thus, the problem is not matchable.
- $(\{A\#B\}, f(A,B)) \preceq (\varnothing, f(A_1,A_2))$. In this case the algorithm computes $\nabla = (\{A =_\# A_1, B =_\# A_2\}, \theta = \varnothing$. The final check $\forall A_1, A_2 \exists A, B : (\varnothing \implies \{A =_\# A_1, B =_\# A_2, A\#B\})$ fails, since A_1 and A_2 can be chosen to be equal. Again, the problem is not matchable.
- $(\varnothing, f(A,A)) \preceq (\{A_1\#\lambda A_2.A_1\}, f(A_1,A_2))$ is solvable, since only instances are valid, where A_1, A_2 are instantiated by the same atom.

Theorem 4.9. *NomMatchAS is sound and complete and computes a most general matcher if there is some matcher.*

Proof. Soundness: Soundness of the rules follows from Schmidt-Schauß et al. (2019). If the final test succeeds it is a most general matcher, since the algorithm produces most general unifiers.

For completeness, we need to show that an output is produced if a matcher exists.

Let $(\Delta_1, s) \preceq (\Delta_2, t)$ be a matching-problem which has a matcher (∇, σ) and let $V_1 = Var(\Delta_1, s)$, $V_2 = Var(\Delta_2, t)$. More concretely this means that

$$\forall V_2 \exists V_1 : (\Delta_2 \implies \Delta_1\sigma \cup \nabla)$$

holds and (∇, σ) is a unifier of $(\Delta_1 \cup \Delta_2, s \doteq t)$.

If the first phase failed, there could not be a matcher. So we can safely assume that it produces some $(\tilde{\nabla}, \sigma')$, which is by construction a most general unifier of $(\varnothing, s \doteq t)$. The would-be output of the algorithm, $(\Delta_2 \cup \Delta_1\sigma \cup \tilde{\nabla}, \sigma')$, is then by construction a most general unifier of $(\Delta_1 \cup \Delta_2, s \doteq t)$. Let $\nabla' = \Delta_2 \cup \Delta_1\sigma \cup \tilde{\nabla}$.

One still need to show that this output satisfies the matching formula:

$$\forall V_2 \exists V_1 : (\Delta_2 \implies \nabla')$$

Let γ be any ground substitution, s.t. $dom(\gamma) = V_2$ and $\Delta_2\gamma$ is valid. Let ρ by some ground substitution, s.t. $dom(\rho) = V_1$ and $(\Delta_1\sigma \cup \nabla)\gamma\rho$ is valid. The conditions are equivalent to $\Delta_2(\sigma \circ \gamma \circ \rho)$, $\Delta_1(\sigma \circ \gamma \circ \rho)$ valid and $\nabla(\sigma \circ \gamma \circ \rho)$ is valid.

Because (∇, σ) was a unifier of $(\Delta_1 \cup \Delta_2, s \doteq t)$, $s(\sigma \circ \gamma \circ \rho) \sim t(\sigma \circ \gamma \circ \rho)$ must also hold, which in turn implies that $(\sigma \circ \gamma \circ \rho)$ is a solution of the unification problem.

Because (∇', σ') was a most general unifier, there must be ρ' s.t.

(1) For all $X \in V_1, V_2$: $(\sigma' \circ \rho')(X) \sim \sigma \circ \gamma \circ \rho(X)$.
(2) $\nabla'(\sigma' \circ \rho')$ is valid.

Because γ was chosen as an arbitrary interpretation of V_2, which satisfied Δ_2 and $(\sigma' \circ \rho')$ differs from γ on V_2 at most by α-equivalence the formula:

$$\forall V_2 \exists V_1 : (\Delta_2 \implies \nabla')$$

holds as well. □

Theorem 4.10. *Matching is Π_2^p-complete.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Proof. We can encode an equivalent problem to the formula in the proof of Theorem 3.13 as a matching problem. To that end, let $\Delta_1' = (\Delta_1 \cup \Delta_2 \cup \nabla)[\mathtt{True}'/\mathtt{True}]$ be a freshness environment with the same structure as in the proof of Theorem 3.13 but with a new atom-variable $\mathtt{True}'$. Then $(\Delta_1', \mathtt{True}') \preceq (\{\mathtt{True\#False}\}, \mathtt{True})$ is solvable iff the formula in Theorem 3.13 is solvable. This implies Π_2^p-hardness. The problem is in Π_2^p because *NomMatchAS* runs in two phases which are both in Π_2^p. □

4.2 Equivalence of constrained expressions

We define equivalence of two constrained expressions with the motivation to use it in a Knuth–Bendix confluence test for the join of critical pairs.

Definition 4.11. *Let* (Δ_1, e_1), (Δ_2, e_2) *be two constrained expressions, let* V *be a set of variables, let* $V_i = Var(\Delta_i, e_i) \setminus V$ *and* $V_1 \cap V_2 = \varnothing$.
Then $(\Delta_1, e_1) \equiv_V (\Delta_2, e_2)$ *iff the following holds:*

(1) $\forall V \exists V_1, V_2 : (\Delta_1 \iff \Delta_2)$
(2) $\forall V \forall V_1, V_2 : (\Delta_1 \cup \Delta_2 \implies e_1 \sim e_2)$

Example 4.12. We illustrate the $\equiv_V$-definition for several examples:

- The typical application is that V is the set of atom-variables occurring in the top expression, and the unmentioned atom-variables are subject to renaming:
  $(A\#B, \lambda A.B\ A)$ and $(A'\#B, \lambda A'.B\ A')$ are equal w.r.t. $\equiv_{\{B\}}$:
  $\forall B. \exists A', A : (A\#B \iff A'\#B)$ holds.
  Also $\forall B. \forall A, A' : (A\#B; A'\#B, \implies \lambda A.B\ A \sim \lambda A'.B\ A')$ holds.
  For $V = \{A, B\}$, or $V = \{A', B\}$, this also holds but not for $V = \{A, A', B\}$.
- As another example consider $(A\#\lambda B.A, (A, B))$ and $(A\#\lambda C.A, (A, C))$ with $V = \{A\}$. Then $\forall A \exists B, C : (A\#\lambda B.A \iff A\#\lambda C.A)$ holds, and
  $\forall A, B, C : (A\#\lambda B.A, A\#\lambda C.A \implies (A, C) \sim (A, B)$ is valid.

The relation $\equiv_V$ should not be seen as some equivalence relation – especially since it is in general not transitive. It simply provides a criterion for determining that a confluence diagram is really closed. More specifically, every time a forking occurs in a diagram, one can choose the current variables as V and use $\equiv_V$ to check whether two constrained expressions below do in fact refer to the same related expressions. We write this more formally as a lemma:

Lemma 4.13. *Let* (Δ, e), (Δ_1, e_1), (Δ_2, e_2) *be constrained expressions, let* $V = Var(\Delta, e)$, $V_i = Var(\Delta_i, e_i) \setminus V$ *and let* $\to$ *be any relation on constrained expressions. Suppose*

$$\begin{array}{ccc} & (\Delta, e) & \\ \swarrow & & \searrow \\ (\Delta_1, e_1) & & (\Delta_2, e_2) \end{array}$$

holds, with $(\Delta_1, e_1) \equiv_V (\Delta_2, e_2)$. *Let* γ *be any ground substitution with* $dom(\gamma) = V$ *s.t.* $\Delta\gamma$ *is valid and let* ρ_i *be any ground substitution with* $dom(\rho_i) = V_i$ *s.t.* $\Delta_i\gamma\rho_i$ *holds. Then* $e_1\gamma\rho_1 \sim e_2\gamma\rho_2$. *Furthermore, such a* ρ_1 *exists iff such a* ρ_2 *exists.*

Proof. The first claim follows directly from criterion 2 and the second one from criterion 1 of Definition 4.11. □

Another way to think of Lemma 4.13 is to say that if $(\Delta, e) \to (\Delta_1, e_1)$, $(\Delta, e) \to (\Delta_2, e_2)$ and $(\Delta_1, e_1) \equiv_V (\Delta_2, e_2)$ then the corresponding induced relations on NL_a are identical modulo α-equivalence.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

4.3 Nominal rewriting

We define nominal rewriting on NL_{AS} on constrained expressions $(\Delta, C[s])$ as targets where s is the sub-expression that is to be modified, C is the context representing the position and Δ is a freshness constraint.

