Learning Nominal Automata

Joshua Moerman  
Radboud University, The Netherlands  
joshua.moerman.cs.ru.nl

Matteo Sammartino  
University College London, UK  
{m.sammartino,alexandra.silva}@ucl.ac.uk

Bartek Klin  
University of Warsaw, Poland  
{klin,szynwelski}@miuw.edu.pl

Abstract

We present an Angluin-style algorithm to learn nominal automata, which are acceptors of languages over infinite (structured) alphabets. The algorithm is sometimes referred to as active learning, where a fixed set of positive and negative examples is given and no interaction with the system is possible.

Categories and Subject Descriptors D.1.1 [Software]: Programming Techniques; F.4.3 [Mathematical Logic and Formal Languages]: Formal Languages; I.3.2 [Artificial Intelligence]: Learning

Keywords Active Learning, (Non)Deterministic Finite Automata, Nominal Automata, Functional Programming

1. Introduction

Automata are a well established computational abstraction with a wide range of applications, including modelling and verification of (security) protocols, hardware, and software systems. In an ideal world, a model would be available before a system or protocol is deployed in order to provide ample opportunity for checking important properties that must hold and only then the actual system would be synthesized from the verified model. Unfortunately, this is not at all the reality: systems and protocols are developed and tested in short spans of time and if mistakes occur they are most likely found after deployment. In this context, it has become popular to infer or learn a model from a given system just by observing its behaviour or response to certain queries. The learned model can then be used to ensure the system is complying to desired properties or to detect bugs and design possible fixes.

Automata learning, or regular inference [3], is a widely used technique for creating an automaton model from observations. The original algorithm [3], by Dana Angluin, works for deterministic finite automata, but since then has been extended to other types of automata [4][5][7], including Mealy machines and I/O automata, and even a special class of context-free grammars. Angluin’s algorithm is sometimes referred to as active learning, because it is based on direct interaction of the learner with an oracle (“the Teacher”) that can answer different types of queries. This is in contrast with passive learning, where a fixed set of positive and negative examples is given and no interaction with the system is possible.

In this paper, staying in the realm of active learning, we will extend Angluin’s algorithm to a richer class of automata. We are motivated by situations in which a program model, besides control flow, needs to represent basic data flow, where data items are compared for equality (or for other theories such as total ordering). In these situations, values for individual symbols are typically drawn from an infinite domain and automata over infinite alphabets become natural models, as witnessed by a recent trend [8][9][12][15][17].

One of the foundational approaches to formal language theory for infinite alphabets uses the notion of nominal sets [9]. The theory of nominal sets originates from the work of Fraenkel in 1922, and they were originally used to prove the independence of the axiom of choice and other axioms. They have been rediscovered in Computer Science by Gabbay and Pitts [36], as an elegant formalism for modeling name binding, and since then they form the basis of many research projects in the semantics and concurrency community. In a nutshell, nominal sets are infinite sets equipped with symmetries which make them finitely representable and tractable for algorithms. We make crucial use of this feature in the development of a learning algorithm.

Our main contributions are the following.

• A generalization of Angluin’s original algorithm to nominal automata. The generalization follows a generic pattern for transporting computation models from finite sets to nominal sets, which leads to simple correctness proofs and opens the door to further generalizations. The use of nominal sets with different symmetries also creates potential for generalization, e.g. to languages with time features [7] or data dependencies represented as graphs [33].

• An extension of the algorithm to nominal non-deterministic automata (nominal NFAs). To the best of our knowledge, this is the first learning algorithm for non-deterministic automata over infinite alphabets. It is important to note that, in the nominal setting, NFAs are strictly more expressive than DFAs. We learn a subclass of the languages accepted by nominal NFAs, which includes all the languages accepted by nominal DFAs. The main advantage of learning NFAs directly is that they can provide exponentially smaller automata when compared to their deterministic counterpart. This can be seen both as a generalization and as an optimization of the algorithm.

• An implementation using our recently developed Haskell library tailored to nominal computation – NLambda [26]. Our implementation is the first non-trivial application of a novel programming paradigm of functional programming over infinite...
we revise some basic concepts of nominal sets and automata. Section
4 contains a discussion of related work. We conclude the paper with a discussion section where also future directions are presented.

2. Overview of the approach

In this section, we give an overview of the work developed in the paper through examples. We will start by explaining the original algorithm for regular languages over finite alphabets, and then explain the challenges in extending it to nominal languages.

Angluin’s algorithm \( L^* \) provides a procedure to learn the minimal DFA accepting a certain (unknown) language \( L \). The algorithm has access to a teacher which answers two types of queries:

- **Membership queries**, consisting of a single word \( w \in A^* \), to which the teacher will reply whether \( w \in L \) or not;
- **Equivalence queries**, consisting of a hypothesis DFA \( H \), to which the teacher replies yes if \( L(H) = L \), and no otherwise, providing a counterexample \( w \in L \triangle L \) (\( \triangle \) denotes the symmetric difference of two languages).

The learning algorithm works by incrementally building an observation table, which at each stage contains partial information about the language \( L \). The algorithm is able to fill the table with membership queries. As an example, and to set notation, consider the following table (over \( A = \{a, b\} \)).

This table indicates that \( L \) contains at least \( aa \) and definitely does not contain the words \( e, a, b, ba, baa, aaa \). Since \( row \) is fully determined by the language \( L \), we will from now on refer to an observation table as a pair \((S, E)\), leaving the language \( L \) implicit.

Given an observation table \((S, E)\) one can construct a deterministic automaton \( M(S, E) = (Q, q_0, \delta, F) \) where

- \( Q = \{row(s) \mid s \in S\} \) is a finite set of states;
- \( F = \{row(s) \mid s \in S, row(s)(e) = 1\} \subseteq Q \) is the set of final states;
- \( q_0 = row(\epsilon) \) is the initial state;
- \( \delta : Q \times A \rightarrow Q \) is the transition function given by \( \delta(row(s), a) = row(sa) \).

For this to be well-defined, we need to have \( e \in S \) (for the initial state) and \( e \in E \) (for final states), and for the transition function there are two crucial properties of the table that need to hold: closedness and consistency. An observation table \((S, E)\) is closed if for all \( t \in S \cdot A \) there exists an \( s \in S \) such that \( row(t) = row(s) \).

An observation table \((S, E)\) is consistent if, whenever \( s_1 \) and \( s_2 \) are elements of \( S \) such that \( row(s_1) = row(s_2) \), for all \( a \in A \), \( row(s_1a) = row(s_2a) \). Each time the algorithm constructs an automaton, it poses an equivalence query to the teacher. It terminates when the answer is yes, otherwise it extends the table with the counterexample provided.

2.1 Simple example of execution

Angluin’s algorithm is displayed in Figure 1. Throughout this section, we will consider the language(s)

\[ L_n = \{ww \mid w \in A^*, |w| = n\} \]

If the alphabet \( A \) is finite then \( L_n \) is regular for any \( n \in \mathbb{N} \), and there is a finite DFA accepting it.

The language \( L_1 = \{aa, bb\} \) looks trivial, but the minimal DFA recognizing it has as many as \( 5 \) states. Angluin’s algorithm will terminate in (at most) \( 5 \) steps. We illustrate some relevant ones.

**Step 1.** We start from \( S, E = \{\epsilon\} \), and we fill the entries of the table below by asking membership queries for \( e, a \) and \( b \). The table is closed and consistent, so we construct the hypothesis \( A_1 \).

\[
\begin{align*}
E & \quad S \subseteq A^* \\
\epsilon & \quad 0 \\
a & \quad 0 \\
aa & \quad 0 \\
b & \quad 0 \\
\end{align*}
\]

The Teacher replies no and gives the counterexample \( aa \), which is in \( L_1 \) but it is not accepted by \( A_1 \). Therefore, line 12 of the algorithm is triggered and we set \( S \leftarrow S \cup \{a, aa\} \).

**Step 2.** The table becomes the one on the left below. It is closed, but not consistent: rows \( e \) and \( aa \) are identical, but appending \( a \) leads to different rows, as depicted. Therefore, line 9 is triggered and an extra column \( a \), highlighted in red, is added. The new table is closed and consistent and a new hypothesis \( A_2 \) is constructed.

\[
\begin{align*}
E & \quad S \subseteq A^* \\
\epsilon & \quad 0 \\
a & \quad 0 \\
aa & \quad 0 \\
ab & \quad 0 \\
\end{align*}
\]

This table indicates that \( L \) contains at least \( aa \) and definitely does not contain the words \( e, a, b, ba, baa, aaa \). Since \( row \) is fully determined by the language \( L \), we will from now on refer to an observation table as a pair \((S, E)\), leaving the language \( L \) implicit.

Given an observation table \((S, E)\) one can construct a deterministic automaton \( M(S, E) = (Q, q_0, \delta, F) \) where

- \( Q = \{row(s) \mid s \in S\} \) is a finite set of states;
- \( F = \{row(s) \mid s \in S, row(s)(e) = 1\} \subseteq Q \) is the set of final states;
- \( q_0 = row(\epsilon) \) is the initial state;
- \( \delta : Q \times A \rightarrow Q \) is the transition function given by \( \delta(row(s), a) = row(sa) \).

For this to be well-defined, we need to have \( e \in S \) (for the initial state) and \( e \in E \) (for final states), and for the transition function there are two crucial properties of the table that need to hold: closedness and consistency. An observation table \((S, E)\) is closed if for all \( t \in S \cdot A \) there exists an \( s \in S \) such that \( row(t) = row(s) \).

An observation table \((S, E)\) is consistent if, whenever \( s_1 \) and \( s_2 \) are elements of \( S \) such that \( row(s_1) = row(s_2) \), for all \( a \in A \), \( row(s_1a) = row(s_2a) \). Each time the algorithm constructs an automaton, it poses an equivalence query to the teacher. It terminates when the answer is yes, otherwise it extends the table with the counterexample provided.

2.1 Simple example of execution

Angluin’s algorithm is displayed in Figure 1. Throughout this section, we will consider the language(s)

\[ L_n = \{ww \mid w \in A^*, |w| = n\} \]

If the alphabet \( A \) is finite then \( L_n \) is regular for any \( n \in \mathbb{N} \), and there is a finite DFA accepting it.

The language \( L_1 = \{aa, bb\} \) looks trivial, but the minimal DFA recognizing it has as many as \( 5 \) states. Angluin’s algorithm will terminate in (at most) \( 5 \) steps. We illustrate some relevant ones.

**Step 1.** We start from \( S, E = \{\epsilon\} \), and we fill the entries of the table below by asking membership queries for \( e, a \) and \( b \). The table is closed and consistent, so we construct the hypothesis \( A_1 \).

\[
\begin{align*}
E & \quad S \subseteq A^* \\
\epsilon & \quad 0 \\
a & \quad 0 \\
aa & \quad 0 \\
b & \quad 0 \\
\end{align*}
\]

The Teacher replies no and gives the counterexample \( aa \), which is in \( L_1 \) but it is not accepted by \( A_1 \). Therefore, line 12 of the algorithm is triggered and we set \( S \leftarrow S \cup \{a, aa\} \).

