Electronic Notes in Theoretical Informatics And Computer Science

ENTICS
https://entics.episciences.org

Volume 1
Proceedings of
MFPS 2022

Guarded Kleene Algebra with Tests: Automata Learning

Stefan Zetzsche[a,1,3] Alexandra Silva[b,a,2] Matteo Sammartino[c,a]

[a] *University College London*
[b] *Cornell University*
[c] *Royal Holloway, University of London*

Abstract

Guarded Kleene Algebra with Tests (GKAT) is the fragment of Kleene Algebra with Tests (KAT) that arises by replacing the union and iteration operations of KAT with predicate-guarded variants. GKAT is more efficiently decidable than KAT and expressive enough to model simple imperative programs, making it attractive for applications to e.g. network verification. In this paper, we further explore GKAT's automata theory, and present GL^*, an algorithm for learning the GKAT automaton representation of a black-box, by observing its behaviour. A complexity analysis shows that it is more efficient to learn a representation of a GKAT program with GL^* than with Angluin's existing L^* algorithm. We implement GL^* and L^* in OCaml and compare their performances on example programs.

Keywords: Automata Learning, Kleene Algebra, Angluin, Coalgebra, Minimization, Moore Automata, Black-box, Model checking, Verification

1 Introduction

As hardware and software systems continue to grow in size and complexity, practical and scalable methods for verification tasks become increasingly important. Classical model checking approaches to verification require the existence of a rich model of the system of interest, able to express all its relevant behaviour. In reality such a model however is rarely available, for instance, when the system comes in the form of a black-box with no access to the source code, or the system is simply too complex for manual processing.

Automata learning, or regular inference, aims to automatically infer an automata model by observing the behaviour of the system. The incremental approach has been successfully applied to a wide range of verification tasks from finding bugs in network protocols [9], reverse engineering smartcard reader for internet banking [7], and industrial applications [15]. A comprehensive survey of the field can be found in [40]. The majority of modern learning algorithms is based on Angluin's L^* algorithm [3], which learns the unique minimal deterministic finite automaton (DFA) accepting a given regular language, or more generally, the unique minimal Moore automaton accepting a weighted language (Algorithm 1). In many

[1] The author has been supported by GCHQ via the VeTSS grant "Automated black-box verification of networking systems" (4207703/RFA 15845) and by the ERC via the Consolidator Grant AutoProbe 101002697.

[2] The author has been supported by the ERC via the Consolidator Grant AutoProbe 101002697 and by a Royal Society Wolfson Fellowship.

[3] Email: stefanzetzsche@gmail.com

Published February 15, 2023
10.46298/entics.10505
Proceedings Available Online at
https://doi.org/10.46298/entics.proceedings.mfps38

Algorithm 1 Angluin's L^* algorithm for Moore automata with input A and output B

$S, E \leftarrow \{\varepsilon\}$
repeat
  while $T = (S, E, row : S \cup S \cdot A \to B^E)$ is not closed **do**
    find $t \in S \cdot A$ with $row(t) \neq row(s)$ for all $s \in S$
    $S \leftarrow S \cup \{t\}$
  end while
  construct and submit $m(T)$ to the teacher
  if the teacher replies *no* with a counterexample $z \in A^*$ **then**
    $E \leftarrow E \cup \mathtt{suf}(z)$
  end if
until the teacher replies *yes*
return $m(T)$

situations, however, targeting a DFA is not feasible, due to an explosion in the size of the state-space. Such cases instead require types of models specifically tailored for their domain-specific purposes.

For instance, modern networking systems can operate on very large data sets, making them very challenging to model. As a result, controlling, reasoning about, or extending networks can be surprisingly difficult. One approach to modernise the field that has recently gained popularity is *Software Defined Networking* (SDN) [11]. Modern SDN programming languages, notably *NetKAT* [2], allow operators to model their network and dynamically fine tune forwarding behaviour in response to events such as traffic shifts. Globally, NetKAT is based on *Kleene Algebra* (KA) [22], the sound and complete theory of regular expressions [21]. Locally, it incorporates *Boolean algebra*, the theory of predicates. Both logics have been unified in the well developed theory of *Kleene Algebra with Tests* (KAT) [23], which subsumes propositional Hoare logic and can be used to model standard imperative programming constructs. The automata theory for NetKAT has been introduced in [13].