Definition 4.14. *Let $(\nabla \vdash l \to r)$ be a rewrite rule and let $(\Delta, C[s])$ be the constrained expression to be rewritten, where $Var(\nabla, l \to r) \cap Var((\Delta, C[s]) = \varnothing$. The condition can be achieved by renaming of $(\nabla, l \to r)$). A* rewrite step *is defined as follows:*

Let (∇', σ) be a most general matcher of $(\nabla, l) \preceq (\Delta, s)$ computed with NomMatchAS and let $\nabla'' = \nabla' \cup \nabla\sigma$. Then the result of rewriting is $(\Delta \cup \nabla'', C[r\sigma])$.
Thus the rewrite step is $(\Delta, C[s]) \to (\Delta \cup \nabla'', C[r\sigma])$.

For a rewrite system $\mathcal{R}$, this defines a rewriting relation $\xrightarrow{\mathcal{R}}$ on constrained expressions over NL_{AS} with transitive closure $\xrightarrow{\mathcal{R},*}$.

4.4 Overlaps, critical pairs and Knuth–Bendix confluence criterion

Now we define overlap, join and critical pairs, the adapted Knuth–Bendix criterion for confluence and sketch completion in our setting of nominal rewriting on NL_a, where rules are formulated in NL_{AS}.

Definition 4.15. *An* overlap *of two rewrite rules is computed by the following algorithm. First the rewrite rules are renamed such that they are variable-disjoint, where also the same rule may be used twice: $(\nabla_1, l_1 \to r_1)$ and $(\nabla_2, l_2 \to r_2)$. Select a non-variable expression-position p in l_1, represented by a context C, such that $C[l_1'] = l_1$ and the hole of C is at position p, and the expression at the position p is not a variable. Apply the unification algorithm in Schmidt-Schauß et al. (2019) to $(\nabla_1, l_1') \doteq (\nabla_2, l_2)$. If there is an overlap, then the result of the unification algorithm is a most general unifier (∇, σ). The resulting overlap in the constrained expression is $(\Delta, l_1\sigma)$, where $\Delta = (\nabla \cup \nabla_1 \cup \nabla_2)\sigma$.*

The critical pair *consists of the corresponding rewriting results $((\Delta, r_1\sigma), (\Delta, C\sigma[r_2\sigma]))$. The* overlap triple *is then $((\Delta, l_1\sigma), (\Delta, r_1\sigma), (\Delta, C\sigma[r_2\sigma]))$. If $(\Delta, r_1\sigma) \equiv_V (\Delta, C\sigma[r_2\sigma])$ where $V = Var(\Delta, r_1\sigma, r_2\sigma)$ holds, the critical pair is trivial.*

Note that the technical treatment is slightly different from the criterion on first-order theories, insofar as rewriting and joining in NL_{AS} uses the common freshness constraints of a rewriting sequence.

Definition 4.16. (Nominal Knuth–Bendix Confluence Criterion). *Let $\mathcal{R}$ be a finite nominal rewrite system over NL_{AS}. Let the following two properties hold:*

(1) Rewriting terminates on NL_{AS}.
(2) All critical pairs can be joined as follows: For every overlap triple $((\Delta, s), (\Delta, s_1), (\Delta, s_2))$ according to Definition 4.15 either the critical pair is trivial, or there are $\mathcal{R}$-reduction sequences $(\Delta, s_1) \to (\Delta_{1,1}, s_{1,2}) \to \ldots \to (\Delta_{1,k_1}, s_{1,k_1})$ and $(\Delta, s_2) \to (\Delta_{2,1}, s_{2,2}) \to \ldots \to (\Delta_{2,k_2}, s_{2,k_2})$ such that $(\Delta_{1,k_1}, s_{1,k_1}) \equiv_V (\Delta_{2,k_2}, s_{2,k_2})$, where $V = Var((\Delta, s)$.

Then we conclude that the rewrite relation of $\xrightarrow{\mathcal{R},NL_a}$ is terminating and confluent. We can also conclude that the congruence generated by $\mathcal{R}$ on NL_a is decidable by rewriting.

4.5 Proofs of correctness

Lemma 4.17. *Let $\mathcal{R}$ be a finite nominal rewrite system over NL_{AS}. If C is a ground context and $s \xrightarrow{\mathcal{R},NL_a} s'$ for two ground expressions, then also $C[s] \xrightarrow{\mathcal{R},NL_a} C[s']$.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Proof. This follows from Definition 4.14 of rewriting. □

Lemma 4.18. *Let $\mathcal{R}$ be rewrite system, and let (Δ, e) be a constrained expression with $Var(\Delta, e) = V$ and let $(\Delta_1, e_1), (\Delta_2, e_2)$ be two constrained expressions, which arise from different branches during rewriting of (Δ, e), i.e.*

$$\begin{array}{ccc} & (\Delta, e) & \\ {\scriptstyle \mathcal{R},*}\swarrow & & \searrow{\scriptstyle \mathcal{R},*} \\ (\Delta_1, e_1) & & (\Delta_2, e_2) \end{array}$$

Then $(\Delta_1, e_1) \equiv_V (\Delta_2, e_2)$ holds iff the second criterion holds, i.e.

$$\forall V \forall V_1, V_2 : (\Delta_1 \cup \Delta_2 \implies e_1 \sim e_2)$$

.

Proof. Because (Δ_i, e_i) arise from rewriting and no shared new variables can be introduced during the procedure, the introduced variables along the different reduction sequences are disjoint. Due to the matching condition, for $\Delta_i' = \Delta \setminus \Delta_i$ the formula $\forall V \exists V_i : (\Delta \implies \Delta_i')$ holds.

Using this we get the equivalence between the formulas $\Delta_1 \iff \Delta_2$ and $\Delta \implies (\Delta_1' \iff \Delta_2')$. The first condition is then equivalent to:

$$\forall V \exists V_1, V_2 : (\Delta \implies (\Delta_1' \iff \Delta_2'))$$

Because for every choice of V that satisfies Δ, one can always choose V_i, s.t. Δ_i' holds, the formula must hold as well. □

Theorem 4.19. *Let $\mathcal{R}$ be a set of rewrite rules over NL_{AS}. If the Knuth–Bendix confluence criterion in Definition 4.16 holds, and if $\xrightarrow{\mathcal{R}}$ is terminating, then the rewrite relation $\xrightarrow{R,NL_a}$ is confluent.*

Proof. Due to the Hindley–Rosen Lemma, it is sufficient to show that $\xrightarrow{R,NL_a}$ is locally confluent. There are three types of divergences:

(i) Two reduction steps of $\xrightarrow{R,NL_a}$ at independent positions in an NL_a-expressions. Then the reductions are $s_1 \xrightarrow{R,NL_a} s_1'$, $s_2 \xrightarrow{R,NL_a} s_2'$, and since reductions in contexts are always possible by Lemma 4.17: $C[s_1, s_2] \to C[s_1', s_2]$ and $C[s_1, s_2] \to C[s_1, s_2']$ can both be reduced to $C[s_1', s_2']$, and hence joined.

(ii) The reduction steps of $\xrightarrow{R,NL_a}$ are at dependent positions (the overlap at or below a variable position) in an NL_a-expression. Then the situation can be captured by $C_1[C_2[s]] \xrightarrow{R,NL_a} C_1[C_2'[s, \ldots, s]]$ and $C_1[C_2[s]] \xrightarrow{R,NL_a} C_1[C_2[s']]$, where the rewrites are $\nabla \vdash \overline{C_2}[X] \xrightarrow{R} \overline{C_2}'[X, \ldots, X]$ with $C_2[s] = \overline{C_2}[X]\gamma$ s.t. $\nabla\gamma$ is valid and $\nabla_s \vdash \bar{s_0} \xrightarrow{R} \bar{s_0}'$ with $s = C_3[s_0\rho]$ for some NL_a context $C_3[]$ and ground substitution ρ with $\nabla_s\rho$ valid.
Since $s \xrightarrow{R,NL_a} s'$, we have $C_1[C_2'[s, \ldots, s]] \xrightarrow{R,NL_a} C_1[C_2'[s', \ldots, s']]$ by Lemma 4.17. The same rewrite step for $C_2[s']$ as $C_2[s]$ is permitted, since the free atoms of s' are all contained in s, and thus the constraints cannot block this rewrite step. It yields $C_1[C_2'[s', \ldots, s']]$. Hence, the expression can be joined by perhaps several reduction steps.