**Step 2.** The table becomes the one on the left below. It is closed, but not consistent: rows \( e \) and \( aa \) are identical, but appending \( a \) leads to different rows, as depicted. Therefore, line 9 is triggered and an extra column \( a \), highlighted in red, is added. The new table is closed and consistent and a new hypothesis \( A_2 \) is constructed.

\[
\begin{align*}
E & \quad S \subseteq A^* \\
\epsilon & \quad 0 \\
a & \quad 0 \\
aa & \quad 0 \\
ab & \quad 0 \\
\end{align*}
\]
The Teacher replies no and gives the counterexample \( bb \), which should be accepted by \( A_2 \) but it is not. Therefore we put \( S \leftarrow S \cup \{ b, bb \} \).

**Step 3.** The new table is the one on the left. It is closed, but \( e \) and \( b \) violate consistency, when \( b \) is appended. Therefore we add the column \( b \) and we get the table on the right, which is closed and consistent. The new hypothesis is \( A_3 \).

\[
\begin{array}{|c|c|c|}
\hline
\varepsilon & a & b \\
\hline
\varepsilon & 0 & 0 & 0 \\
\hline
\varepsilon & 0 & 1 & 0 \\
\hline
a & 0 & 0 & 0 \\
\hline
a & 1 & 1 & 0 \\
\hline
b & 0 & 0 & 0 \\
\hline
b & 0 & 1 & 0 \\
\hline
ab & 0 & 0 & 0 \\
\hline
aaa & 0 & 0 & 0 \\
\hline
aab & 0 & 0 & 0 \\
\hline
ba & 0 & 0 & 0 \\
\hline
bba & 0 & 0 & 0 \\
\hline
bba & 0 & 0 & 0 \\
\hline
\end{array}
\]

\( A_3 = \)

The Teacher replies no and provides the counterexample \( babb \), so \( S \leftarrow S \cup \{ ba, bab \} \).

**Step 4.** One more step brings us to the correct hypothesis \( A_4 \) (details are omitted).

\[
A_4 = \]

2.2 Learning nominal languages

Consider now an infinite alphabet \( A = \{ a, b, c, d, \ldots \} \). The language \( L_3 \) becomes \( \{ aa, bb, cc, dd, \ldots \} \). Classical theory of finite automata does not apply to this kind of languages, but one may draw an infinite deterministic automaton that recognizes \( L_3 \) in the standard sense:

\[
A_5 = \]

where \( \rightarrow \) and \( \overrightarrow{\not= a} \) stand for the infinitely-many transitions labelled by elements of \( A \) and \( A \setminus \{ a \} \), respectively. This automaton is infinite, but it can be finitely presented in a variety of ways, for example:

\[
\forall x \in A
\]

One can formalize the quantifier notation above (or indeed the “dots” notation above that) in several ways. A popular solution is to consider finite register automata \([18,25]\), i.e., finite automata equipped with a finite number of registers where alphabet letters can be stored and later compared for equality. Our language \( L_3 \) is recognized by a simple automaton with four states and one register. The problem of learning registered automata has been successfully attacked before \([21]\).

In this paper, however, we will consider nominal automata \([9]\) instead. These automata ostensibly have infinitely many states, but the set of states can be finitely presented in a way open to effective manipulation. More specifically, in a nominal automaton the set of states is subject to an action of permutations of a set \( \mathcal{A} \) of atoms, and it is finite up to that action. For example, the set of states of \( A_5 \) is:

\[
\{ q_0, q_3, q_1 \} \cup \{ q_a \mid a \in A \}
\]

and it is equipped with a canonical action of permutations \( \pi: \mathcal{A} \rightarrow \mathcal{A} \) that maps every \( q_a \) to \( q_{\pi(a)} \), and leaves \( q_0, q_3 \) and \( q_1 \) fixed. Technically speaking, the set of states has four orbits (one infinite orbit and three fixed points) of the action of the group of permutations of \( \mathcal{A} \). Moreover, it is required that in a nominal automaton the transition relation is equivariant, i.e., closed under the action of permutations. The automaton \( A_5 \) has this property: for example, it has a transition \( q_0 \xrightarrow{a} q_3 \), and for any \( \pi: \mathcal{A} \rightarrow \mathcal{A} \) there is also a transition \( \pi(q_0) = q_{\pi(a)} = q_{\pi(3)} \).

Nominal automata with finitely many orbits of states are equi-expressive with finite register automata \([9]\), but they have an important theoretical advantage: they are a direct reformulation of the classical notion of finite automaton, where one replaces finite sets with orbit-finite sets and functions (or relations) with equivariant ones. A research programme advocated in \([8,9]\) is to transport various computation models, algorithms and theorems along this correspondence. This can often be done with remarkable accuracy, and our paper is a witness to this. Indeed, as we shall see, nominal automata can be learned with an algorithm that is almost a verbatim copy of the classical Angluin’s one.

Indeed, considering Angluin’s algorithm to our new language \( L_1 \). The key idea is to change the basic data structure: our observation table \( (S, E) \) will be such that \( S \) and \( E \) are equi-invariant subsets of \( A' \), i.e., they are closed under the canonical action of atom permutations. In general, such a table has infinitely many rows and columns, so the following aspects of the algorithm seem problematic:

- **line 3** closedness and consistency tests range over infinite sets;
- **line 5** and **line 8** finding witnesses for closedness or consistency violations potentially require checking all infinitely many rows;
- **line 12** every counterexample \( t \) has only finitely many prefixes, so it is not clear how one would construct an infinite set \( S \) in finite time. However, an infinite \( S \) is necessary for the algorithm to ever succeed, because no finite automaton recognizes \( L_1 \).

At this stage, we need to observe that due to equivariance of \( S, E \) and \( L_1 \), the following crucial properties hold:

- (P1) the sets \( S, S \cdot A \) and \( E \) admit a finite representation up to permutations;
- (P2) the function \( row \) is such that \( row(\pi(s))(\pi(e)) = row(s)(e) \), for all \( s \in S \) and \( e \in E \), so the observation table admits a finite symbolic representation.

Intuitively, checking closedness and consistency, and finding a witness for their violations, can be done effectively on the representations up to permutations (P1). This is sound, as (row) is invariant w.r.t. permutations (P2).

We now illustrate these points through a few steps of the algorithm for \( L_1 \).

**Step 1:** We start from \( S, E = \{ e \} \). We have \( S \cdot A = A \), which is infinite but admits a finite representation. In fact, for any \( a \in A \), we have \( A = \{ \pi(a) \mid \pi \text{ is a permutation} \} \). Then, by (P2), \( row(\pi(a))(e) = row(a)(e) = 0 \), for all \( \pi \), so the first table can be written as:
We found a “symbolic” witness we extend words of length 2 with two repeated letters are accepted. Therefore (row 1)

The lower part stands for elements of nominal setting. However, there are challenges in the extension that are exponentially more succinct than DFAs. This is true also in the (row 2)

how to extend the algorithm to the nominal setting can be done in a systematic way. We will show original development, exploring extensions of other variations of (row 3)

Since our extension of Angluin’s hypothesis automaton, shown earlier in (row 4)

2.3 Generalization to non-deterministic automata

Since our extension of Angluin’s L* algorithm stays close to her original development, exploring extensions of other variations of L* to the nominal setting can be done in a systematic way. We will show how to extend the algorithm NL* for learning NFAs by Bollig et al. (row 5). This has practical implications: it is well-known that NFAs are exponentially more succinct than DFAs. This is true also in the nominal setting. However, there are challenges in the extension that require particular care.

- Nominal NFAs are strictly more expressive than nominal DFAs. We will show that the nominal version of NL* terminates for all nominal NFAs that have a corresponding nominal DFA and, more surprisingly, that it is capable of learning some languages that are not accepted by nominal DFAs.
- Language equivalence of nominal NFAs is undecidable. This does not affect the correctness proof, as it assumes a teacher which is able to answer equivalence queries accurately. For our implementation, we will describe heuristics that produce correct results in many cases.

For the learning algorithm the power of non-determinism means that we can make some shortcuts during learning: if we want to make the table closed, we were previously required to find an equivalent row in the upper part; now we may find a sum of rows which, together, are equivalent to an existing row. This means that in some cases fewer rows will be added for closedness.

### 3. Preliminaries

We recall the notions of nominal sets, nominal automata and nominal regular languages (see [9] for a detailed account).

Let $\mathbb{A}$ be a countable set and let $\text{Perm}(\mathbb{A})$ be the set of permutations on $\mathbb{A}$, i.e., the bijective functions $\pi: \mathbb{A} \to \mathbb{A}$. Permutations form a group where the identity permutation $id$ is the unit element, inverse is functional inverse and multiplication is function composition.

A nominal set $\mathcal{A}$ is a set $X$ plus a function $*: \text{Perm}(X) \times X \to X$, interpreting permutations over $X$. Such function must be a group action of $\text{Perm}(X)$, i.e., it must satisfy $id \cdot x = x$ and $\pi \cdot (\pi' \cdot x) = (\pi \circ \pi') \cdot x$. We say that a finite $A \subseteq \mathcal{A}$ supports $x \in X$ whenever, for all $\pi$ acting as the identity on $A$, we have $\pi \cdot x = x$. In other words, permutations that only move elements outside $A$ do not affect $x$. The support of $x \in X$, denoted $\text{supp}(x)$, is the smallest finite set supporting $x$. We require nominal sets to have finite support, meaning that $\text{supp}(x)$ exists for all $x \in X$.

The orbit $\text{orb}(x)$ of $x \in X$ is the set of elements in $X$ reachable from $x$ via permutations, explicitly

$$\text{orb}(x) = \{ \pi \cdot x \mid \pi \in \text{Perm}(X) \}$$

Then $X$ is orbit-finite whenever it is a union of finitely many orbits. Given a nominal set $X$, a subset $Y \subseteq X$ is equivariant if it is preserved by permutations, i.e., $\pi \cdot y \in Y$, for all $y \in Y$. In other words, $Y$ is the union of orbits of $X$. This definition extends to the notion of an equivariant relation $R \subseteq X \times Y$, by setting $\pi \cdot (x, y) = (\pi \cdot x, \pi \cdot y)$, for $(x, y) \in R$; similarly for relations of greater arity. The dimension of nominal set $X$ is the maximal size of $\text{supp}(x)$, for any $x \in X$. Every orbit-finite set has finite dimension.

We define $\mathcal{A}^{(k)} = \{(a_1, \ldots, a_k) \mid a_i \neq a_j, \text{ for } i \neq j\}$. For every single-orbit nominal set $X$ with dimension $k$, there is a surjective equivariant map $f_X: \mathcal{A}^{(k)} \to X$.