Verifying properties about realistic networks reduces in NetKAT to deciding the behavioural equivalence of pairs of automata. Unfortunately, NetKAT's decision procedure is PSPACE-complete, mainly due its foundations in KAT. As a consequence, more efficiently decidable fragments of KAT have been considered. In [38] it was hinted that the *guarded fragment* of KAT is notably more efficiently decidable than the full language, while still remaining sufficiently expressive for networking purposes. The idea has been taken further in [37], which formally introduced *Guarded Kleene Algebra with Tests* (GKAT), a variation on KAT that arises by replacing the union and iteration operations from KAT with guarded variants. In contrast to KAT, the equational theory of GKAT is decidable in (almost) linear time. These properties make GKAT a promising candidate for the foundations of a SDN programming language that is more efficiently decidable than NetKAT.

In view of the potential applications of GKAT to the field of verification, this paper further investigates its automata theory. In detail, the paper makes the following contributions:

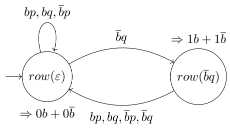
- For any GKAT automaton, we define a second automaton, which we call its minimization (Theorem 4.4). We show that in the class of normal GKAT automata, the minimization of an automaton is the unique size-minimal normal automaton accepting the same language (Theorem 4.12). We show that the minimization of a normal automaton is isomorphic to the automaton that arises by identifying semantically equivalent pairs among reachable states (Theorem 4.9), and that the minimizations of two language equivalent normal automata are isomorphic (Theorem 4.11). Finally, we show that minimizing a normal GKAT automaton preserves important invariants such as the nesting coequation (Theorem 4.10).
- We present GL^*, an active-learning algorithm (Algorithm 2) that incrementally infers a GKAT automaton from a black-box by querying an *oracle* (Section 5). We show that if the oracle is instantiated with the language accepted by a finite normal GKAT automaton, then the algorithm terminates with its minimization in finite time (Theorem 5.9).

	ε
ε	$0b+0\bar{b}$
bp	$0b+0\bar{b}$
bq	$0b+0\bar{b}$
$\bar{b}p$	$0b+0\bar{b}$
$\bar{b}q$	$1b+1\bar{b}$

(a)

	ε
ε	$0b+0\bar{b}$
$\bar{b}q$	$1b+1\bar{b}$
bp	$0b+0\bar{b}$
bq	$0b+0\bar{b}$
$\bar{b}p$	$0b+0\bar{b}$
$\bar{b}qbp$	$0b+0\bar{b}$
$\bar{b}qbq$	$0b+0\bar{b}$
$\bar{b}q\bar{b}p$	$0b+0\bar{b}$
$\bar{b}q\bar{b}q$	$0b+0\bar{b}$

(b)



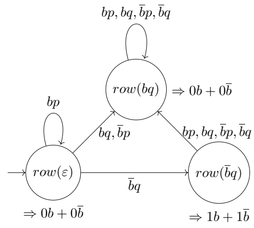
(c)

	ε	$\bar{b}q$	$bq\bar{b}q$
ε	$0b+0\bar{b}$	$1b+1\bar{b}$	$0b+0\bar{b}$
$\bar{b}q$	$1b+1\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
bp	$0b+0\bar{b}$	$1b+1\bar{b}$	$0b+0\bar{b}$
bq	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}p$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}qbp$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}qbq$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}q\bar{b}p$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}q\bar{b}q$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$

(d)

	ε	$\bar{b}q$	$bq\bar{b}q$
ε	$0b+0\bar{b}$	$1b+1\bar{b}$	$0b+0\bar{b}$
$\bar{b}q$	$1b+1\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
bq	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
bp	$0b+0\bar{b}$	$1b+1\bar{b}$	$0b+0\bar{b}$
$\bar{b}p$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}qbp$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}qbq$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}q\bar{b}p$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$\bar{b}q\bar{b}q$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$bqbp$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$bqbq$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$bq\bar{b}p$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$
$bq\bar{b}q$	$0b+0\bar{b}$	$0b+0\bar{b}$	$0b+0\bar{b}$

(e)



(f)

Fig. 1. An example run of Angluin's L^* algorithm for the target language $[\![(\texttt{while}\ b\ \texttt{do}\ p); q]\!]$.