(iii) The two reduction steps are at dependent positions, but not at or below a variable position. This corresponds to a critical pair. Since rewriting $\xrightarrow{R,NL_a}$ is derived from the general rewrite rules, there is a critical pair that has these two reductions as instance. By assumption, the critical pair can be joined up to $\equiv_V$ where V is the set of variables of the overlap. Then

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Lemma 4.18 shows that the instance critical pair can be joined such that the final expressions are α-equivalent. Note that the used ground substitution may be extended during the reductions, but only for bound variables.

□

Theorem 4.20. *Let $\mathcal{R}$ be a rewrite system over NL_{AS}. If the Knuth–Bendix Confluence Criterion in Definition 4.16 holds, then the rewrite theory $=_{\mathcal{R},NL_a}$ on NL_a is decidable.*

Proof. This follows from Theorem 4.19, and the fact that all (finite) critical pairs can be effectively computed and also tested whether they are joinable. Moreover, rewriting is terminating by assumption, the rewrite steps are effective and the final test $\equiv_V$ is also decidable. □

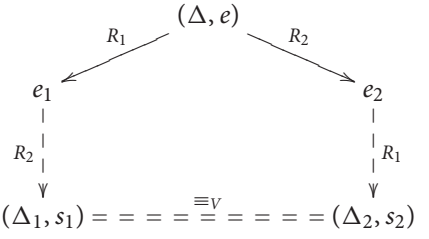
Remark 4.21. For a finite rewrite system $\mathcal{R}$, we have a decidable test for confluence on NL_a, but not on the general level. To investigate the issue of confluence on the constrained expressions is future work. This might entail the generalization of the current confluence test and/or the replacement of $\equiv_V$ with some $\equiv'$ which is independent of the start expression (Δ, e) of the critical triple.

4.6 Notation in diagrams

In diagrams we usually use $\xrightarrow{R}$ to indicate that the rule R has been used. We use normal arrows $\xrightarrow{R}$ at the position of critical pair and dashed arrows $\overset{R}{\dashrightarrow}$ for any further rewrites with the respective rules.

The symbol $\overset{\equiv_V}{=\!=}$ indicates that two constrained-expressions are $\equiv_V$-equivalent (see Definition 4.11). Furthermore, in each rewriting step we only provide the newly added constraints.

Simply put, the diagrams represent an $\forall\exists$-relation: for all instances of the critical pair (modulo α), there are rewrites $\overset{R}{\dashrightarrow}$ such that the diagram is valid. For example, the following diagram would imply the commutativity of two rules R_1, R_2 modulo α, i.e. for all instances of the critical pair (modulo α) there are rewrites, according to the diagram, to α-equivalent expressions.



5. A Convergent Rewrite System for the Monad Laws

As an extended example, illustrating also the ideas and potential of the nominal modelling and unification in rewriting, in particular with atom-variables, we consider the monad laws (Wadler 1995). An informal explanation is that monads are a functional implementation of sequential actions, as an extension of the lambda calculus, where $a_1 \gg\!= a_2$ means a sequential combination of actions: a_1 is executed before a_2, and the return-value v of a_1 is used in action a_2, written in lambda notation as $(a_2\ v)$. These are used as programming device in Haskell (Haskell-community

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

2019; Peyton Jones 2003; Peyton Jones et al. 1996) for programming with state and to implement IO and concurrency. Besides the operational behaviour, there is a set of monad laws, describing the desired behaviour of monadic combinations as a set of rewrite rules (see below). Hamana (2017) used second-order unification, which is unification in the quotient by the α, β and η axioms, to show confluence. However, second-order unification is undecidable, and thus the application of this idea to other examples will in general lead to undecidable algorithmic questions. In addition, η is not correct in call-by-need functional languages like Haskell. Thus, we use (decidable) nominal unification with atom-variables to obtain also confluence, however, for a finer notion of unification and of equivalence, since we use only α-equivalence. An application of the rewrite system may be normalization of larger monadic expressions. This would require the correctness of the monad theory in the programming language in question, which holds for example in the call-by-need calculus CHF (Sabel and Schmidt-Schauß 2011).

We will use the following encoding: `return` is a function symbol of arity 0, `app` and `>>=` are function symbols of arity 2, where we write `>>=` as infix, and `app` as juxtaposition. A, B, C denote atom-variables, and other uppercase letters X, F, G, M expression-variables.
The three monad laws are encoded as rewrite rules as follows:

$$\begin{array}{lll} (Id_l)\ \varnothing & \vdash (\texttt{return}\ X)\ \texttt{>>=}\ F & \to F\ X \\ (Id_r)\ \varnothing & \vdash M\ \texttt{>>=}\ \texttt{return} & \to M \\ (A)\ \ A\#F, A\#G & \vdash (M\ \texttt{>>=}\ F)\ \texttt{>>=}\ G & \to M\ \texttt{>>=}\ (\lambda A.(F\ A)\ \texttt{>>=}\ G) \end{array}$$

It is a bit unusual that there are variables on the right-hand side which do not occur on the left-hand side. In this case we assume that the names of the introduced variables are fresh ones, i.e. these do not occur elsewhere in the same computation. In addition these fresh names are bound on the right-hand side. Note also that the constraints in rules restrict the introduced variables on the right-hand side of the rewrite rules. An overlap of the rules Id_r, Id_l with A leads to two extra rules $B\beta$, $B\eta$, and an overlap of $B\beta$ with Id_r to $B\beta FX$, see Figure 3.

Note that the three rules $B\eta$, $B\beta$ and $B\beta FX$ are consequences of the monad laws as equations (w.r.t. α-equivalence), see Figure 3. Note also that β or η as more general rules are inappropriate, since they would prevent an embedding of monad laws into call-by-need lambda calculi with contextual equivalence due to inconsistency of η in these semantics, and since the rule β (in general) leads to nontermination of rewrite rules (Sabel and Schmidt-Schauß 2012).

$$\begin{array}{lll} (B\eta)\ \ A\#F & \vdash (M\ \texttt{>>=}\ \lambda A.F\ A) & \to M\ \texttt{>>=}\ F \\ (B\beta)\ \ A\#F, A\#G & \vdash (\lambda A.(F\ A)\ \texttt{>>=}\ G)\ X & \to (F\ X)\ \texttt{>>=}\ G \\ (B\beta FX)\ A\#F & \vdash (\lambda A.(F\ A))\ X & \to (F\ X) \end{array}$$

The combined rewriting system $\mathcal{R}_{monad}$ consists of the six rules $\{Id_l, Id_r, A, B\eta, B\beta$ and $B\beta FX\}$. Note that the rewrite rules satisfy Definition 4.2, which follows, since (A) only introduces bound fresh names, and the other rules do not introduce fresh names. It is terminating, since the rules either strictly decrease the size, or move the `>>=` -bracketing to the right and increase the size by a constant (say 3). Termination of the rewrite system is a prerequisite for applying the Knuth–Bendix confluence test.