This map can be used to get an upper bound for the number of orbits of $X_1 \times \cdots \times X_n$, for $X_i$ a nominal set with $l_i$ orbits and dimension $k_i$. Suppose $O_i$ is an orbit of $X_i$. Then we have a surjection

$$\mathcal{A}^{(k_1)} \times \cdots \times \mathcal{A}^{(k_n)} \xrightarrow{f_{O_1} \times \cdots \times f_{O_n}} O_1 \times \cdots \times O_n$$

stipulating that the codomain cannot have more orbits than the domain. Let $f_x(\{k_i\})$ denote the number of orbits of $\mathcal{A}^{(k_1)} \times \cdots \times \mathcal{A}^{(k_n)}$, for any finite sequence of natural numbers $\{k_i\}$. We can form at most $l_1 l_2 \cdots l_n$ tuples of the form $O_1 \times \cdots \times O_n$, so $X_1 \times \cdots \times X_n$ has at most $f_x(k_1, \ldots, k_n)$ orbits.

For $X$ single-orbit, the local symmetries are defined by the group

$$\{ g \in S_k \mid f(x_1, \ldots, x_k) = f(x_{g(1)}, \ldots, x_{g(k)}) \text{ for all } x_i \in X \},$$

Paper accepted at POPL 2017 with DOI http://dx.doi.org/10.1145/3009837.3009879 4 2016/11/9
where $k$ is the dimension of $X$ and $S_k$ is the symmetric group of permutations over $k$ distinct elements.

NFAs on sets have a finite state space. We can define nominal NFAs, with the requirement that the state space is orbit-finite and the transition relation is equivariant. A nominal NFA is a tuple $(Q, A, Q_0, F, \delta)$, where:

- $Q$ is an orbit-finite nominal set of states;
- $A$ is an orbit-finite nominal alphabet;
- $Q_0, F \subseteq Q$ are equivariant subsets of initial and final states;
- $\delta \subseteq Q \times A \times Q$ is an equivariant transition relation.

A nominal DFA is a special case of nominal NFA where $Q_0 = \{q_0\}$ and the transition relation is an equivariant function $\delta : Q \times A \to Q$. Equivariance here can be rephrased as requiring $\delta(\pi \cdot q, \pi \cdot a) = \pi \cdot \delta(q, a)$. In most examples we take the alphabet to be $A = \mathbb{Q}$, but it can be any orbit-finite nominal set. For instance, $A = \text{Act} \times \mathbb{Q}$, where $\text{Act}$ is a finite set of actions, represents actions $\text{act}(x)$ with one parameter $x \in \mathbb{Q}$ (actions with arity $n$ can be represented via $n$-fold products of $\mathbb{Q}$).

A language $L$ is nominal regular if it is recognized by a nominal DFA. The theory of nominal regular languages recasts the classical one using nominal concepts. A nominal Myhill-Nerode-style syntactic congruence is defined: $w, w' \in A^*$ are equivalent w.r.t. $L$, written $w \equiv L w'$, whenever

$$w v \in L \iff w' v \in L$$

for all $v \in A^*$. This relation is equivariant and the set of equivalence classes $[w]_L$ is a nominal set.

**Theorem 1** (Myhill-Nerode theorem for nominal sets). Let $L$ be a regular nominal language. The following conditions are equivalent:

1. the set of equivalence classes of $\equiv_L$ is orbit-finite;
2. $L$ is recognized by a nominal DFA.

Unlike what happens for ordinary regular languages, nominal NFAs and nominal DFAs are not equi-expressive. Here is an example of a language accepted by a nominal NFA, but not by a nominal DFA:

$$L_{\mathbb{Q}} = \{a_1 \ldots a_n \mid a_i = a_j, \text{for some } i < j \in \{1, \ldots, n\}\}$$

In the theory of nominal regular languages, several problems are decidable: language inclusion and minimality test for nominal DFAs. Moreover, orbit-finite nominal sets can be finitely-represented, and so can be manipulated by algorithms. This is the key idea underpinning our implementation.

### 3.1 Different atom symmetries

An important advantage of nominal set theory as considered in [8] is that it retains most of its properties when the structure of atoms $\mathbb{Q}$ is replaced with an arbitrary infinite relational structure subject to a few model-theoretic assumptions. An example alternative structure of atoms is the total order of rational numbers $(\mathbb{Q}, <)$, with the group of monotone bijections of $\mathbb{Q}$ taking the role of the group of all permutations. The theory of nominal automata remains similar, and an example nominal language over the atoms $(\mathbb{Q}, <)$ is:

$$\{a_1 \ldots a_n \mid a_i \leq a_j, \text{for some } i < j \in \{1, \ldots, n\}\}$$

which is recognized by a nominal DFA over those atoms.

To simplify the presentation, in this paper we concentrate on the “equality atoms” only. Also our implementation of nominal learning algorithms is restricted to equality atoms. However, both the theory and the implementation can be generalized to other atom structures, with the “ordered atoms” $(\mathbb{Q}, <)$ as the simplest other example. We leave the details of this for a future extended version of this paper.

### 4. Angluin’s algorithm for nominal DFAs

In our algorithm, we will assume a teacher as described at the start of Section 2. In particular, the teacher is able to answer membership queries and equivalence queries, now in the setting of nominal languages. We fix a target language $L$, which is assumed to be a nominal regular language.

The learning algorithm for nominal automata, $\nu L^*$, will be very similar to $L^*$ in Figure 1. In fact, we only change the following lines:

1. $S' \leftarrow S \cup \text{orb}(sa)$
2. $E' \leftarrow E \cup \text{orb}(ac)$
3. $S \leftarrow S \cup \text{prefixes}(\text{orb}(l))$

The basic data structure is an observation table $(S, E, T)$ where $S$ and $E$ are orbit-finite subsets of $A^*$ and $T : S \cup \mathbb{Q} \times A \to 2^E$ is an equivariant function defined by $T(s, e) = \text{orb}(se)$ for each $s \in S \cup \mathbb{Q}$ and $e \in E$. Since $T$ is determined by $L$ we omit it from the notation. Let row : $\mathbb{Q} \times S \cdot A \to 2^E$ denote the curried counterpart of $T$. Let $u \leadsto v$ denote the relation $\text{row}(u) = \text{row}(v)$.

**Definition 1.** The table is called closed if for each $t \in S \cdot A$ there is a $s \in S$ with $t \sim s$. The table is called consistent if for each pair $s_1, s_2 \in S$ with $s_1 \sim s_2$ we have $s_1 \sim s_2$ for all $a \in A$.

The above definitions agree with the abstract definitions given in [24] and we may use some of their results implicitly. The intuition behind the definitions is as follows. Closedness assures us that for each state we have a successor state for each input. Consistency assures us that each state has at most one successor for each input. Together it allows us to construct a well-defined minimal automaton from the observations in the table.

The algorithm starts with a trivial observation table and tries to make it closed and consistent by adding orbits of rows and columns, filling the table via membership queries. When the table is closed and consistent it constructs a hypothesis automaton and poses an equivalence query.

The pseudocode for the nominal version is the same as listed in Figure 1 modulo the changes displayed in [2]. However, we have to take care to ensure that all manipulations and tests on the (possibly) infinite sets $S, E$ and $A$ terminate in finite time. We refer to [8] and [26] for the full details on how to represent these structures and provide a brief sketch here. The sets $S, E, A$ and $S \cdot A$ can be represented by choosing a representative for each orbit. The function $T$ in turn can be represented by cells $T_{i, j} : \text{orb}(s_i) \times \text{orb}(e_j) \to 2$ for each representative $s_i$ and $e_j$. Note, however, that the product of two orbits may consist of several orbits, so that $T_{i, j}$ is not a single boolean value. Each cell is still orbit-finite and can be filled with only finitely many membership queries. Similarly the curried function $\text{row}$ can be represented by a finite structure.

To check whether the table is closed, we observe that if we have a corresponding row $s \in S$ for some $t \in S \cdot A$, this holds for any permutation of $t$. Hence it is enough to check the following: for all representatives $t \in S \cdot A$ there is a representative $s \in S$ with $\text{row}(t) = \pi \cdot \text{row}(s)$ for some permutation $\pi$. Note that we only have to consider finitely many permutations, since the support is finite and so we can decide this property. Furthermore if the property does not hold, we immediately find a witness represented by $t$.

Consistency is a bit more complicated, but it is enough to consider the set of inconsistencies, $\{(s_1, s_2, a, e) \mid \text{row}(s_1) = \text{row}(s_2) \land \text{row}(s_1)(e) \neq \text{row}(s_2)(e)\}$. It is an equivariant subset of $S \times S \times A \times E$ and so it is orbit-finite. Hence we can decide emptiness and obtain representatives if it is non-empty.

Constructing the hypothesis happens in the same way as before (Section 2), where we note the state space is orbit-finite since it is a quotient of $S$. Moreover the function $\text{row}$ is equivariant, so all structure $(Q_0, F$ and $\delta)$ is equivariant as well.

Paper accepted at POPL 2017 with DOI http://dx.doi.org/10.1145/3009837.3009879 2016/11/9
The representation given above is not the only way to represent nominal sets. For example, first-order definable sets can be used as well \[\mathcal{L}\]. From now on we assume to have set theoretic primitives so that each line in Figure 1 is well defined.

The representation given above is not the only way to represent nominal sets. For example, first-order definable sets can be used as well \[\mathcal{L}\]. From now on we assume to have set theoretic primitives so that each line in Figure 1 is well defined.

4.1 Correctness

To prove correctness we only have to prove that the algorithm terminates, that is, only finitely many hypotheses will be produced. Correctness follows trivially from termination since the last step of the algorithm is an equivalence query to the teacher inquiring whether an hypothesis automaton accepts the target language. We start out by listing some facts about observation tables.

Lemma 1. The relation \(\sim\) is an equivariant equivalence relation. Furthermore, for all \(u, v \in S\) we have that \(u \equiv \sim v\) implies \(u \sim v\).

Lemma 1 implies that at any stage of the algorithm the number of orbits of \(S/\sim\) does not exceed the number of orbits of the minimal acceptor with state space \(A'/\equiv \sim\) (recall that \(\equiv \sim\) is the nominal Myhill-Nerode equivalence relation). Moreover, the following lemma shows that the dimension of the state space never extends the dimension of the minimal acceptor. Recall that the dimension is the maximal size of the support of any state, which is different than the number of orbits.

Lemma 2. We have \(\text{supp}([u]_\sim) \subseteq \text{supp}([u]_{\equiv \sim}) \subseteq \text{supp}(u)\) for all \(u \in S\).

Lemma 3. The automaton constructed from a closed and consistent table is minimal.

Proof. Follows from the categorical perspective given in [24].

We note that the constructed automaton is consistent with the table (we use that the set \(S\) is prefix-closed and \(E\) is suffix-closed). The following lemma shows that there are no strictly “smaller” automata consistent with the table. So the automaton is not just minimal, it is minimal w.r.t. the table.