- We show that the semantics of GKAT automata (2) can be reduced to the well-known semantics [4] of Moore automata. That is, there exists a language preserving embedding of GKAT automata into Moore automata (Theorem 6.1), which maps the minimization of a normal GKAT automaton to the language equivalent minimal Moore automaton (Theorem 6.2). In consequence, GKAT programs could thus, in principle, be also represented by Moore automata, instead of GKAT automata.
- We present a complexity analysis which shows that for GKAT programs it is more efficient to learn a GKAT automaton representation with GL^* than a Moore automaton representation with Angluin's L^* algorithm (Theorem 6.3). We implement GL^* and L^* in OCaml and compare their performances on example programs (Figure 6).

2 Overview of the approach

In this section, we give an overview of this paper through examples. We begin by presenting Algorithm 1, a slight variation of Angluin's L^* algorithm for finite Moore automata. We exemplify the algorithm by executing it for the language semantics of a simple GKAT program. We then propose a new algorithm, which, instead of a Moore automaton, infers a GKAT automaton.

2.1 L^* *algorithm*

Angluin's L^* algorithm learns the minimal DFA accepting a given regular language [3]. The algorithm has since been modified and generalised for a broad class of transition systems. The variation we present here step-wise infers the minimal Moore automaton accepting a generalised language $L : A^* \to B$ for a finite input set A and a finite output set B [31]. The algorithm assumes the existence of a *teacher* (or *oracle*), which can respond to two types of queries:

- **Membership queries**, consisting of a word $w \in A^*$, to which the teacher returns the output $L(w) \in B$;
- **Equivalence queries**, consisting of a hypothesis Moore automaton H, to which the teacher responds *yes*, if H accepts L, and *no* otherwise, providing a counterexample $z \in A^*$ in the symmetric difference of L and the language accepted by H.

The algorithm incrementally builds an *observation table*, which contains partial information about the language L obtained by performing membership queries. A table consists of two parts: a top part, with rows indexed by a finite set $S \subseteq A^*$; and a bottom-part, with rows ranging over $S \cdot A$. Columns are indexed by a finite set $E \subseteq A^*$. For any $t \in S \cup S \cdot A$ and $e \in E$, the entry at row t and column e, denoted

[4] In the language of Coalgebra, the semantics is given by the final coalgebra homomorphism for the functor defined by $FX = X^A \times B$, where $A = \mathrm{At} \cdot \Sigma = \{\alpha \cdot p \mid \alpha \in \mathrm{At},\ p \in \Sigma\}$ and $B = 2^{\mathrm{At}}$, for finite sets Σ and At. The carrier of the final coalgebra for F is $\mathcal{P}((\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At})$, the set of *guarded string languages*; the semantics of GKAT automata is given by the subclass of *deterministic* guarded string languages.

by $row(t)(e)$, is given by the output $L(te) \in B$. Note that the sets S and $S \cdot A$ can intersect. In such a case, elements in the intersection are only shown in the top part. Formally, we refer to a table as a tuple $T = (S, E, row)$, leaving the language L implicit.

Given a table T, one can construct a Moore automaton $m(T) = (X, \delta, \varepsilon, x)$, where $X = \{row(s) \mid s \in S\}$ is a finite set of states; the transition function $\delta : X \to X^A$ is given by $\delta(row(s), a) = row(sa)$; the output function $\varepsilon : X \to B$ satisfies $\varepsilon(row(s)) = row(s)(\varepsilon)$ (we abuse notation by writing ε both for the empty string and for the output function); and $x = row(\varepsilon)$ is the initial state. For $m(T)$ to be well-defined, the table T has to satisfy $\varepsilon \in S$ and $\varepsilon \in E$, and two properties called closedness and consistency. An observation table 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 is *consistent*, if whenever $s, s' \in S$ satisfy $row(s) = row(s')$, then $row(sa) = row(s'a)$ for all $a \in A$. A table is consistent in particular if the function row is injective.

The algorithm incrementally updates the table to satisfy those properties. If a well-defined hypothesis $m(T)$ can be constructed, the algorithm poses an equivalence query to the teacher, and either terminates, or refines the hypothesis with a counterexample $z \in A^*$. Since we respond to a negative equivalence query by adding the suffixes[5] of a counterexample to the set E (opposed to adding the prefixes of a counterexample to the set S), rows will always be distinct, rendering consistency trivial[6]. At all times, the set S is prefix-closed and the set E is suffix-closed[7].