The nominal monad rewrite system $\mathcal{R}_{monad}$ is between first order and higher order. We use nominal unification for computing the critical pairs and nominal matching for rewriting, where we permit atom-variables in every case.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

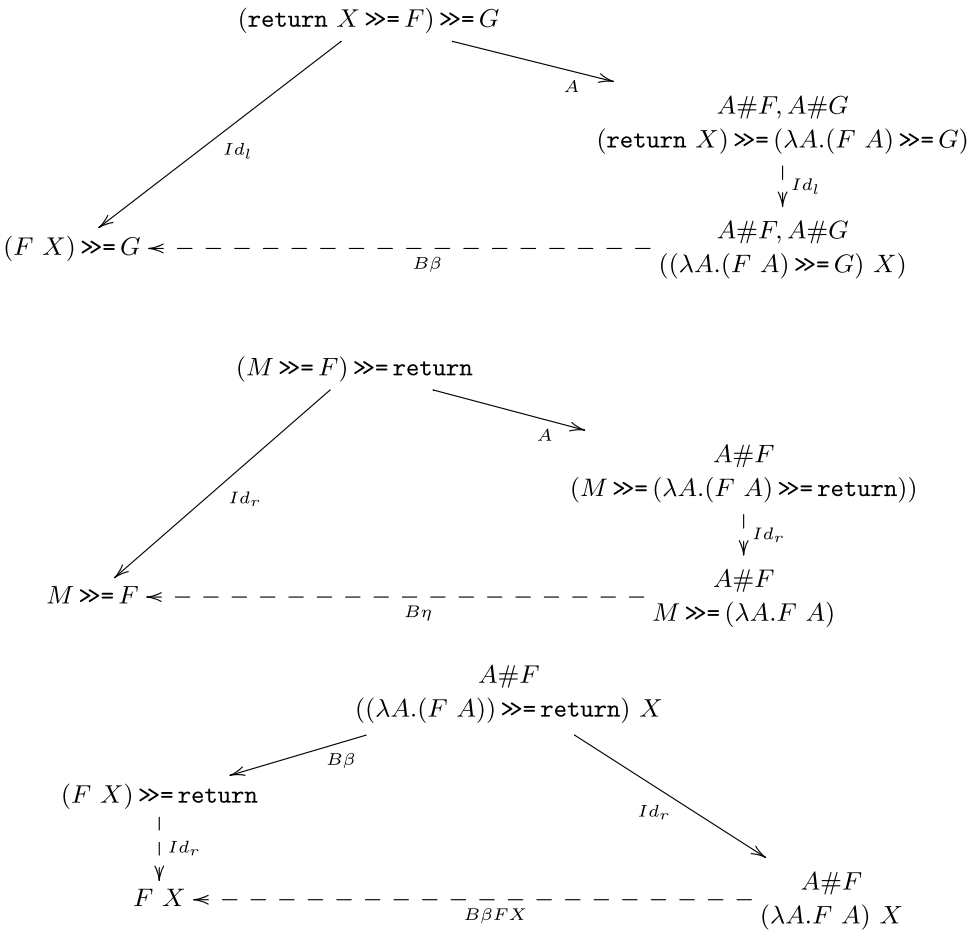


Figure 3. Completion of the Monad Rules

The following table shows the overlap possibilities.

	Id_l Id_r	A	$B\eta$	$B\beta$	$B\beta FX$
Id_l	*trivial*	*Figure* 3	*Figure* 6	−−	−−
Id_r		*Figures* 3 and 4	−−	*Figure* 3	−−
A		*Figure* 6	*Figure* 4C and D	−−	−−
$B\eta$			−−	*Figures* 4 and 6	*Figure* 6
$B\beta$				*Figure* 8	*Figure* 5
$B\beta FX$					*Figure* 6

Where *trivial* means that the critical pair is trivial, and −− means there is no overlap. We omit $B\beta FX$, since there are no overlaps.

Lemma 5.1. *The final expressions in Figure 7 can be joined under the union of all constraints.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

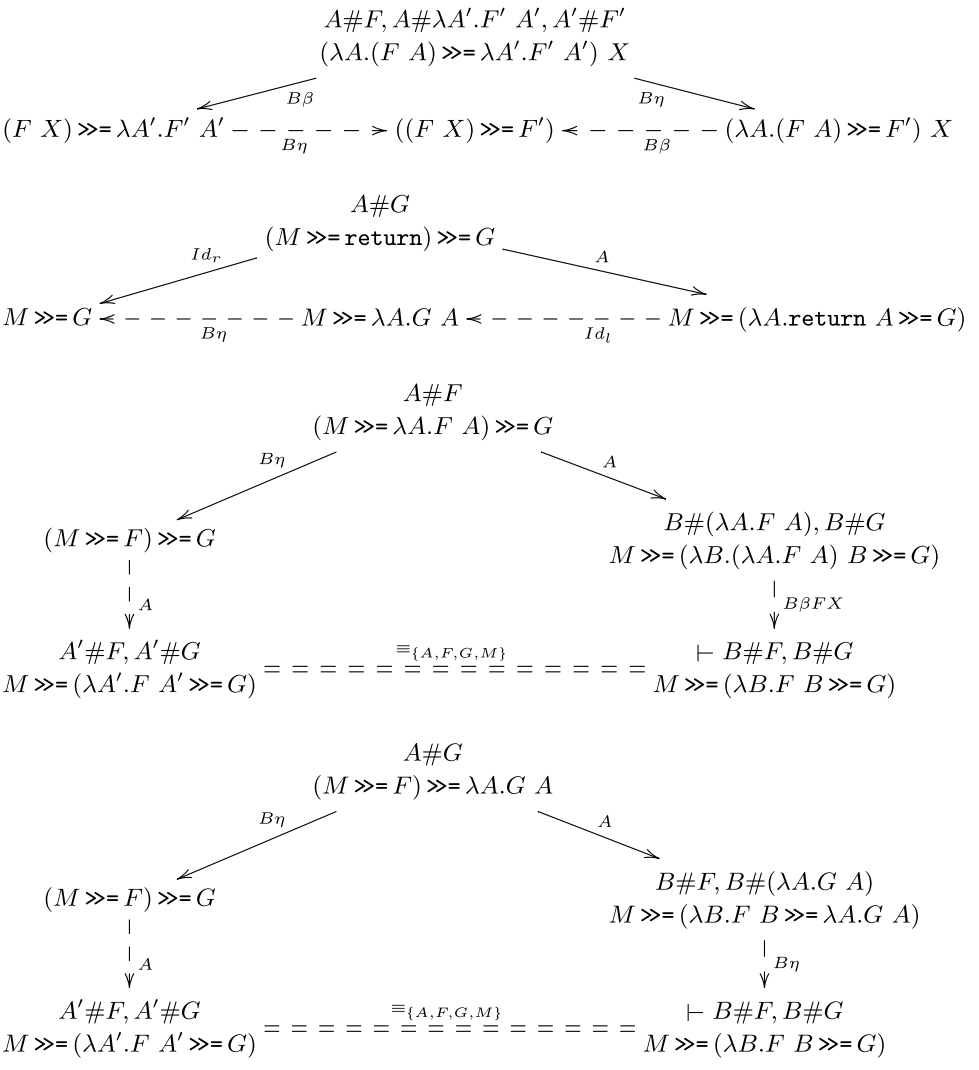


Figure 4. Joining the nontrivial critical pairs of Monad Theory: diagrams first part.

Proof. The constraints are: $A\#\lambda A'.F\ A', A'\#F$. This implies $A\#F$ by a case analysis whether A and A' are equally instantiated or not. This in turn implies $F' \sim (A\ A')\cdot F'$. □

Before we prove that the nontrivial A–A-overlap can be joined, we look at a seemingly trivial overlap. It is reducing $(M \gg\!= F) \gg\!= G$ in two ways using (A) on the top: One result is $M \gg\!= (\lambda A.(F\ A) \gg\!= G)$ with $A\#F, G$, and another one is $M \gg\!= (\lambda B.(F\ B) \gg\!= G)$ with $B\#F, G$. The essential step in showing $\equiv_{\{M,F,G\}}$ of the resulting constrained expressions is to argue that $\lambda A.(F\ A) \gg\!= G \sim \lambda B.(F\ B) \gg\!= G$ by arguing that $(F\ A) \gg\!= G \sim (A\ B)\cdot(F\ B) \gg\!= G$, where the freshness constraints show that this reasoning is correct.