Lemma 4. Let \(H\) be the automaton associated with a closed and consistent table \((S, E)\). If \(M'\) is an automaton consistent with \((S, E)\) (meaning that \(s \in L(M') \iff s \in L(H)\) for all \(s \in S\cup S\cdot A\) and \(e \in E\)) and \(M'\) has at most as many orbits as \(H\), then there is a surjective map \(f : Q_{M'} \to Q_H\). If moreover

- \(M'\)’s dimension is bounded by the dimension of \(H\), i.e. \(\text{supp}(m) \subseteq \text{supp}(f(m))\) for all \(Q_{M'}\), and
- \(M'\) has no fewer local symmetries than \(H\), i.e. \(\pi \cdot f(m) = f(m)\) implies \(\pi \cdot m = m\) for all \(m \in Q_{M'}\),

then \(f\) defines an isomorphism \(M' \cong H\) of nominal DFAs.

Proof. (All maps in this proof are equivariant.) Define a map \(\text{row}' : Q_{M'} \to 2^k\) by restricting the language map \(Q_{M'} \to 2^A\) to \(E\). First, observe that \(\text{row}'(\delta (q_0^*, s)) = \text{row}(s)\) for all \(s \in S\cup S\cdot A\), since \(e \in E\) and \(M'\) is consistent with the table. Second, we have \(\{\text{row}'(\delta (q_0^*, s)) | s \in S\} \subseteq \{\text{row}'(q) | q \in M'\}\).

Let \(n\) be the number of orbits of \(H\). The former set has \(n\) orbits by the first observation, the latter set has at most \(n\) orbits by assumption. We conclude that the two sets (both being equivariant) must be equal. That means that for each \(q \in M'\) there is a \(s \in S\) such that \(\text{row}'(q) = \text{row}(s)\). We see that \(\text{row}' : M' \to \{\text{row}'(\delta (q_0^*, s)) | s \in S\}\) is a surjective map. Since a surjective map cannot increase the dimensions of orbits and the dimensions of \(M'\) are bounded, we note that the dimensions of the orbits in \(H\) and \(M'\) have to agree. Similarly, surjective maps preserve local symmetries. This map must hence be an isomorphism of nominal sets. Note that \(\text{row}'(q) = \text{row}'(\delta (q_0^*, s))\) implies \(q = \delta (q_0^*, s)\).

It remains to prove that it respects the automaton structures. It preserves the initial state: \(\text{row}'(q_0^*) = \text{row}(\delta (q_0^*, e)) = \text{row}(e)\). Now let \(q \in M'\) be a state and \(s \in S\) such that \(\text{row}'(q) = \text{row}(s)\). It preserves final states: \(q \in F' \iff \text{row}'(q)(e) = 1 \iff \text{row}(s)(e) = 1\). Finally, it preserves the transition structure:

\[
\text{row}'(\delta'(q, a)) = \text{row}'(\delta'(q_0^*, s), a) = \text{row}'(\delta'(q_0^*, sa)) = \text{row}(sa) = \delta(\text{row}(s), a)
\]

The above proof is an adaptation of Angluin’s proof for automata over sets. We will now prove termination of the algorithm by proving that all steps are productive.

Theorem 2. The algorithm terminates and is hence correct.

Proof. Provided that the if-statements and set operations terminate, we are left proving that the algorithm adds (orbits of) rows and columns only finitely often. We start by proving that a table can be made closed and consistent in finite time.

If the table is not closed, we find a row \(s_1 \in S\cdot A\) such that \(\text{row}(s_1) \neq \text{row}(s)\) for all \(s \in S\). The algorithm then adds the orbit containing \(s_1\) to \(S\). Since \(s_1\) was nonequivalent to all rows, we find that \(S \cup \text{orb}(t)/\sim\) has strictly more orbits than \(S/\sim\). Since orbits of \(S/\sim\) cannot be more than those of \(A'/\equiv \sim\), this happens finitely often.

Columns are added in case of an inconsistency. Here the algorithm finds two elements \(s_1, s_2 \in S\) with \(\text{row}(s_1) = \text{row}(s_2)\) but \(\text{row}(s_1 a) \neq \text{row}(s_2 a)\) for some \(a \in A\) and \(e \in E\). Adding \(ae\) to \(E\) will ensure that \(\text{row}(s_1) \neq \text{row}(s_2)\) (\(\text{row}\) is the function belonging to the updated observation table). If the two elements \(\text{row}(s_1), \text{row}(s_2)\) are in different orbits, the number of orbits is increased. If they are not in the same orbit, we have \(\text{row}(s_2) = \pi \cdot \text{row}(s_1)\) for some permutation \(\pi\). Using \(\text{row}(s_1) = \text{row}(s_2)\) and \(\text{row}(s_1) \neq \text{row}(s_2)\) we have:

\[
\text{row}(s_1) = \pi \cdot \text{row}(s_1) \Rightarrow \text{row}(s_1) \neq \pi \cdot \text{row}(s_1)
\]

Consider all such \(\pi\) and suppose there is a \(\pi\) and \(x \in \text{supp}(\text{row}(s_1))\) such that \(\pi \cdot x \notin \text{supp}(\text{row}(s_1))\). Then we find that \(\pi \cdot x \in \text{supp}(\text{row}(s_1))\), and so the support of the row has grown. By Lemma 2 this happens finitely often. Suppose such \(\pi\) and \(x\) do not exist, then we consider the finite group \(R = \{\rho \mid \text{supp}(\rho(s_1)) = \rho \cdot \text{row}(s_1)\}\). We see that \(\{\rho \mid \text{supp}(\rho(s_1)) = \rho \cdot \text{row}(s_1)\}\) is a proper subgroup of \(R\). So, adding a column in this case decreases the size of the group \(R\), which can happen only finitely often. In this case a local symmetry is removed.

In short, the algorithm will succeed in producing a hypothesis in each round. It remains to prove that it needs only finitely many equivalence queries.

Let \((S, E)\) be the closed and consistent table and \(H\) its corresponding hypothesis. If it is incorrect a second hypothesis \(H'\) will be constructed which is consistent with the old table \((S, E)\). The two hypotheses are nonequivalent, as \(H'\) will handle the counter example correctly and \(H\) does not. Therefore, \(H'\) will have at least one orbit more, one local symmetry less, or one orbit will have strictly bigger dimension (Lemma 4), all of which can only happen finitely often.

We remark that all the lemmas and proofs as above are close to the original ones of Angluin. However, two things are crucially different. First, adding a column does not always increase the number of (orbits of) states. It can happen that by adding a column a bigger support is found or that a local symmetry is broken. Second, the new hypothesis does not necessarily have more states, again it might have bigger dimensions or less local symmetries.

From the proof Theorem 2 we observe moreover that the way we handle counterexamples is not crucial. Any other method which
ensures a non-equivalent hypothesis will work. In particular our algorithm is easily adapted to include optimizations such as the ones in [37] and [31], where counterexamples are added as columns.

4.2 Example

Consider the target automaton in Figure 2 and an observation table $T_1$ at some stage during the algorithm. We remind the reader that the table is represented in a symbolic way: the sequences in the rows and columns stand for whole orbits and the cells denote functions from the product of the orbits to $2$. Since the cells can consist of multiple orbits, where each orbit is allowed to have a different value, we use a formula to specify which orbits have a local symmetry being equal or different from $a$, similarly for $row(ab)(a')$.

The table $T_2$ is still not consistent as we see that $row(ab)\neq row(ab)$ but $row(ab)(c) = 1$ and $row(ab)(c) = 0$. Hence the algorithm adds the columns $orb(bc)$, obtaining table $T_3$. We note that in this case, no new orbits are added and no support has grown. In fact, the only change here is that the local symmetry between $row(ab)$ and $row(ab)$ is removed. This last table, $T_3$, is closed and consistent and will produce the correct hypothesis.

4.3 Query Complexity

In this section, we will analyse the number of queries made by the algorithm in the worst case. Let $M$ be the minimal target automaton with $n$ orbits and of dimension $k$. We will use log in base two.

Lemma 5. The number of equivalence queries $E_{n,k}$ is $O(nk\log k)$.

Proof. By Lemma 4, each hypothesis will be either 1) bigger in the number of orbits, which is bounded by $n$, or 2) bigger in the dimension of an orbit, which is bounded by $k$ or 3) smaller in local symmetries of an orbit. For the last part we want to know how long a subgroup series of the permutation group $S_k$ can be. This is bounded by the number of divisors of $k!$, as each subgroup divides the order of the group. We can easily bound the number of divisors of any $m$ by $\log m$ and so one can at take a subgroup at most $k\log k$ times when starting with $S_k$.

Since the hypothesis will grow monotonically in the number of orbits and for each orbit will grow monotonically w.r.t. the remaining two dimensions, the number of equivalence queries is bound by $n+n(k+k\log k)$.

Next we will give a bound for the size of the table.

Lemma 6. The table has at most $n + m E_{n,k}$ orbits in $S$ with sequences of at most length $n + m$, where $m$ is the length of the longest counter example given by the teacher. The table has at most $n(k+k\log k+1)$ orbits in $E$ of at most length $n(k+k\log k+1)$.

Proof. In the termination proof we noted that rows are added at most $n$ times. In addition (all prefixes of) counter examples are added as rows which add another $m E_{n,k}$ rows. Obviously counter examples are of length at most $m$ and are extended at most $n$ times, making the length at most $m+n$ in the worst case.

In columns we note that one of three dimensions approaches a bound similar to the proof of Lemma 5. So at most $n(k+k\log k+1)$ columns are added. Since they are suffix closed, the length is at most $n(k+k\log k+1)$.

Let $p$ and $l$ denote respectively the dimension and the number of orbits of $A$.

Lemma 7. The number of orbits in the lower part of the table, $S \cdot A$, is bounded by $(n + m E_{n,k}) (|f_s(p(n+m),p) + 1) n(k+k\log k+1)$.

Proof. Any sequence in $S$ is of length at most $n+m$, so it contains at most $p(n+m)$ distinct atoms. When we consider $S \cdot A$, the extension can either reuse atoms from those $p(n+m)$, or none at all. Since the extra letter has at most $p$ distinct atoms, the set $\mathcal{A}^{(n+m)} \times \mathcal{A}^{(p)}$ gives a bound $f_s(p(n+m),p)$ for the number of orbits of $O_S \times O_A$, with $O_S$ an orbit of $X$. Multiplying by the number of such ordered pairs, namely $(n + m E_{n,k}) l$, gives a bound for $S \cdot A$.

Let $C_{n,k,m} = (n + m E_{n,k}) (|f_s(p(n+m),p) + 1) n(k+k\log k+1)$ be the maximal number of cells in the table. We note that this number is polynomial in $k, l, m$ and $n$ but not in $p$.

Corollary 1. The number of membership queries is bounded by $C_{n,k,m} f_s(n + m, p(m + k\log k + 1))$.