2.1.1 Example of execution

We now execute Angluin's L^* (Algorithm 1) for the target language

$$L = [\![(\texttt{while } b \texttt{ do } p); q]\!] = \{\bar{b}qb, \bar{b}q\bar{b}, bp\bar{b}qb, bp\bar{b}q\bar{b}, ...\} \subseteq (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}, \tag{1}$$

where $\mathrm{At} = \{b, \bar{b}\}$ is a finite set of *atoms* and $\Sigma = \{p, q\}$ is a finite set of *actions*. The language L represents the semantics of a program that performs the action p while b is true, and otherwise continues with q. It can be viewed as a generalised language $\widehat{L}$ with input $A = (\mathrm{At} \cdot \Sigma)$ and output $B = 2^{\mathrm{At}}$ via currying. We denote functions $f \in B$ as formal sums $\sum_{\alpha \in \mathrm{At}} f(\alpha)\alpha$. Each query to $\widehat{L}$ requires $|\mathrm{At}|$ many queries to L.

Initially, the sets S and E are set to the singleton $\{\varepsilon\}$. We build the observation table in Figure 1a. Since the row indexed by $\bar{b}q$ does not appear in the upper part, i.e. differs from the row indexed by ε, the table is not closed. To resolve the closedness defect we add $\bar{b}q$ to S. The observation table (Figure 1b) is now closed. We derive from it the hypothesis depicted in Figure 1c. Next, we pose an equivalence query, to which the oracle replies *no* and informs us that the word $z = bq\bar{b}q$ has been falsely classified. Indeed, given z, the language accepted by the hypothesis outputs $1b + 1\bar{b}$, whereas (1) produces $0b + 0\bar{b}$. To respond to the counterexample z, we add its suffixes to E. In this case, there are only the two suffixes $\bar{b}q$ and $bq\bar{b}q$. The next observation table (Figure 1d) again is not closed: the row indexed by e.g. bq does not equal any of the two upper rows indexed by ε and $\bar{b}q$. To resolve the closedness defect we add bq to S, and obtain the table in Figure 1e. The observation table is now closed. We derive from it the automaton in Figure 1f. Next, we pose an equivalence query, to which the oracle replies *yes*.

2.2 GL^* *algorithm*

In this section, we propose a new algorithm (Algorithm 2) for learning GKAT program representations, which we call GL^*. The new algorithm modifies Algorithm 1 by addressing a number of observations.

First, we note that the Moore automaton in Figure 1f admits multiple transitions to $row(bq)$, a *sink-state*, which does not accept any words. Second, we observe that languages induced by GKAT programs are *deterministic*[8]. Such languages are naturally represented by GKAT automata, which keep some

[5] The set $\texttt{suf}(z)$ of suffixes for $z \in A^*$ is defined by $\texttt{suf}(\varepsilon) = \{\varepsilon\}$ and $\texttt{suf}(aw) = \{aw\} \cup \texttt{suf}(w)$.
[6] This variation of L^* has been introduced by Maler and Pnueli [29].
[7] A set $X \subseteq A^*$ is called *suffix-closed*, if $\texttt{suf}(z) \subseteq X$ for all $z \in X$.
[8] Deterministic in the sense that, whenever two strings agree on the first n atoms, then they agree on their first n actions (or lack thereof).

Algorithm 2 The GL^* algorithm for GKAT automata

$S \leftarrow \{\varepsilon\}, E \leftarrow \mathrm{At}$
repeat
  while $T = (S, E, row : S \cup S \cdot (\mathrm{At} \cdot \Sigma) \to 2^E)$ is not closed **do**
    find $t \in S \cdot (\mathrm{At} \cdot \Sigma)$ with $row(t)(e) = 1$ for some $e \in E$, but $row(t) \neq row(s)$ for all $s \in S$
    $S \leftarrow S \cup \{t\}$
  end while
  construct and submit $m(T)$ to the teacher
  if the teacher replies *no* with a counterexample $z \in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$ **then**
    $E \leftarrow E \cup \mathtt{suf}(z)$
  end if
until the teacher replies *yes*
return $m(T)$

transitions implicit. Third, in some cases [9] the deterministic nature of the target language allows us to fill-in parts of the observation table without performing any membership queries. Fourth, the cells of the observation table are labelled by functions, each of which requires two membership queries to (1); as a consequence, table extensions require an unfeasible amount of queries.