The pair arising from the proper overlap of the associativity rule (A) with itself needs a check if the final expressions are equivalent under the union of the constraints, which requires a bit more of computations.

Lemma 5.2. *The final expressions in the A–A diagram in Figure 6 are joinable.*

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

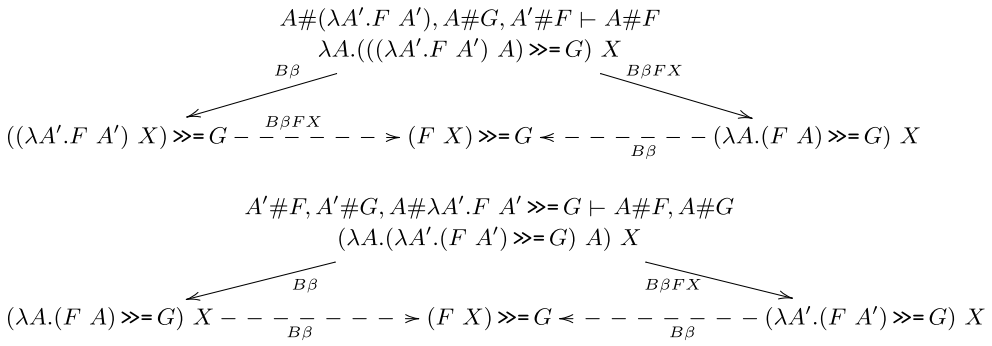


Figure 5. Joining the nontrivial critical pairs of Monad Theory: *BβFX* and *Bβ*

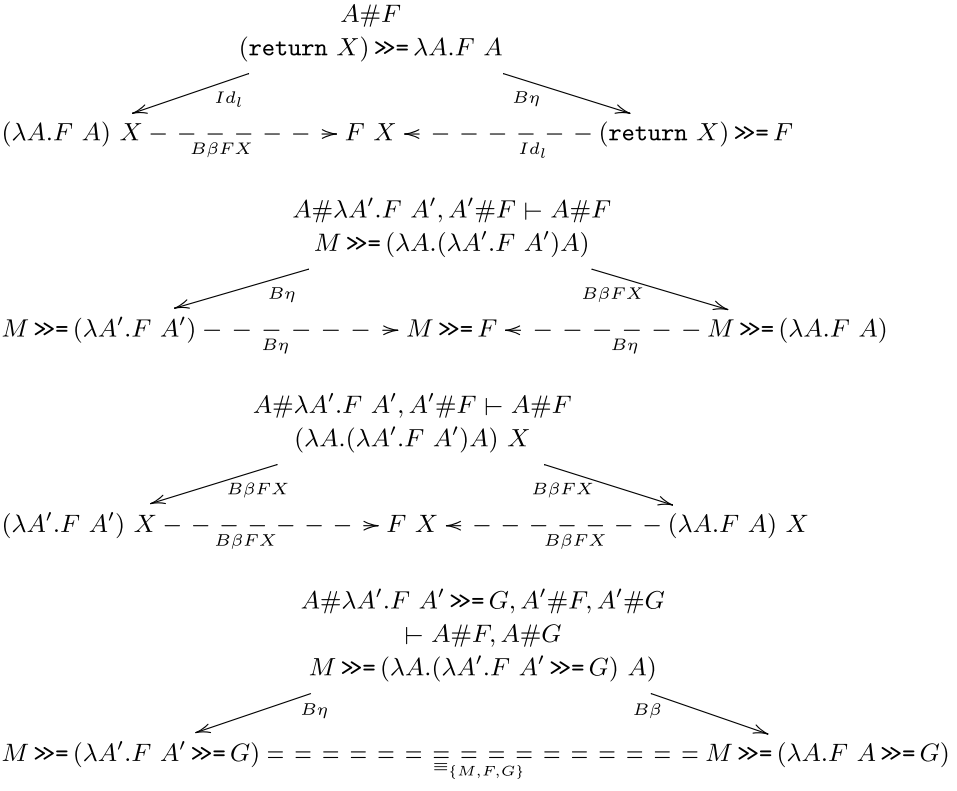


Figure 6. Joining the nontrivial critical pairs of Monad Theory: diagrams second part.

Proof. The freshness constraints in the A–A diagram in Figure 6 are as follows:

left:	$A\#F, G$	$A'\#G, G'$	$B'\#F$	$B'\#\lambda A'.G\ A' >\!\!>\!\!= G'$
right:	$A\#F, G$	$A'\#G, G'$	$B\#G'$	$B\#\lambda A.F\ A >\!\!>\!\!= G$ $\quad C\#G, G'$

We can derive the following further constraints:

(1) (right): $B\#F, G$: If $\gamma(B) = \gamma(A)$, then this follows from $A\#F, G$.
If $\gamma(B) \neq \gamma(A)$, then it follows from $B\#\lambda A.F\ A >\!\!>\!\!= G$.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

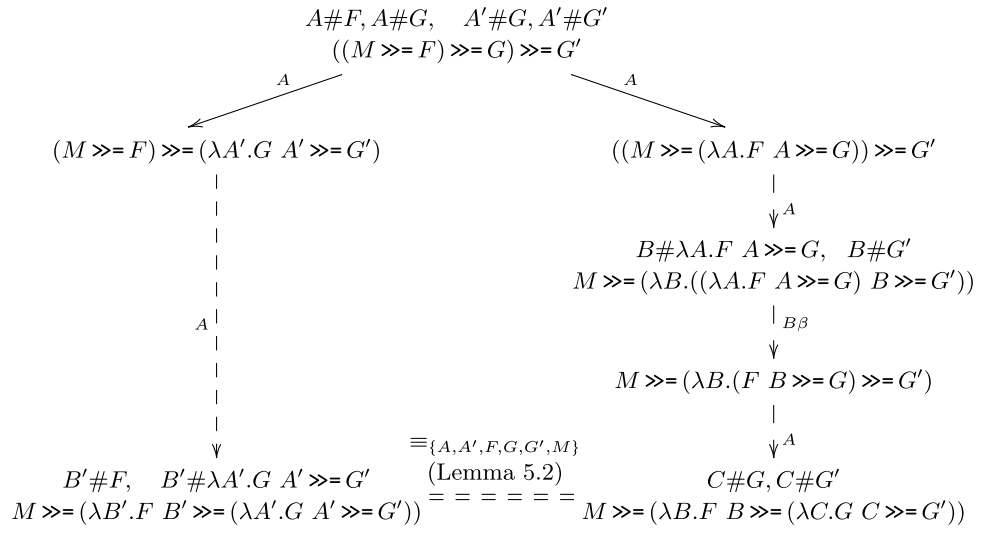


Figure 7. Joining the nontrivial critical pairs of Monad Theory: the A–A diagram

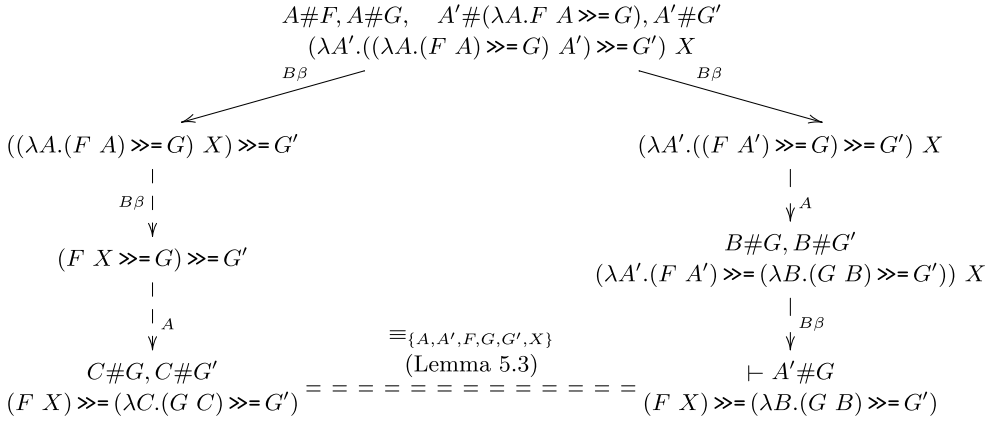


Figure 8. Joining the nontrivial critical pairs of Monad Theory: the $B\beta$–$B\beta$ diagram

(2) (left) $B'\#G$, G': If $\gamma(B') = \gamma(A')$, then this follows from $A\#G$, G'.
If $\gamma(B) \neq \gamma(A')$, then it follows from $B'\#\lambda A'.G\ A' \gg\!= G'$.