5. Learning non-deterministic nominal automata

In this section, we introduce a variant of $\nu L^*$, which we call $\nu NL^*$, where the learnt automaton is non-deterministic. It will be based on $NL^*$ [11], an Angluin-style algorithm for learning NFAs. The algorithm is shown in Figure 3. We first illustrate $NL^*$, then we discuss its extension to nominal automata.
We write (line 8). Notice that counterexamples supplied by the teacher are incomparable. A new column is added to distinguish those rows containing of two existing rows, so those rows are actually consistent, then there is a suffix which does not preserve the part. This row is then added to part of the table which is prime, but not contained in the top part. 

Definition 3. 

A table (S, E) with a union operation, allowing for the detection of composed and prime rows.

Definition 2. Let \( (row(s_1) \cup row(s_2))(e) = row(s_1)(e) \lor row(s_2)(e) \) (regarding cells as booleans). This operation induces an ordering between rows: \( row(s_1) \subseteq row(s_2) \) whenever \( row(s_1)(e) = 1 \) implies \( row(s_2)(e) = 1 \), for all \( e \in E \).

A row \( row(s) \) is composed if \( row(s) = row(s_1) \cup \ldots \cup row(s_n) \), for \( row(s_1) \neq row(s) \). Otherwise it is prime. We denote by \( PR^T(S, E) \) the rows in the top part of the table (ranging over \( S \)) which are prime w.r.t. the whole table (not only w.r.t. the top part). We write \( PR(S, E) \) for all the prime rows of \( S, E \).

As in \( L' \), states of hypothesis automata will be rows of \( S, E \) but, as the aim is to construct a minimal RFSA, only prime rows are picked. New notions of closedness and consistency are introduced, to reflect features of RFSA.

Definition 3. A table \( (S, E) \) is:

- RFSA-closed if, for all \( t \in S \cdot A \), \( row(t) = \bigl( row(s) \in PR^T(S, E) \mid row(s) \subseteq row(t) \bigr) \);
- RFSA-consistent if, for all \( s_1, s_2 \in S \) and \( a \in A \), \( row(s_1) \subseteq row(s_2) \) implies \( row(s_1) \subseteq row(s_2) \).

If \( (S, E) \) is not RFSA-closed, then there is a row in the bottom part of the table which is prime, but not contained in the top part. This row is then added to \( S \) (line 5). If \( (S, E) \) is not RFSA-consistent, then there is a suffix which does not preserve the containment of two existing rows, so those rows are actually incomparable. A new column is added to distinguish those rows (line 8). Notice that counterexamples supplied by the teacher are added to columns (line 12). Indeed, in [11] it is shown that treating the counterexamples as in the original \( L' \), namely adding them to rows, does not lead to a terminating algorithm.

Definition 4. Given a RFSA-closed and RFSA-consistent table \( (S, E) \), the conjecture automaton is \( N(S, E) = (Q, Q_0, F, \delta) \), where:

- \( Q = PR^T(S, E) \);
- \( Q_0 = \{ r \in Q \mid r \subseteq row(e) \} \);
- \( F = \{ r \in Q \mid e = \delta(r, a) \} \);
- the transition relation \( \delta \subseteq Q \times A \times Q \) is given by \( \delta(r, a) = \{ r \in Q \mid r \subseteq row(sa) \} \).

As observed in [11], \( N(S, E) \) is not necessarily a RFSA, but it is a canonical RFSA if it is consistent with \( (S, E) \). If the algorithm terminates, then \( N(S, E) \) must be consistent with \( (S, E) \), which ensures correctness. The termination argument is more involved than \( L' \), but still it relies on the minimal DFA.

Developing an algorithm to learn nominal NFAs is not an obvious extension of \( L' \): non-deterministic nominal languages strictly contain nominal regular languages, so it is not clear what the developed algorithm should be able to learn. To deal with this, we introduce a nominal notion of RFSA. They are a proper subclass of nominal NFAs, because they recognize nominal regular languages. Nonetheless, they are more succinct than nominal DFAs.

5.1 Nominal residual finite-state automata

Let \( L \) be a nominal regular language and let \( u \) be a finite string. The derivative of \( L \) w.r.t. \( u \) is \( u^{-1}L = \{ v \in A^* \mid uv \in L \} \). A set \( L' \subseteq A^* \) is a residual of \( L \) if there is \( u \) with \( L' = u^{-1}L \). Note that a residual might not be equivalent, but it does have a finite support. We write \( R(L) \) for the set of residuals of \( L \). Residuals form an orbit-finite nominal set: they are in bijection with the state-space of the minimal nominal DFA for \( L \).

A nominal residual finite-state automaton for \( L \) is a nominal NFA whose states are subsets of such minimal automaton. Given a state \( q \) of an automaton, we write \( L(q) \) for the set of words leading from \( q \) to a set of states containing a final one.

Definition 5. A nominal residual finite-state automaton (nominal RFSA) is a nominal NFA \( \mathcal{A} \) such that \( L(q) \in R(L(\mathcal{A})) \), for all \( q \in Q_\mathcal{A} \).

Intuitively, all states of a nominal RSFA recognize residuals, but not all residuals are recognized by a single state: there may be a residual \( L' \) and a set of states \( Q' \) such that \( L' = \bigcup_{q \in Q'} L(q) \), but no state \( q' \) is such that \( L(q') = L' \). A residual \( L' \) is called composed if it is equal to the union of the components it strictly contains, explicitly

\[ L' = \bigcup_{q' \in Q'} (L(q') \mid L(q') \neq L') \:
\]
otherwise it is called prime. In an ordinary RFSA, composed residuals have finitely-many components. This is not the case in a nominal RFSA. However, the set of components of \( L' \) always has a finite support, namely \( \text{supp}(L') \).

The set of prime residuals \( PR(L) \) is an orbit-finite nominal set, and can be used to define a canonical nominal RFSA for \( L \), which has the minimal number of states and the maximal number of transitions. This can be regarded as obtained from the minimal nominal DFA by removing composed states and adding all initial states and transitions that do not change the recognized language. This automaton is necessarily unique.

Lemma 8. Let the canonical nominal RFSA of \( L \) be \( (Q, Q_0, F, \delta) \) such that:

- \( Q = PR(L) \);
- \( Q_0 = \{ L' \in Q \mid L' \subseteq L \} \);
- \( F = \{ L' \in Q \mid \epsilon \in L' \} \);
- \( \delta(\{1\}, a) = \{ L_2 \in Q \mid L_2 \subseteq a^{-1}L_1 \} \).

It is a well-defined nominal NFA accepting \( L \).
5.2 νRL*

Our nominal version of νL* again makes use of an observation table (S, E) where S and E are equivariant subsets of A* and row is an equivariant function. As in the basic algorithm, we equip (S, E) with a union operation ∪ and row containment relation ⊆, defined as in Definition 2. It is immediate to verify that ∪ and ⊆ are equivariant.

Our algorithm is a simple modification of the algorithm in Figure 1 where a few lines are replaced:

\begin{align*}
6' & S \leftarrow S \cup \text{orb}(sa) \\
9' & E \leftarrow E \cup \text{orb}(ae) \\
12' & E \leftarrow E \cup \text{suffixes}(\text{orb}(t))
\end{align*}

Switching to nominal sets, several decidability issues arise. The most critical one is that rows may be the union of infinitely many component rows, as happens for residuals of nominal languages, so finding all such components can be challenging. We adapt the notion of composed to rows: \( \text{row}(t) \) is composed whenever

\[
\text{row}(t) = \bigsqcup \{ \text{row}(s) \mid \text{row}(s) \subseteq \text{row}(t) \}.
\]

where \( \subseteq \) is strict row inclusion; otherwise \( \text{row}(t) \) is prime.

We now check that relevant parts of our algorithm terminate.

**Row containment check.** The basic containment check row(s) \( \subseteq \) row(t) is decidable, as row(s) and row(t) are supported by the finite supports of s and t respectively.

**Line 3** RFSA-closedness and RFSA-consistency checks. We first show that prime rows form orbit-finite nominal sets.

**Lemma 9.** \( PR(S, E), PR^\top(S, E) \) and \( PR(S, E) \setminus PR^\top(S, E) \) are orbit-finite nominal sets.

Consider now RFSA-closedness. It requires computing the set \( C(\text{row}(t)) \) of components of row(t) contained in \( PR^\top(S, E) \) (possibly including \( \text{row}(t) \)). This may not be equivariant under permutations Perm(\( \tilde{\kappa} \)), but it is if we pick a subgroup.

**Lemma 10.** The set \( C(\text{row}(t)) \) has the following properties:

1. \( \text{supp}(C(\text{row}(t))) \subseteq \text{supp}(\text{row}(t)) \).
2. It is equivariant and orbit-finite under the action of the group \( G \), which fixes supp(\( \text{row}(t) \))

\[
G = \{ \pi \in \text{Perm}(\kappa) \mid \pi|_{\text{supp}(\text{row}(t))} = \text{id} \}
\]

of permutations fixing \( \text{supp}(\text{row}(t)) \).

We established that \( C(\text{row}(t)) \) can be effectively computed, and the same holds for \( \bigsqcup C(\text{row}(t)) \). In fact, \( \bigsqcup \) is equivariant w.r.t. the whole \( \text{Perm}(\kappa) \) and then, in particular, w.r.t. \( G \), so it preserves orbit-finiteness. Now, to check \( \text{row}(t) = \bigsqcup C(\text{row}(t)) \), we can just pick one representative of every orbit of \( S \cdot A \), because we have \( C(\pi \cdot \text{row}(t)) = \pi \cdot C(\text{row}(t)) \) and permutations distribute over \( \cup \), so permuting both sides of the equation gives again a valid equation.

For RFSA-consistency, consider the two sets:

\[
N = \{ (s_1, s_2) \in S \times S \mid \text{row}(s_1) \subseteq \text{row}(s_2) \} \\
M = \{ (s_1, s_2) \in S \times S \mid \forall a \in A : \text{row}(s_1.a) \subseteq \text{row}(s_2.a) \}
\]

They are both orbit-finite nominal sets, by equivariance of row, \( \subseteq \) and \( A \). We can check RFSA-consistency in finite time by picking orbit representatives from \( N \) and \( M \). For each representative \( n \in N \), we look for a representative \( m \in M \) and a permutation \( \pi \) such that \( n = \pi \cdot m \). If no such \( m \) and \( \pi \) exist, then \( n \) does not belong to any orbit of \( M \), so it violates RFSA-consistency.

**Line 5 and 8 finding witnesses for violations.** We can find witnesses by comparing orbit representatives of orbit-finite sets, as we did with RFSA-consistency. Specifically, we can pick representatives in \( S \times A \) and \( S \times S \times A \times E \) and check them against the following orbit-finite nominal sets:

- \( \{ (s, a) \in S \times A \mid \text{row}(sa) \in PR(S, E) \setminus PR^\top(S, E) \} \)
- \( \{ (s_1, s_2, a, e) \in S \times S \times A \times E \mid \text{row}(s_1.a)(e) = 1, \text{row}(s_2.a)(e) = 0, \text{row}(s_1) \subseteq \text{row}(s_2) \} \)

5.3 Correctness

Now we prove correctness and termination of the algorithm. First, we prove that hypothesis automata are nominal NFAs.