As before, we assume two finite sets, At and Σ, and a deterministic language $L \subseteq (\mathrm{At}\cdot\Sigma)^*\cdot\mathrm{At}$. The oracle of GL^* can answer two types of queries: membership queries consist of a word $w \in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$, to which the oracle returns the output $L(w) \in 2$; equivalence queries consist of a hypothesis GKAT automaton H, to which the oracle responds *yes*, if H accepts L, and *no* otherwise, providing a counterexample $z \in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$ in the symmetric difference of L and the language accepted by H.

An observation table in GL^* consists of two parts: a top part, with rows indexed by a finite set $S \subseteq (\mathrm{At} \cdot \Sigma)^*$; and a bottom-part, with rows ranging over $S \cdot \mathrm{At} \cdot \Sigma$. Columns range over a finite set $E \subseteq (\mathrm{At}\cdot\Sigma)^*\cdot\mathrm{At}$. The entry of the observation table at row t and column e, denoted by $row(t)(e)$, is given by $L(te) \in 2$. We refer to a table by $T = (S, E, row)$ and leave the deterministic language L implicit.

Given an observation table T, we construct a GKAT automaton $m(T) = (X, \delta, x)$, where $X = \{row(s) \mid s \in S\}$ is a finite set of states; $x = row(\varepsilon)$ is the initial state; and $\delta : X \to (2 + \Sigma \times X)^{\mathrm{At}}$ is the transition function which evaluates $\delta(row(s))(\alpha)$ to $(p, row(s\alpha p))$, if there exists an $e \in E$ with $row(s\alpha p)(e) = 1$; to 1, if $row(s)(\alpha) = 1$; and to 0, otherwise.

Most of the properties a table needs to satisfy such that the hypothesis $m(T)$ is well-defined are guaranteed by the construction of Algorithm 2, since L is deterministic. We only have to verify that the table is *closed*, that is, for all $t \in S \cdot \mathrm{At} \cdot \Sigma$ with $row(t)(e) = 1$ for some $e \in E$, there exists some $s \in S$ such that $row(t) = row(s)$. As in the case of L^*, the algorithm incrementally updates the table until closedness is guaranteed. It then constructs a well-defined hypothesis, and poses an equivalence query to the teacher. If the oracle replies *yes*, the algorithm terminates, and if the response is *no*, it adds the suffixes [10] of a counterexample $z \in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$ to E.

The differences between GL^* and L^* (instantiated for $A = \mathrm{At} \cdot \Sigma$ and $B = 2^{\mathrm{At}}$) are essentially a consequence of currying. In the former case, the set E contains elements of type $(\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$, and the table is filled with booleans in 2; in the latter case, the set E contains elements of type $(\mathrm{At} \cdot \Sigma)^*$, and the table is filled with functions $\mathrm{At} \to 2$. This, however, does not mean that GL^* is merely a shift in perspective: its new types induce independent definitions, and termination needs to be established with novel correctness proofs (Section 5). A thorough comparison with L^* is given in Section 6.

2.2.1 Example of execution

We now execute Algorithm 2 for the target language (1). Initially, $S = \{\varepsilon\}$ and $E = \mathrm{At}$. We build the observation table in Figure 2a. Since the bottom row indexed by $\bar{b}q$ contains a non-zero entry and differs

[9] For instance, the entries of the row indexed by bq in Figure 1d must all be zero, since the row indexed by bp admits a non-zero entry.

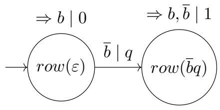
[10] The set $\mathtt{suf}(z)$ of suffixes for $z \in A^* \cdot B$ is defined by $\mathtt{suf}(wb) = \{vb \mid v \in \mathtt{suf}(w)\}$.

	b	$\bar{b}$
ε	0	0
bp	0	0
bq	0	0
$\bar{b}p$	0	0
$\bar{b}q$	1	1

(a)

	b	$\bar{b}$
ε	0	0
$\bar{b}q$	1	1
bp	0	0
bq	0	0
$\bar{b}p$	0	0
$\bar{b}qbp$	0	0
$\bar{b}qbq$	0	0
$\bar{b}q\bar{b}p$	0	0
$\bar{b}q\bar{b}q$	0	0

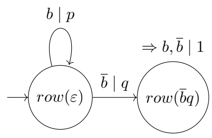
(b)