Now we have to verify the following equivalence:

$$M \gg\!= (\lambda B'.F\ B' \gg\!= (\lambda A'.G\ A' \gg\!= G')) \equiv_{\{A,A',F,G,G',M\}} M \gg\!= (\lambda B.F\ B \gg\!= (\lambda C.G\ C \gg\!= G'))$$

This is equivalent to verifying:

$$(\lambda B'.F\ B' \gg\!= (\lambda A'.G\ A' \gg\!= G')) \equiv_{\{A,A',F,G,G',M\}} (\lambda B.F\ B \gg\!= (\lambda C.G\ C \gg\!= G'))$$

Using the given and derived constraints, and since B, $B'\#F$, G, G', this is equivalent to verifying:

$$F\ B' \gg\!= (\lambda A'.G\ A' \gg\!= G') \equiv_{\{A,A',F,G,G',M\}} F\ B' \gg\!= (\lambda (B\ B')\cdot C.(G\ (B\ B')\cdot C) \gg\!= G'))$$

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

A case analysis shows the remaining parts:

(1) If $\gamma(A') = \gamma((B\ B')\cdot C)$, then this is correct by a direct decomposition.
(2) If $\gamma(A') \neq \gamma((B\ B')\cdot C)$, then after an application of $(A'\ \ (B\ B')\cdot C))$, and due to $A'\#G, G'$, and $B, B'\#G, G'$ a direct decomposition shows equality.

Thus, we have shown that for $V = \{A, A', F, G, G', M\}$ the formula:

$$\forall V : \nabla_l \cup \nabla_r \implies (\lambda B'.F\ B' \gg\!= (\lambda A'.G\ A' \gg\!= G')) \sim (\lambda B.F\ B \gg\!= (\lambda C.G\ C \gg\!= G'))$$

holds. Lemma 4.18 then implies the $\equiv_V$-equivalence and the join. □

Lemma 5.3. *The final expressions in the $B\beta$–$B\beta$ diagram are joinable.*

Proof. The proof is analogous to the proof in Lemma 5.2. □

As a summary we obtain:

Theorem 5.4. *The monad axioms (Id_l), (Id_r) and (A) modulo α-equivalence have as completion the additional rewrite rules $(B\eta)$, $(B\beta)$ and $(B\beta FX)$.*
The rewrite system consisting of these six rewrite rules is terminating and confluent (as a ground rewriting system), and a decision algorithm for the word-problem of the rewrite-theory of monad axioms in NL_a, modulo α-equality.

Proof. This follows from our computations in this section, the join-diagrams in this section, in particular Lemma 5.2, and the correctness of the Knuth–Bendix confluence test for NL_{AS} in Theorems 4.19 and 4.20. □

6. Comparison of Our Approach with Nominal Rewriting with Atoms

Nominal rewriting was introduced by Fernández et al. (2004) as a way to define equivariant relations on NL_a similar to first-order rewriting. We provide a description of this approach while using our notations. To distinguish it from our formalism, it will be referred to as *equivariant rewriting*.

Definition 6.1. *Let NL_{aS} be the nominal language built with atoms and expression-variables. Let $s, t \in NL_{aS}$ be two expressions and let ∇ be a freshness environment on NL_{aS}-expressions. A rewrite judgement is defined as: $\nabla \vdash l \to r$.*

The semantics of the induced relation on NL_a can be defined as follows (note that several equivalent definitions exist).

(1) The relation $\to$ on NL_a is equivariant, i.e. if $e_1 \to e_2$ holds, then $\pi \cdot e_1 \to \pi \cdot e_2$ holds as well for all permutations π on atoms.
(2) For all ground substitutions γ for which $\nabla\gamma$ is valid, $s\gamma \to t\gamma$ holds.

During rewriting the first condition is "hidden" in an equivariant matching procedure. That is, rather than trying to match two NL_{aS} constrained expressions, $(\nabla, l) \preceq (\Delta, e)$ with only a substitution and a freshness environment, one can also use a permutation on atoms π to make the two expressions equal.

Specifically, this means finding a triple (∇', θ, π) s.t. $\nabla' \vDash l^\pi\theta \sim e$ and $\Delta \vDash \nabla^\pi\theta \cup \nabla'$, where l^π denotes the application on π only on atoms – not on expression-variables.

As a result, the atoms in such a rewrite rule gain a variable like character. As a matter of fact, one could define an equivalent matching procedure in NL_{aAS} – different from the one used in this paper.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

To do that, one would map every atom a_i on the left side of the matching equation $(\nabla, l) \preceq (\Delta, t)$ to an atom-variable A_i and utilize the additional freshness constraints $\nabla' = \{A_i \# A_j \mid i, j \in \{1, \ldots, k\}, i < j\}$ to enforce that any solution of the matching problem matches the atom-variables to different atoms. The part of the solution which matches atom-variables to atoms would then work like the permutation π in equivariant matching, with the only difference of it being a bijection between atom-variables and atoms, rather than atoms and atoms.

This brings us to the first obvious difference of our formalism to the framework of Fernández et al. (2004), the usage of atom-variables rather than atoms.

Example 6.2. Consider a simple version of (cpcx) in the concurrent calculus CHF (Sabel and Schmidt-Schauß 2011, 2012) or in other functional programming calculi, formulated as a rewrite rule:

$$\{B \# A_i \mid i \in \{1, \ldots, k\}\} \vdash \texttt{let}\ B = c\ A_1 \ldots A_k\ \texttt{in}\ B \to\ \texttt{let}\ B = c\ A_1 \ldots A_k\ \texttt{in}\ c\ A_1 \ldots A_k$$

where we do not care about the equality/inequality of the variable names occurring in this context. To define an equivalent relation $\to$ on NL_a in equivariant rewriting, one would need to add a rule for each variant of equality/inequality of the atom-variables, yielding exponentially many rules.

The second difference, which is more subtle and at the same time semantically more meaningful, is which expressions can in principle be matched.

Example 6.3. Consider the η-expansion of the lambda calculus formulated as a rule in equivariant rewriting:

$$a \# S \vdash S \to \lambda a.\texttt{app}\ S\ a$$

Within the framework of equivariant rewriting, the matching problem

$$(\{a \# S, s\}) \preceq (\varnothing, S')$$

has no matcher, even though there always exists an atom b, s.t. $b \# S'$ holds. However,

$$(\{a \# S, s\}) \preceq (\{b \# S'\}, S')$$

has a matcher in $(\varnothing, \{S \mapsto S'\}, (a\ b))$.

In equivariant rewriting no new freshness constraints can be introduced, even if such an introduction would be semantically correct. This has the benefit that the constrained implication check of the procedure, $\Delta \vDash \nabla^\pi \theta \cup \nabla'$, collapses to checking a subset property $\nabla^\pi \theta \cup \nabla \subseteq \Delta$ which in turn allows fixing the initial constraint set Δ. However, it introduces a mismatch between what can semantically be matched and what is procedurally matched. Fernández and Gabbay (2010) note that "this mismatch between nominal rewriting and nominal algebra could be solved by including fresh atom generation in the definition of a rewriting step". This is in fact what is happening during the rewriting step of the approach taken in this paper, with the benefit of being able to match things like η-expansion directly and the downside of having to reason about a changing freshness environment.