**Lemma 11.** The hypothesis automaton \( N(S, E) \) (see Definition 2) is a nominal NFA.

\( N(S, E) \), as in ordinary νL*, is not always a nominal RFSA. However, we have the following.

**Theorem 3.** If the table \( (S, E) \) is RFSA-closed, RFSA-consistent and \( N(S, E) \) is consistent with \( (S, E) \), then \( N(S, E) \) is a canonical nominal RFSA.

This is proved in [10] for ordinary RFSA, using the standard theory of regular languages. The nominal proof is exactly the same, using derivatives of nominal regular languages and nominal NFAs as defined in Section 5.1.

**Lemma 12.** The table \( (S, E) \) cannot have more than \( n \) orbits of distinct rows, where \( n \) is the number of orbits of the minimal normal DFA for the target language.

**Proof.** Rows are residuals of \( L \), which are states of the minimal normal DFA for \( L \), so orbits cannot be more than \( n \). □

**Theorem 4.** The algorithm νRL* terminates and returns the canonical nominal RFSA for \( L \).

**Proof.** If the algorithm terminates, then it must return the canonical nominal RFSA for \( L \) by Theorem 5. We prove that a table can be made RFSA-closed and RFSA-consistent in finite time. This is similar to the proof of Theorem 2 and is inspired by the proof [10].

If the table is not closed, we find a row \( s \in S \cdot A \) such that \( \text{row}(s) \in PR(S, E) \setminus PR^\top(S, E) \). The algorithm then adds \( \text{orb}(s) \) to \( S \). Since \( s \) was non-equivalent to all upper prime rows, and thus from all the rows indexed by \( S \), we find that \( S \cup \text{orb}(t)/\sim \) has strictly more orbits than \( S/\sim \) (recall that \( s \sim t \iff \text{row}(s) = \text{row}(t) \)). This addition can only be done finitely-many times, because the number of orbits of \( S/\sim \) is bounded, by Lemma 12.

Now, the case of RFSA-consistency needs some additional notions. Let \( R \) be the (orbit-finite) nominal set of all rows, and let \( I = \{(r, r') \in R \times R \mid r \sim r'\} \) be the set of all inclusion relations among rows. The set \( I \) is orbit-finite. In fact, consider

\[
J = \{ (s, t) \in (S \cup S \cdot A) \times (S \cup S \cdot A) \mid \text{row}(s) \subseteq \text{row}(t) \}
\]

This set is an equivariant, thus orbit-finite, subset of \( (S \cup S \cdot A) \times (S \cup S \cdot A) \). The set \( I \) is the image of \( J \) via \( \text{row} \times \text{row} \), which is equivariant, so it preserves orbit-finiteness.

Now, suppose the algorithm finds two elements \( s_1, s_2 \in S \) with \( \text{row}(s_1) \subseteq \text{row}(s_2) \) but \( \text{row}(s_1.a)(e) = 1 \) and \( \text{row}(s_2.a)(e) = 0 \) for some \( a \in A \) and \( e \in E \). Adding a column to fix RFSA-consistency may:

- (C1) increase orbits of \( (S \cup S \cdot A)/\sim \); or
- (C2) decrease orbits of \( I \); or
- (C3) decrease local symmetries/increase dimension of one orbit of rows. In fact, if no new rows are added (C1), we have two cases.

- If \( \text{row}(s_1) \nsubseteq \text{row}(s_2) \), i.e., \( (\text{row}(s_1), \text{row}(s_2)) \notin I \), then \( \text{row}(s_1) \nsubseteq \text{row}(s_2) \), where \( \text{row} \) is the new table. Therefore the orbit of \( \text{row}(s_1), \text{row}(s_2) \) is not in \( I \). Moreover, \( \text{row}(s) \subseteq \text{row}(t) \) implies \( \text{row}(s) \subseteq \text{row}(t) \) (as no new rows are added), so no new pairs are added to \( I \). Overall, \( I \) has less orbits (C2).
We now give bounds for the number of equivalence and membership (i.e., the size of the maximum support) of its nominal set of states. Therefore all the above changes can happen finitely-many times.

Lemma 14. Let \( m \) be the length of the longest counterexample given by the teacher. Then the table has:

- at most \( n \) orbits in \( S \), with words of length at most \( n \);
- at most \( mE_{n,k}' \) orbits in \( E \), with words of length at most \( mE_{n,k}' \).

Proof. By Lemma 12 the number of orbits of rows indexed by \( S \) is at most \( n \). Now, notice that line 5 does not add orb \((sa)\) to \( S \) if \( sa \in S \), and lines 12 and 9 cannot identify rows, so \( S \) has at most \( n \) orbits. The length of the longest word in \( S \) must be at most \( n \), as \( S = \{ e \} \) when the algorithm starts, and line 6 adds words with one additional symbol than those in \( S \).

For columns, we note that both fixing RFSA-consistency and adding counterexamples increase the number of columns, but this can happen at most \( E_{n,k}' \) times (see proof of Lemma 13). Each time at most \( m \) suffixes are added to \( E \).

We compute the maximum number of cells as in Section 4.3

Lemma 15. The number of orbits in the lower part of the table, \( S\cdot A \), is bounded by \( n f_a(p, p) \).

Then \( C_{k,m} = n(f_a(p, p) + 1)mE_{n,k}' \) is the maximal number of cells in the table. This bound is polynomial in \( n, m \), and \( l \), but not in \( k \) and \( p \).

Corollary 2. The number of membership queries is bounded by \( C_{n,k,m}f_a(p, pmE_{n,k}') \).

6. Implementation and preliminary experiments

Our algorithms for learning nominal automata operate on infinite sets of rows and columns, and hence it is not immediately clear how to actually implement them on a computer. We have used NLambda [26], our recently developed Haskell library designed to allow direct manipulation of infinite (but orbit-finite) nominal sets, within the functional programming paradigm. The semantics of NLambda is based on [8], and the library itself is inspired by Fresh O’Cam [39], a language for functional programming over nominal data structures with binding.

6.1 NLambda

NLambda extends Haskell with a new type \( \text{Atoms} \). Values of this type are atomic values that can be compared for equality and have no other discernible structure. They correspond to the elements of the infinite alphabet \( A \) described in Section 3.

Furthermore, NLambda provides a unary type constructor \( \text{Set} \). This appears similar to the the \( \text{Data.Set} \) type constructor from the standard Haskell library, but its semantics is markedly different: whereas the latter is used to construct finite sets, the former has orbit-finite sets as values. The new constructor \( \text{Set} \) can be applied to a range of equality types that include \( \text{Atoms} \), but also the tuple type (\( \text{Atoms}.\text{Atoms} \)), the list type (\( \text{Atoms} \)), the set type \( \text{Set} \), and other types that provide basic infrastructure necessary to speak of supports and orbits. All these are instances of a type class \( \text{NominalType} \) specified in NLambda for this purpose.

NLambda, in addition to all the standard machinery of Haskell, offers primitives to manipulate values of any nominal types \( \tau, \sigma \):

- empty : \( \text{Set} \tau \), returns the empty set of any type;
- atoms : \( \text{Set} \text{Atoms} \), returns the (infinite but single-orbit) set of all atoms;
- insert : \( \tau \rightarrow \text{Set} \tau \rightarrow \text{Set} \tau \), adds an element to a set;
- map : \( \tau \rightarrow \sigma \rightarrow (\text{Set} \tau \rightarrow \text{Set} \sigma) \), applies a function to every element of a set;
- sum : \( \text{Set} \tau \rightarrow \text{Set} \tau \), computes the union of a family of sets;
is Empty : Set τ → Formula, checks whether a set is empty.
The type Formula takes the role of a Boolean type. For technical reasons it is distinct from the standard Haskell type Bool, but it provides standard logical operations such as

not : Formula → Formula
or : Formula → Formula → Formula,
as well as a conditional operator ite : Formula → τ → τ → τ
that mimics the standard if construction. It is also the result type of a
built-in equality test on atoms, eq : Atoms → Atoms → Formula.

Using these primitives, one builds more functions to operate on
orbit-finite sets, as well as to predict whether a given predicate:

filter : (τ → Formula) → Set τ → Set τ
filter p s = sum (map (λx.ite (p x) (singleton x) empty) s)
of functions to quantify a predicate over a set:

exists, forall : (τ → Formula) → Set τ → Formula
exists p s = not (isEmpty (filter p s))
forall p s = isEmpty (filter (λx.not (p x)) s)
and so on. Note that these functions are written in exactly the same
way as they would be for finite sets and the standard Data.Set type.
This is not an accident, and indeed the programmer can use
the convenient set-theoretic intuition of NLambda primitives. For
example, one could conveniently construct various orbit-finite sets
such as the set of all pairs of atom variables

atomPairs = sum (map (λx.map (λy.(x,y)) atoms) atoms),

the set of all pairs of distinct atoms:

distPairs = filter (λ(x,y).not(eq x y)) atomPairs

and so on.

It should be stressed that all these constructions terminate in finite
time, even though they formally involve infinite sets. To achieve this,
values of orbit-finite set types Set τ are internally not represented
as lists or trees of elements of type τ. Instead, they are stored and
manipulated symbolically, using first-order formulas over variables
that range over atom values. For example, the value of distPairs
above is stored as the formal expression:

\{(a,b) | a, b ∈ A, a ≠ b\}
or, more specifically, as a triple:

• a pair (a, b) of “atom variables”,
• a list [a, b] of those atom variables that are bound in the expres-
sion (in this case, the expression contains no free variables),
• a formula a ≠ b over atom variables.

All the primitives listed above, such as isEmpty, map and sum,
are implemented on this internal representation. In some cases,
this involves checking the satisfiability of certain formulas over
atoms. In the current implementation of NLambda, an external SMT
solver Z3 [34] is used for that purpose. For example, to evaluate
the expression isEmpty distPairs, NLambda makes a system call to
the SMT solver to check whether the formula a ≠ b is satisfiable in
the first-order theory of equality and, after receiving the affirmative
answer, returns the value False.

For more details about the semantics and implementation of
NLambda, see [26]. The library itself can be downloaded from [40].