(c)

	b	$\bar{b}$	$bp\bar{b}qb$	$\bar{b}qb$
ε	0	0	1	1
$\bar{b}q$	1	1	0	0
bp	0	0	1	1
bq	0	0	0	0
$\bar{b}p$	0	0	0	0
$\bar{b}qbp$	0	0	0	0
$\bar{b}qbq$	0	0	0	0
$\bar{b}q\bar{b}p$	0	0	0	0
$\bar{b}q\bar{b}q$	0	0	0	0

(d)



(e)

Fig. 2. An example run of GL^* for the target language $[\![(\texttt{while}\ b\ \texttt{do}\ p); q]\!]$.

$$0 \equiv \texttt{false} \qquad 1 \equiv \texttt{true} \qquad t \equiv t \qquad b \cdot c \equiv b\ \texttt{and}\ c \qquad b + c \equiv b\ \texttt{or}\ c \qquad \bar{b} \equiv \texttt{not}\ b$$
$$p \equiv \texttt{do}\ p \qquad b \equiv \texttt{assert}\ b \qquad e \cdot f \equiv e; f \qquad e^{(b)} \equiv \texttt{while}\ b\ \texttt{do}\ e \qquad e +_b f \equiv \texttt{if}\ b\ \texttt{then}\ e\ \texttt{else}\ f$$

Fig. 3. Identifying GKAT expressions with imperative programs.

from all upper rows (in this case, only the row indexed by ε), the table is not closed. We resolve the closedness defect by adding $\bar{b}q$ to S. The observation table (Figure 2b) is now closed. Note that the row indexed by $\bar{b}q$ indicates that the words $\bar{b}qb$ and $\bar{b}q\bar{b}$ are accepted. Since we know the target language is deterministic, the last four rows of the table can be filled with zeroes, without performing any membership queries. From Figure 2b we derive the hypothesis depicted in Figure 2c. Next, we pose an equivalence query, to which the oracle replies *no* and provides us with the counterexample $z = bp\bar{b}qb$, which is in the language (1), but not accepted by the hypothesis. We respond to the counterexample by adding its suffixes $bp\bar{b}qb$, $\bar{b}qb$ and b to E. The resulting observation table is depicted in Figure 2d. The table is closed, since the only non-zero bottom row is the one indexed by bp, which coincides with the upper row indexed by ε. Since the row indexed by bp has a non-zero entry, the row indexed by bq can automatically be filled with zeroes. We derive from Figure 2d the automaton in Figure 2e. Finally, we pose an equivalence query, to which the oracle replies *yes*.

3 Preliminaries

This section introduces the syntax and semantics of GKAT, an abstract imperative programming language with uninterpreted actions. For most parts, we follow the relevant bits of the original presentation in [37].

3.1 Syntax

The syntax of GKAT is inductively built from disjoint non-empty sets of *primitive tests*, T, and *actions*, Σ. In a first step, one generates from T a set of Boolean expressions, BExp. In a second step, the set is extended with Σ, to the full set of GKAT expressions, Exp:

$$b, c, d \in \text{BExp} ::= 0 \mid 1 \mid t \in T \mid b \cdot c \mid b + c \mid \bar{b}$$
$$e, f, g \in \text{Exp} ::= p \in \Sigma \mid b \in \text{BExp} \mid e \cdot f \mid e +_b f \mid e^{(b)}$$

By a slight abuse of notation, we will sometimes write ef for $e \cdot f$ and keep parenthesis implicit, e.g. $bc + d$ should be read as $(b \cdot c) + d$.

It is natural to view GKAT expressions as uninterpreted imperative programs. Under this view, one makes the identifications depicted in Figure 3.

Readers familiar with KAT will notice that the grammar for GKAT is similar to the one of KAT. It

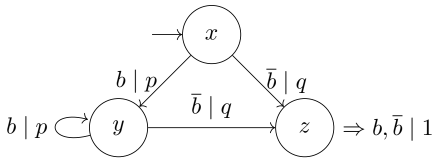


Fig. 4. The Thompson-automaton $\mathscr{X}_{p^{(b)}q}$ for $T = \{b\}$ and $\Sigma = \{p, q\}$.

differs in that GKAT replaces KAT's union $(+)$ with the guarded union $(+_b)$, and KAT's iteration (e^*) with the guarded iteration $(e^{(b)})$. GKAT's expressions can be encoded within KAT's grammar via the standard embedding that maps a conditional $e +_b f$ to $be + \overline{b}f$, and a while-loop $e^{(b)}$ to $(be)^*\overline{b}$.