6.1 On orthogonality and alpha-stability

In this section we sketch out the differences and similarities between properties of nominal orthogonal rewriting systems in the previous and in our approach. Some of the questions which have been studied are: which additional properties need to be checked to obtain a similar behaviour as first-order rewriting systems. For example, the following questions are of interest:

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

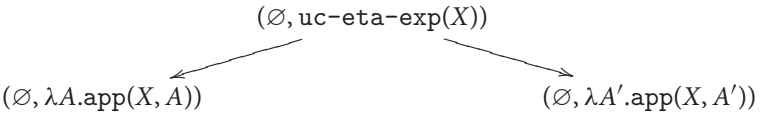
(1) Which conditions have to be met to restrict the check of critical pairs in the Knuth–Bendix Test to proper critical pairs, i.e. critical pairs which do not arise from the overlap at the top position of a rule with a copy of itself? (Suzuki et al. 2016)
(2) Under which circumstances are orthogonal rewriting systems confluent? (Suzuki et al. 2015)
(3) Can these properties be checked efficiently? (Ayala-Rincón et al. 2016)

A first necessary condition is uniformity, which prevents rules from introducing fresh unbound atoms (see Definition 4.2) However, this is not a sufficient condition, as an example from Suzuki et al. (2015) shows.

Example 6.4. This example is borrowed from Suzuki et al. (2015) (Example 19) but adapted to the formalism in this paper. It formulates an unconditional η-expansion:

$$\varnothing \vdash \texttt{uc-eta-exp}(X) \to \lambda A.\texttt{app}(X, A)$$

It has a critical pair on top position, which is:



To check if it is trivial, we start off by using `EqToCons` on $\lambda A.\texttt{app}(X, A) \sim \lambda A'.\texttt{app}(X, A')$. The algorithm computes the constraints $\{A\#\lambda B.X, B\#\lambda A.X, A\#\lambda B.XB\}$ which can be transformed into the *QFL*-formula

$$(A\#B \wedge A\#X \wedge B\#X) \vee A =_{\#} B$$

Finally, we need to check

$$\forall A, B, X : \varnothing \implies ((A\#B \wedge A\#X \wedge B\#X) \vee A =_{\#} B)$$

Since $\varnothing$ is the trivial constraint, this is equivalent to:

$$\forall A, B, X : ((A\#B \wedge A\#X \wedge B\#X) \vee A =_{\#} B)$$

This *QFL* formula is false since $\rho(A) = a$, $\rho(B) = b$, $\rho(X) = \texttt{app}(a, b)$ is a falsifying interpretation. Thus, even though the rule is left-linear, its induced relation is not confluent.

This implies that (1) on uniform rules (see Definition 4.2), the check of non-proper CPs is still necessary in general and (2) that uniform orthogonal rewriting systems are not necessarily confluent. This brought about the notion of alpha-stability defined in Suzuki. In our formalism this is written as follows:

Definition 6.5. *Let $R = \nabla \vdash l \to r$ be a rewrite rule. Then it is called α-**stable** if for all NL_a-expressions $s_1, s_2, t_1, t_2 \in NL_a$ s.t. $s_1 \sim s_2$, $s_1 \xrightarrow{R,NL_a,\epsilon} t_1$ and $s_2 \xrightarrow{R,NL_a,\epsilon} t_2$ the α-equivalence $t_1 \sim t_2$ holds.*

The definition is equivalent to the definition in Suzuki et al. (2016) on ground relations for rewrite rules where all atom-variables are forced to be different using the constraints. Suzuki proved that uniformity plus alpha-stability are sufficient for orthogonal rewrite systems to be confluent. This carries over to our formalism.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Lemma 6.6. *Let $R = \nabla \vdash l \to r$ be a rewrite rule and $R' = \nabla' \vdash l' \to r'$ be a fresh copy of R. Let (Δ, σ) be the MGU of $(\nabla, l) \doteq (\nabla', l')$. Then R is α-stable if and only if:*

$$\begin{array}{ccc} & (\Delta, l\sigma) & \\ {\scriptstyle R}\swarrow & & \searrow{\scriptstyle R} \\ (\Delta, r\sigma) & \overset{\equiv_V}{=\!=\!=\!=\!=} & (\Delta, r'\sigma) \end{array}$$

Proof. First assume that the critical pair is trivial.

Let $s_1, s_2, t_1, t_2 \in NL_a$ be expressions s.t. $s_1 \sim s_2$, $s_1 \xrightarrow{R,NL_a,\epsilon} t_1$ and $s_2 \xrightarrow{R,NL_a,\epsilon} t_2$ hold. By definition of $\xrightarrow{R,NL_a,\epsilon}$, there are ground substitutions γ_1, γ_2 s.t. $\nabla\gamma_1$ valid, $\nabla'\gamma_2$, $dom(\gamma_1) \cap dom(\gamma_2) = \varnothing$ and:

$$\begin{array}{ccccccc} l\gamma_1 & \sim & s_1 & \sim & s_2 & \sim & l'\gamma_2 \\ \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon \\ r\gamma_1 & \sim & t_1 & & t_2 & \sim & r'\gamma_2 \end{array}$$

where $\downarrow\epsilon$ is used instead of $\xrightarrow{R,NL_a,\epsilon}$ for better readability. We need to show that $t_1 \sim t_2$. Because $dom(\gamma_1) \cap dom(\gamma_2) = \varnothing$ we can define $\gamma = \gamma_1 \cup \gamma_2$ and obtain $l\gamma_1 = l\gamma \sim l'\gamma = l'\gamma_2$.

Thus, γ is a solution of the unification problem $(\nabla, l) \doteq (\nabla', l')$.

Because (Δ, σ) is a MGU of the unification problem, there must be ρ, s.t. $\gamma \sim \sigma \circ \rho$. This yields:

$$\begin{array}{ccccccccccc} l\sigma\rho & \sim & l\gamma & \sim & s_1 & \sim & s_2 & \sim & l'\gamma & \sim & l'\sigma\rho \\ \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon & & \downarrow\epsilon \\ r\sigma\rho & \sim & r\gamma & \sim & t_1 & & t_2 & \sim & r'\gamma & \sim & r'\sigma\rho \end{array}$$

From $(\Delta, r\sigma) \equiv_V (\Delta, r'\sigma)$ and Lemma 4.13, we obtain $r\sigma\rho \sim r'\sigma\rho$. Because $\sim$ is an equivalence relation, it follows that $t_1 \sim t_2$.

Now assume that R is α-stable. Because of Lemma 4.18 we only need to prove:

$$\forall V : \Delta \implies r\sigma \sim r'\sigma$$

Let ρ be an arbitrary ground substitution with $\Delta\rho$ valid and

$$\begin{array}{ccc} l\sigma\rho & \sim & l'\sigma\rho \\ \downarrow\epsilon & & \downarrow\epsilon \\ r\sigma\rho & & r'\sigma\rho \end{array}$$

Because of α-stability $r\sigma\rho \sim r'\sigma\rho$ must hold, and because ρ was chosen arbitrarily the following formula follows:

$$\forall V : \Delta \implies r\sigma \sim r'\sigma.$$ □

Theorem 6.7. *Let $\mathcal{R}$ be a set of α-stable, left-linear rewrite rules with no proper critical pairs. Then its induced relation is locally confluent.*

Proof. Local confluence follows from Lemma 6.6 and Theorem 4.19. □

The problem with α-stability is that in general it cannot be checked efficiently. To get around this, Suzuki et al. (2015) defined the notion *abstract skeleton preserving*, which implies α-stability but can be efficiently checked. Ayala-Rincón et al. (2016) extended this research further by introducing the notion closed rewrite rules, which again are α-stable but can be reduced to nominal

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

matching and therefore be efficiently checked. The relation of these concept to the formalism in this paper is subject to future research.

7. Conclusion

We have developed a nominal matching algorithm for constrained nominal expressions, and determined the complexity. We succeeded in formulating a variant of the Knuth–Bendix confluence test for rewrite system based on our nominal language NL_{AS} with atom-variables, where the objects to be rewritten are constrained expressions. We obtained a decidable criterion for testing confluence, which in the successful case leads to a decidable α-equivalence check for theories on NL_{AS}, i.e. we obtain also decidability of word-problems modulo α-equivalence.

Thus, our method extends the rewriting and confluence check method of Fernández and Gabbay (2007) by improving the treatment of (dis-)equality of atoms in a more systematic way and by computing new compatible constraints. Previous results on critical pairs, α-stability and orthogonal rewriting systems were shown to carry over.