<table>
<thead>
<tr>
<th></th>
<th>DFA</th>
<th>(\nu L^*) (s)</th>
<th>(\nu L^*) (c)</th>
<th>RFSA</th>
<th>(\nu NL^*) (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIFO_0</td>
<td>2</td>
<td>1.9</td>
<td>2</td>
<td>0</td>
<td>2.4</td>
</tr>
<tr>
<td>FIFO_1</td>
<td>3</td>
<td>12.9</td>
<td>7.4</td>
<td>3</td>
<td>17.3</td>
</tr>
<tr>
<td>FIFO_2</td>
<td>5</td>
<td>45.6</td>
<td>22.6</td>
<td>5</td>
<td>70.3</td>
</tr>
<tr>
<td>FIFO_3</td>
<td>10</td>
<td>189.3</td>
<td>107</td>
<td>10</td>
<td>476</td>
</tr>
<tr>
<td>FIFO_4</td>
<td>25</td>
<td>370</td>
<td>267</td>
<td>25</td>
<td>1230</td>
</tr>
<tr>
<td>FIFO_5</td>
<td>77</td>
<td>1337</td>
<td>697</td>
<td>∞</td>
<td>∞</td>
</tr>
<tr>
<td>(L_0)</td>
<td>2</td>
<td>1.3</td>
<td>1.4</td>
<td>2</td>
<td>1.4</td>
</tr>
<tr>
<td>(L_1)</td>
<td>4</td>
<td>29.6</td>
<td>4.7</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>(L_2)</td>
<td>7</td>
<td>229</td>
<td>23.1</td>
<td>7</td>
<td>84.7</td>
</tr>
<tr>
<td>(L_3)</td>
<td>3</td>
<td>4.4</td>
<td>4.9</td>
<td>3</td>
<td>11.3</td>
</tr>
<tr>
<td>(L_4)</td>
<td>5</td>
<td>15.4</td>
<td>15.4</td>
<td>5</td>
<td>66.4</td>
</tr>
<tr>
<td>(L_5)</td>
<td>9</td>
<td>46.3</td>
<td>40.5</td>
<td>5</td>
<td>210</td>
</tr>
<tr>
<td>(L_6)</td>
<td>17</td>
<td>89.0</td>
<td>60.8</td>
<td>6</td>
<td>566</td>
</tr>
<tr>
<td>(L_{eq})</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>3</td>
<td>16.3</td>
</tr>
</tbody>
</table>

Table 1. Results of experiments. The column DFA (resp. RFSA)
shows the number of orbits (left sub-column) and dimension (right
sub-column) of the learnt minimal DFA (resp. canonical RFSA). We
use \(\infty\) when the running time is too high.

6.2 Implementation of \(\nu L^*\) and \(\nu NL^*

Using NLambda we implemented the algorithms from Sections [4]
and [5]. We note that the internal representation is slightly
different than the one discussed in Section [4]. Instead of representing
the table (S, E) with actual representatives of orbits, the sets are
represented logically as described above. Furthermore the control
flow of the algorithm is adapted to fit in the functional programming
paradigm. In particular, recursion is used instead of a while loop.
In addition to the nominal adaptation of Angluin’s algorithm \(\nu L^*\),
we implemented a variant, \(\nu L^*_c\) which adds counterexamples to the
columns instead of rows.

Target automata are defined using NLambda as well, using the
automaton data type provided by the library. Membership queries
are already implemented by the library. Equivalence queries are
implemented by constructing a bisimulation (recall that bisimulation
implies language equivalence), where a counterexample is obtained
when two DFAs are not bisimilar. For nominal NFAs, however, we
cannot implement a complete equivalence query as their language
equivalence is undecidable. We approximated the equivalence by
bounding the depth of the bisimulation for nominal NFAs. As an
optimization, we use bisimulation up to congruence [13].

Having an approximate teacher is a minor issue since in many applications
no complete teacher can be implemented and one relies on testing [2] [12].
For the experiments listed here the bound was chosen large
enough for the learner to terminate with the correct automaton.

We remark that our algorithms seamlessly merge with teachers
written in NLambda, but the current version of the library does not
allow generating concrete membership queries for external teachers.
We are currently working on a new version of the library in which
this will be possible.

6.3 Test cases

To provide a benchmark for future improvements, we tested our
algorithms on a few simple automata described below. We report
results in Table 1. The experiments were performed on a machine
with an Intel Core i5 (Skylake, 2.4 GHz) and 8 GB RAM.

Queue data structure. A queue is a data structure to store ele-
ments which can later be retrieved in a first-in, first-out order.
It has two operations: push and pop. We define the alphabet
\(\Sigma_{FIFO} = \{\text{push}(a), \text{pop}(a) | a ∈ A\}\). The language \(FIFO_n\)
contains all valid traces of push and pop using a bounded queue of
size \(n\). The minimal nominal DFA for \(FIFO_2\) is
We stress that no comparison is possible for works with the whole alphabet from the very start, and it exploits whole language. In Sakamoto’s approach, any learning algorithm where the transition from some letter appears twice. This is accepted by an NFA which Transitions are defined symbolically using propositional logic. We This section compares benchmarks appear in \[2, 23\].

\[\]\

\[\text{Double word. } \mathcal{L}_n = \{ww \mid w \in \mathbb{A}^n\} \text{ from Section}\[3\]

\[\text{NFA. Consider the language } \mathcal{L}_{eq} = \bigcup_{a \in \mathbb{A}^*} a \mathbb{A}^* a \mathbb{A}^* \text{ of words where some letter appears twice. This is accepted by an NFA which guesses the position of the first occurrence of a repeated letter } a \text{ and then waits for the second } a \text{ to appear. The language is not accepted by a DFA } [9].\text{ Despite this } \nu \mathcal{L}^* \text{ is able to learn the automaton:}

\[\]

\[\]

\[\text{where the transition from } q'_{2,2} \text{ to } q'_{1,2} \text{ is defined as } \delta(q'_{2,2}, a) = \{q'_{1, b} \mid b \in \mathbb{A}\}.\]

\(n\)-last position. A prototypical example of regular languages which are accepted by very small NFAs is the set of words where a distinguished symbol \(a\) appears on the \(n\)-last position \([11]\). We define a similar nominal language \(\mathcal{L}_n' = \bigcup_{a \in \mathbb{A}^*} a \mathbb{A}^* a \mathbb{A}^*.\) To accept such words non-deterministically, one simply guesses the \(n\)-last position. This language is also accepted by a much larger deterministic automat.

\[\]

\[\]

\[\text{7. Related work}\]

This section compares \(\nu \mathcal{L}^*\) with other algorithms from the literature. We stress that no comparison is possible for \(\nu \mathcal{L}^*\), as it is the first learning algorithm for non-deterministic automata over infinite alphabets.

The first one to consider learning automata over infinite alphabets was Sakamoto \([15]\). In his work the problem is reduced to \(\mathcal{L}^*\) with some finite sub-alphabet. The sub-alphabet grows in stages and \(\mathcal{L}^*\) is rerun at every stage, until the alphabet is big enough to capture the whole language. In Sakamoto’s approach, any learning algorithm can be used as a back-end. This, however, comes at a cost: it has to be rerun at every stage, and each symbol is treated in isolation, which might require more queries. Our algorithm \(\nu \mathcal{L}^*\), instead, works with the whole alphabet from the very start, and it exploits its symmetry. An example is in Sections \([27, 28]\) the ordinary learner uses four equivalence queries, whereas the nominal one, using the symmetry, only needs three. Moreover, our algorithm is easier to generalize to other alphabets and computational models, such as non-determinism.

More recently papers appeared on learning register automata \([15, 21]\). Their register automata are as expressive as our deterministic nominal automata. The state-space is similar to our orbit-wise representation: it is formed by finitely many locations with registers. Transitions are defined symbolically using propositional logic. We remark that the most recent paper \([15]\) generalizes the algorithm to alphabets with different structures (which correspond to different atom symmetries in our work), but at the cost of changing Angluin’s framework. Instead of membership queries the algorithm requires more sophisticated tree queries. In our approach, using a different symmetry does not affect neither the algorithm nor its correctness proof. Tree queries can be reduced to membership queries by enumerating all \(n\)-types for some \(n\) (\(n\)-types in logic correspond to orbits in the set of \(n\)-tuples). Keeping that in mind, their complexity results are roughly the same as ours, although this is hard to verify, as they do not give bounds on the length of individual tree queries. Finally, our approach lends itself better to be extended to other variations on \(\mathcal{L}^*\) (of which many exist), as it is closer to Angluin’s original work.

Another class of learning algorithms for systems with large alphabets is based on abstraction and refinement, which is orthogonal to the approach in the present paper but connections and possible transference of techniques are worth exploring in the future. In \([2, 23]\), the alphabet is reduced to a finite alphabet of abstractions, and \(\mathcal{L}^*\) for ordinary DFAs over such finite alphabet is used. Abstractions are refined by counterexamples. Other similar approaches are \([20, 22]\), where global and local per-state abstractions of the alphabet are used, and \([29, 32]\), where the alphabet can also have additional structure (e.g., an ordering relation). We can also mention \([14]\), a framework for learning symbolic models of software behavior. In \([5, 6]\), authors cope with an infinite alphabet by running \(\mathcal{L}^*\) (adapted to Mealy machines) using a finite approximation of the alphabet, which may be augmented when equivalence queries are answered. A smaller symbolic model is derived subsequently. Their approach, unlike ours, does not exploit the symmetry over the full alphabet. The symmetry allows our algorithm to reduce queries and to produce the smallest possible automaton at every step.

Finally we compare with results on session automata \([12]\). Session automata are defined over finite alphabets just like the work by Sakamoto. However, session automata are more restrictive than deterministic nominal automata. For example, the model cannot capture an acceptor for the language of words where consecutive data values are distinct. This language can be accepted by a three orbit nominal DFA, which can be learned by our algorithm.

We implemented our algorithms in the nominal library NLambda as sketched before. Other implementation options include Fresh O’Caml \([39]\), a functional programming language designed for programming over nominal data structures with binding, and LOIS \([27, 28]\), a C++ library for imperative nominal programming. We chose NLambda for its convenient set-theoretic primitives, but the other options remain to be explored, in particular the low-level LOIS could be expected to provide more efficient implementations.

\[\]

\[\text{8. Discussion and future work}\]

In this paper we defined and implemented extensions of several versions of \(\mathcal{L}^*\) and of \(\nu \mathcal{L}^*\) for nominal automata.

We highlight two features of our approach:

- it has strong theoretical foundations: the theory of nominal languages, covering different alphabets and symmetries (see Section \([11]\), category theory, where nominal automata have been characterized as coalgebras \([16, 29]\) and many properties and algorithms (e.g., minimization) have been studied at this abstract level.

- it follows a generic pattern for transporting computation models and algorithms from finite sets to nominal sets, which leads to simple correctness proofs.