3.2 Semantics: Language Model

In this section, we introduce the language semantics of GKAT, which assigns to a program the traces it could produce once executed. Intuitively, an execution trace is a string of the shape $\alpha_0 p_1 \alpha_1 ... p_n \alpha_n$. It can be thought of as a sequence of states α_i a system is in at point i in time, beginning with α_0 and ending in α_n, intertwined with actions p_i that transition from the state α_{i-1} to the state α_i.

More formally, let $\equiv_{\mathrm{BA}}$ denote the equivalence relation between Boolean expressions induced by the Boolean algebra axioms. The quotient $\mathrm{BExp}/_{\equiv_{\mathrm{BA}}}$, that is, the free Boolean algebra on generators T, admits a natural preorder $\leq$ defined by $b \leq c \Leftrightarrow b + c \equiv_{\mathrm{BA}} c$. The minimal nonzero elements with respect to this order are called *atoms*, the set of which is denoted by At. If $T = \{t_1, ..., t_n\}$ is finite, an atom $\alpha \in \mathrm{At}$ is of the form $\alpha = c_1 \cdot ... \cdot c_n$ with $c_i \in \{t_i, \overline{t_i}\}$.

A *guarded string* is an element of the set $\mathrm{GS} := \mathrm{At} \cdot (\Sigma \cdot \mathrm{At})^*$, or equivalently, $(\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$. The set of guarded strings without terminating atom is $\mathrm{GS}^- := (\mathrm{At} \cdot \Sigma)^*$.

A guarded string language $L \subseteq \mathrm{GS}$ is *deterministic* [37, Def. 2.2], if, whenever $\alpha_1 p_1 ... \alpha_{n-1} p_{n-1} \alpha_n v \in L$ and $\alpha_1 q_1 ... \alpha_{n-1} q_{n-1} \alpha_n w \in L$, then $p_i = q_i$ for all $1 \leq i \leq n-1$, and either $v = w = \varepsilon$, or $v = p_n v'$ and $w = q_n w'$ with $p_n = q_n$. The set of deterministic guarded string languages is denoted by $\mathscr{L}$.

Guarded strings can be partially composed via the *fusion product* defined by $v\alpha \diamond \beta w := v\alpha w$, if $\alpha = \beta$, and undefined otherwise. The partial product lifts to a total function on guarded languages by $L \diamond K := \{v \diamond w \mid v \in L, w \in K\}$. The n-th power of a guarded language is inductively defined by $L^0 := \mathrm{At}$ and $L^{n+1} := L^n \diamond L$. For $B \subseteq \mathrm{At}$ and $\overline{B} := \mathrm{At} \setminus B$, the guarded sum and the guarded iteration of languages are given by

$$L +_B K := (B \diamond L) \cup (\overline{B} \diamond K) \qquad L^{(B)} := \cup_{n \geq 0} (B \diamond L)^n \diamond \overline{B}.$$

The *language model* of GKAT is given by the semantic function $[\![-]\!] : \mathrm{Exp} \to \mathscr{P}(\mathrm{GS})$, which is inductively defined as follows:

$$[\![p]\!] := \{\alpha p \beta \mid \alpha, \beta \in \mathrm{At}\} \qquad [\![b]\!] := \{\alpha \in \mathrm{At} \mid \alpha \leq b\}$$
$$[\![e \cdot f]\!] := [\![e]\!] \diamond [\![f]\!] \qquad [\![e +_b f]\!] := [\![e]\!] +_{[\![b]\!]} [\![f]\!] \qquad [\![e^{(b)}]\!] := [\![e]\!]^{([\![b]\!])}.$$

Equivalently, the language semantics of GKAT can be constructed by post-composing the embedding of GKAT expressions into KAT expressions with the semantics of KAT.

The guarded string language $[\![e]\!]$ accepted by a GKAT program e is deterministic.

Example 3.1 Let the sets of primitive tests and actions be defined by $T := \{b\}$ and $\Sigma := \{p, q\}$, respectively. Then there exist only two atoms, $\mathrm{At} = \{b, \overline{b}\}$. The language model assigns to the program $p^{(b)}q \equiv (\texttt{while } b \texttt{ do } p); q$ the guarded deterministic language (1).