We also investigated as an extended example the higher-order theory of monads, which illustrates the application of the Knuth–Bendix confluence criterion. We also obtained a result for the theory of monads: A confluent rewrite system for monads is constructed as a completion of the three defining rules. This is more fine-grained than the system in Hamana (2017), which uses full beta-reduction.

Future work is to investigate whether also for (general) NL_{AS}-rewriting on constrained expressions a variant of the Knuth–Bendix criterion for confluence can be constructed. Another direction of future work is to extend the Knuth–Bendix criterion for nominal rewriting with atom-variables to rewriting modulo an equivalence relation.

Furthermore, we hope to extend the method to equational theories that are defined in more general ways, for example, using descriptions of infinite sets of equations by context variables in rules, and applying the nominal unification algorithm as described in Schmidt-Schauß and Sabel (2018).

We also plan to implement a confluence tester for nominal term rewriting systems using our Knuth–Bendix algorithm with atom-variables.

A potential application is some reduction rules in the call-by-need calculus of Ariola et al. (1995) and also to the concurrent Haskell variant CHF (Sabel and Schmidt-Schauß 2011, 2012) like $\texttt{let}\ y = v\ \texttt{in}\ C[y] \to \texttt{let}\ y = v\ \texttt{in}\ C[v]$, where v is a value, or similar rules.

Notes

1 Inspired by an anonymous reviewer.

References

Aoto, T. and Kikuchi, K. (2016). Nominal confluence tool. In: *International Joint Conference on Automated Reasoning*, Springer, 173–182.

Ariola, Z. M., Felleisen, M., Maraist, J., Odersky, M. and Wadler, P. (1995). A call-by-need lambda calculus. In: *POPL 1995*, ACM Press, 233–246.

Ayala-Rincón, M., de Carvalho-Segundo, W., Fernández, M. and Nantes-Sobrinho, D. (2019a). A formalisation of nominal c-matching through unification with protected variables. *Electronic Notes in Theoretical Computer Science* **344** 47–65.

Ayala-Rincón, M., Fernández, M., Gabbay, M. J. and Rocha-Oliveira, A. C. (2016). Checking overlaps of nominal rewriting rules. *Electronic Notes in Theoretical Computer Science* **323** 39–56.

Ayala-Rincón, M., Fernández, M., Silva, G. F. and Nantes-Sobrinho, D. (2019b). A certified functional nominal c-unification algorithm. In: *Pre-Proceedings of the 29th International Symposium Logic-Based Program Synthesis and Transformation (LOPSTR)*.

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press

Calvès, C. and Fernández, M. (2008). A polynomial nominal unification algorithm. *Theoretical Computer Science* **403** (2-3) 285–306.
Cheney, J. (2004). *Nominal Logic Programming*. PhD thesis, Cornell University.
Cheney, J. (2010). Equivariant unification. *Journal of Automated Reasoning* **45** (3) 267–300.
Fernández, M. and Gabbay, M. J. (2007). Nominal rewriting. *Information and Computation* **205** (6) 917–965.
Fernández, M. and Gabbay, M. J. (2010). Closed nominal rewriting and efficiently computable nominal algebra equality. In: Crary, K. and Miculan, M. (eds.) *Proceedings 5th International Workshop on Logical Frameworks and Meta-languages: Theory and Practice, LFMTP 2010, Edinburgh, UK, 14th July 2010*, EPTCS, vol. 34, 37–51.
Fernández, M., Gabbay, M. J. and Mackie, I. (2004). Nominal rewriting systems. In: *Proceedings of the 6th ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming*, PPDP 2004, ACM, 108–119.
Fernández, M. and Rubio, A. (2012). Nominal completion for rewrite systems with binders. In Czumaj, A., Mehlhorn, K., Pitts, A. M. and Wattenhofer, R. (eds.) *Proceedings 39th ICALP Part II*, LNCS, vol. 7392, Springer, 201–213.
Hamana, M. (2017). How to prove your calculus is decidable: practical applications of second-order algebraic theories and computation. *Proceedings of the ACM on Programming Languages* **1** (ICFP) 22:1–22:28.
Haskell-community (2019). *Haskell Main Website*. www.haskell.org.
Kikuchi, K., Aoto, T., and Toyama, Y. (2017). Parallel closure theorem for left-linear nominal rewriting systems. In: *International Symposium on Frontiers of Combining Systems*, Springer, 115–131.
Knuth, D. and Bendix, P. B. (1970). Simple word problems in universal algebra. In: Leech, J. (ed.) *Computational Problems in Abstract Algebra*, Pergamon Press, 263–297.
Levy, J. and Villaret, M. (2010). An efficient nominal unification algorithm. In: Lynch, C. (ed.) *Proceedings of 21st RTA*, LIPIcs, vol. 6, Schloss Dagstuhl, 209–226.
Papadimitriou, C. (1994). *Computational Complexity*. Addison-Wesley.
Peyton Jones, S. L. (2003). *Haskell 98 Language and Libraries: The Revised Report*. Cambridge University Press. www.haskell.org.
Peyton Jones, S. L., Gordon, A. and Finne, S. (1996). Concurrent Haskell. In *Proceedings of 23rd ACM POPL 1996*, ACM, 295–308.
Pitts, A. (2016). Nominal techniques. *ACM SIGLOG News* **3** (1) 57–72.
Pitts, A. M. (2013). *Nominal Sets: Names and Symmetry in Computer Science*. Cambridge University Press.
Sabel, D. and Schmidt-Schauß, M. (2011). A contextual semantics for concurrent Haskell with futures. In: Schneider-Kamp, P. and Hanus, M. (eds.) *Proceedings of 13th ACM PPDP 2011*, ACM, 101–112.
Sabel, D. and Schmidt-Schauß, M. (2012). Conservative concurrency in Haskell. In: *LICS 2012*, IEEE, 561–570.
Schmidt-Schauß, M. and Sabel, D. (2018). Nominal unification with atom and context variables. In: Kirchner, H. (ed.) *3rd International Conference on Formal Structures for Computation and Deduction, FSCD 2018, July 9–12, 2018, Oxford, UK*, LIPIcs, vol. 108, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 28:1–28:20.
Schmidt-Schauß, M., Sabel, D. and Kutz, Y. D. K. (2019). Nominal unification with atom-variables. *Journal of Symbolic Computation* **90** 42–64.
Suzuki, T., Kikuchi, K., Aoto, T. and Toyama, Y. (2015). Confluence of orthogonal nominal rewriting systems revisited. In: *26th International Conference on Rewriting Techniques and Applications (RTA 2015)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
Suzuki, T., Kikuchi, K., Aoto, T. and Toyama, Y. (2016). Critical pair analysis in nominal rewriting. In: *SCSS*, 156–168.
Urban, C. (2008). Nominal techniques in Isabelle/HOL. *Journal of Automated Reasoning* **40** (4) 327–356.
Urban, C. and Kaliszyk, C. (2012). General bindings and alpha-equivalence in nominal Isabelle. *Logical Methods in Computer Science* **8** (2) 1–35.
Urban, C., Pitts, A. M. and Gabbay, M. (2003). Nominal unification. In: *17th CSL, 12th EACSL, and 8th KGC*, LNCS, vol. 2803, Springer, 513–527.
Urban, C., Pitts, A. M. and Gabbay, M. J. (2004). Nominal unification. *Theoretical Computer Science* **323** (1–3) 473–497.
Wadler, P. (1995). Monads for functional programming. In: Jeuring, J. and Meijer, E. (eds.) *Advanced Functional Programming, First International Spring School on Advanced Functional Programming Techniques, Båstad, Sweden, May 24-30, 1995, Tutorial Text*, LNCS, vol. 925, Springer, 24–52.

Cite this article: Kutz Y and Schmidt-Schauß M (2020). Rewriting with generalized nominal unification. *Mathematical Structures in Computer Science* **30**, 710–735. https://doi.org/10.1017/S0960129520000122

https://doi.org/10.1017/S0960129520000122 Published online by Cambridge University Press