These features pave the way to several extensions and improvements. Future work includes a general version of \(\nu \mathcal{L}^*\), parametric in the notion of side-effect (an example is non-determinism). Different notions will yield models with different degree of succinctness w.r.t. deterministic automata. The key observation here is that many forms of non-determinism and other side effects can be captured via the
categorical notion of monad, i.e., an algebraic structure, on the state-space. Monads allow generalizing the notion of composed and prime state: a state is composed whenever it is obtained from other states via an algebraic operation. Our algorithm \(\mathcal{LR}L\) is based on the powerser monad, representing classical non-determinism. We are currently investigating a substitution monad, where the operation is “applying a (possibly non-injective) substitution of states in the support”. A minimal automaton over this monad, akin to a RFSA, will have states that can generate all the states of the associated minimal DFA via a substitution, but cannot be generated by other states (they are prime). For instance, we can give an automaton over the substitution monad that recognizes \(L_2\) from Section [2].

\[
\begin{array}{c}
\phi_0 \xrightarrow{y} x, [y \rightarrow x] \neq x \\
\phi_1 \xrightarrow{y} u, y \neq u \\
\phi_2 \xrightarrow{y} A \\
\phi_3 \xrightarrow{y} A
\end{array}
\]

Here \([y \rightarrow x]\) means that, if that transition is taken, \(\phi_{2,0}\) (hence its subject) is subject to \(y \rightarrow x\). In general, the size of the minimal DFA for \(L_n\) grows more than exponentially with \(n\), but an automaton with substitutions on transitions, like the one above, only needs \(O(n)\) states.

In principle, thanks to the generic approach we have taken, all our algorithms should work for various kinds of atoms with more structure than just equality, as advocated in [9]. Details, such as precise assumptions on the underlying structure of atoms necessary for proofs to go through, remain to be checked. For an implementation of automata learning over other kinds of atoms without compromizing the generic approach, an extension of NLambda to those atoms will be needed, as the current version of the library only supports equality and totally ordered atoms.

The efficiency of our current implementation, as measured in Section [6.3] leaves much to be desired. There is plenty of potential for running time optimization, ranging from improvements in the learning algorithms itself, to optimizations in the NLambda library (such as replacing the external and general-purpose SMT solver with a purpose-built, internal one, or a tighter integration of nominal computation. In \(\text{POPL}\), pages 401–412, 2012.

Acknowledgements. We thank Frits Vaandrager and Gerco van Heerdt for useful comments and discussions. We also thank the anonymous reviewers.

References


A. Omitted proofs

A.1 Section 4

Lemma 1. The relation \( \sim \) is an equivariant equivalence relation.

Proof. Since the language \( L \) is equivariant, so is \( row \). The relation \( \sim \) is defined as kernel of \( row \) and is hence equivariant and an equivalence relation.

Lemma 2. For all \( u, v \in S \) we have that \( u \equiv_L v \) implies \( u \sim v \).

Proof. If \( u \equiv_L v \) then \( L(uw) = L(vw) \) for all \( w \in A^* \). In particular \( row(u)(e) = L(ue) = L(v e) = row(v)(e) \) for all \( e \in E \). Hence \( row(u) = row(v) \).

Lemma 3. We have \( \text{supp}(\{u\}_\sim) \subseteq \text{supp}(\{u\}_\equiv) \subseteq \text{supp}(u) \) for all \( u \in S \).

Proof. By Lemma 1 we have an equivariant function \( S/\equiv \rightarrow S/\sim \) sending \( [u]_\equiv \) to \( [u]_\sim \). Since equivariant functions preserve supports (Lemma 4.8 in [9]) we have \( \text{supp}(\{u\}_\sim) \subseteq \text{supp}(\{u\}_\equiv) \).

A.2 Section 5

Lemma 4. The canonical nominal RFSA is a proper nominal NFA.

Proof.

- \( Q \) is orbit-finite, as \( PR(L) \) is an equivariant subset of \( R(L) \), which is orbit-finite. We now show equivariance of \( PR(L) \).
- Suppose \( L' \in PR(L) \) but \( \pi \cdot L' \notin PR(L) \). We have \( \pi \cdot L' \in R(L) \), by equivariancy of \( R(L) \), so \( \pi \cdot L' \) is the union of the finite residuals it strictly contains. By equivariancy of \( R(L) \), \( \pi \cdot L' \) is composed: its components are those of \( \pi \cdot L' \) permuted via \( \pi^{-1} \). This is a contradiction.
- \( Q_0 \) is an equivariant, orbit-finite subset of \( PR(L) \). We have \( \text{supp}(L) = \emptyset \) and \( L = \bigcup Q_0 \) so \( \text{supp}(Q_0) = \emptyset \), i.e., \( Q_0 \) is equivariant. Being an an equivariant subset of \( Q \), which is orbit-finite, it is itself orbit-finite.
- \( F \) is equivariant. In fact, take \( L' \in F \). Byequivariancy of \( Q \), \( \pi \cdot L' \in Q \), and we have \( \pi \equiv row(\pi \cdot L') \). We prove that \( \pi \cdot L' \) is finitely-sent in the usual argument.
- \( \delta \) is an equivariant relation, i.e., \( (L_1, a, L_2) \in \delta \) implies \( (\pi \cdot L_1, \pi \cdot a, \pi \cdot L_2) \in \delta \). Take \( L_1 \in \pi \cdot L' \) and \( \delta \cdot L_1 \), i.e., \( v \in L_2 \) implies \( \pi \cdot v \in L_1 \). Then \( \pi^{-1} \cdot v \in L_2 \), so \( \pi^{-1} \cdot L_1 \), and then \( (\pi \cdot a) \pi^{-1} \cdot L_1 \), as required.

\( \square \)

Lemma 9. \( PR(S, E), PR^T(S, E) \) and \( PR(S, E) \setminus PR^T(S, E) \) are orbit-finite nominal sets.

Proof. We prove that \( PR(S, E) \) is equivariant. We know that the set \( R(S, E) \) of rows of \( (S, E) \) is an orbit-finite nominal set. Suppose by contradiction that \( row(t) \in PR(S, E) \) but \( \pi \cdot row(t) \notin PR(S, E) \). Then \( \pi \cdot row(t) = \bigcup \{row(s) | row(s) \subseteq \pi \cdot row(t)\} \).

Then, by equivariancy of \( \subseteq \), \( row(t) \) is the union of \( \pi^{-1} \cdot row(s) \), with \( row(s) \) in the equation above, so it is composed, a contradiction. Since \( PR(S, E) \) is an equivariant subset of an orbit-finite nominal set, it is orbit-finite. A similar argument gives \( PR^T(S, E) \) orbit-finite. Finally, \( PR(S, E) \setminus PR^T(S, E) \) is obtained by removing some orbits from \( PR(S, E) \), so it is orbit-finite.

\( \square \)

Lemma 10. The set \( C(row(t)) \) has the following properties:

1. \( \text{supp}(C(row(t))) \subseteq \text{supp}(row(t)) \).
2. it is orbit-finite under the action of the group \( G_t = \{ \pi \in \text{Perm}(\lambda) | \pi[\text{supp}(row(t))] = \text{id} \} \) of permutations fixing \( \text{supp}(row(t)) \).

Proof.

1. We prove that permutations fixing \( \text{supp}(row(t)) \) also fix \( C(row(t)) \). Take \( \pi \) such that \( \pi[\text{supp}(row(t))] = \text{id} \) and \( row(s) \in C(row(t)) \). We want to prove that \( \pi \cdot row(s) \in C(row(t)) \). If we have \( row(s) \subseteq row(t) \) and, by equivariancy of \( \subseteq \), \( \pi \cdot row(s) \subseteq \pi \cdot row(t) \). But \( \pi \cdot row(t) = row(t) \), as \( \pi \) fixes \( \text{supp}(row(t)) \), so \( \pi \cdot row(s) \subseteq row(t) \), as required.

2. In the previous point we proved that \( C(row(t)) \) is equivariant w.r.t. permutations in \( G_t \). To show that it is orbit-finite, it is enough to show that \( PR^T(S, E) \) is orbit-finite w.r.t. \( G_t \); orbit-finiteness of \( C(row(t)) \) will follow by equivariancy. We call \( G_t \)-orbit (resp. \( \text{Perm}(\lambda) \)-orbit) an orbit w.r.t. the group of permutations \( G_t \) (resp. \( \text{Perm}(\lambda) \)). Each \( G_t \)-orbit of \( PR^T(S, E) \) is clearly included in one of its \( \text{Perm}(\lambda) \)-orbits, so we show that each orbit of the latter type contains finitely-many orbits of the former type. Every \( \text{Perm}(\lambda) \)-orbit of dimension \( k \) in \( PR^T(S, E) \) is image of \( \lambda^{(k)} \) via an equivariant surjective function. Such functions can only decrease the number of orbits, so we prove that \( \lambda^{(k)} \) is orbit-finite w.r.t. \( G_t \). Take \( (a_1, \ldots, a_k) \in \lambda^{(k)} \). Then \( (a_1, \ldots, a_k) \) and \( (a_i', \ldots, a_k') \) are in the same \( G_t \)-orbit if and only if \( a_i \in \text{supp}(row(t)) \) implies \( a_i = a_i' \). Hence, the number of \( G_t \)-orbits of \( PR^T(S, E) \) contained in one of its \( \text{Perm}(\lambda) \)-orbit is at most the number of subsets of size \( k \) of a set of size \( |\text{supp}(row(t))|\).

\( \square \)
**Lemma (11).** The conjecture automaton \( N(S, E) \) (see Definition 4) is a nominal NFA.

**Proof.** Let \( N(S, E) = (Q, Q_0, F, \delta) \). Then:

- \( Q = PR(S, E) \) is an orbit-finite nominal set (Lemma 9);
- \( Q_0 \) is an equivariant, thus orbit-finite, subset of \( Q \). In fact \( \text{supp}(\text{row}(\varepsilon)) \subseteq \text{supp}(\varepsilon) = \emptyset \) (Lemma 10), so \( \text{supp}(Q_0) = \emptyset \) by Lemma 10(1), i.e., it is equivariant.
- \( F \) is an orbit-finite, thus orbit-finite, subset of \( Q \). Suppose \( r \in F \), i.e., \( r(\varepsilon) = 1 \). Then
  \[
  (\pi \cdot r)(\varepsilon) = \pi \cdot r(\pi^{-1} \cdot \varepsilon) = \pi \cdot r(\varepsilon) = 1
  \]
  where the second equation uses the action of permutations over functions \( 2^E \). Therefore \( (\pi \cdot r) \in F \).
- The transition relation \( \delta \) is equivariant. To prove this, we need to show that \( (\text{row}(s), a, r') \in \delta \) implies \( (\pi \cdot \text{row}(s), \pi(a), \pi \cdot r') \in \delta \). By definition, \( (\text{row}(s), a, r') \in \delta \) only if \( r' \subseteq \text{row}(sa) \). Using equivariance of \( \subseteq \), \( \pi \cdot r' \subseteq \pi \cdot \text{row}(sa) \) and, using equivariance of \( \text{row} \), \( \pi \cdot \text{row}(sa) = \text{row}(\pi \cdot s \pi(a)) \). Therefore \( \pi \cdot r' \subseteq \text{row}(\pi \cdot s \pi(a)) \), which gives \( (\pi \cdot \text{row}(s), \pi(a), \pi \cdot r') \in \delta \).  

\[\square\]