3.3 Semantics: Automata Model

In this section, we introduce the automata model of GKAT, the central subject of this paper. As before, we assume two finite sets of tests T and actions Σ, the former of which induces a finite set of atoms, At.

Let G be the functor on the category of sets which is defined on objects by $GX = (2 + \Sigma \times X)^{\mathrm{At}}$, where $2 = \{0, 1\}$ is the two-element set, and on morphisms in the usual way. A G-*coalgebra* consists of a pair $\mathscr{X} = (X, \delta)$, where X is a set called *state-space* and $\delta : X \to GX$ is a function called *transition map*. A G-coalgebra *homomorphism* $f : (X, \delta^X) \to (Y, \delta^Y)$ is a function $f : X \to Y$ that commutes with the transition maps, $\delta^Y \circ f = Gf \circ \delta^X$. A G-*automaton* is a G-coalgebra $\mathscr{X}$ with a designated initial state $x \in X$. A homomorphism $f : (\mathscr{X}, x) \to (\mathscr{Y}, y)$ between G-automata is a homomorphism between the underlying G-coalgebras that maps initial state to initial state, $f(x) = y$.

For each state $x \in X$, given an input $\alpha \in \mathrm{At}$, a G-coalgebra either i) halts and accepts, that is, satisfies $\delta(x)(\alpha) = 1$; ii) halts and rejects, that is, satisfies $\delta(x)(\alpha) = 0$; or iii) produces an output p and moves to a new state y, that is, satisfies $\delta(x)(\alpha) = (p, y)$. Intuitively, for each state $x \in X$, a guarded string $\alpha_0 p_1 \alpha_1 ... p_n \alpha_n$ is accepted, if the G-coalgebra in state x produces the output $p_1 ... p_n$, halts and accepts. Formally, one defines a function $[\![-]\!] : X \to \mathscr{P}(\mathrm{GS})$ as follows:

$$\alpha \in [\![x]\!] :\Leftrightarrow \delta(x)(\alpha) = 1; \qquad \alpha p w \in [\![x]\!] :\Leftrightarrow \exists y \in X : \delta(x)(\alpha) = (p, y) \text{ and } w \in [\![y]\!]. \tag{2}$$

A G-coalgebra is *observable*, if the function $[\![-]\!]$ is injective.

A guarded string $w \in \mathrm{GS}$ is *accepted* by a state $x \in X$, if $w \in [\![x]\!]$. The language accepted by a G-automaton, $[\![\mathscr{X}]\!]$, is the language accepted by its initial state. Every language accepted by a G-automaton satisfies the determinacy property [37, Thm. 5.8]. Conversely, one can equip the set of deterministic languages with a G-coalgebra structure $(\mathscr{L}, \delta^{\mathscr{L}})$ defined by

$$\delta^{\mathscr{L}}(L)(\alpha) = \begin{cases} (p, (\alpha p)^{-1} L) & \text{if } (\alpha p)^{-1} L \neq \emptyset \\ 1 & \text{if } \alpha \in L \\ 0 & \text{otherwise} \end{cases},$$

where $(\alpha p)^{-1} L = \{ w \in \mathrm{GS} \mid \alpha p w \in L \}$. Since $[\![L]\!] = L$ for any $L \in \mathscr{L}$ [37, Thm. 5.8], every deterministic language can thus be recognized by a G-automaton with possibly infinitely many states.

A G-coalgebra (X, δ) is *normal*, if it only transitions to *live* states, that is, $\delta(x)(\alpha) = (p, y)$ implies $[\![y]\!] \neq \emptyset$, for all $x, y \in X$. For any G-automaton $\mathscr{X}$ one can construct a language equivalent normal G-automaton $\widehat{\mathscr{X}}$ [37, Lem. 5.6]. If $\mathscr{X}$ is normal, the function $[\![-]\!] : X \to \mathscr{P}(\mathrm{GS})$ is the unique coalgebra homomorphism $[\![-]\!] : (X, \delta) \to (\mathscr{L}, \delta^{\mathscr{L}})$ [37, Thm. 5.8].

Two states $x, y \in X$ of a normal coalgebra accept the same language, $[\![x]\!] = [\![y]\!]$, if and only if they are *bisimilar*, $x \simeq y$, that is, there exists a binary relation $R \subseteq X \times X$, such that, if xRy, then it holds:

- if $\delta(x)(\alpha) \in 2$, then $\delta(y)(\alpha) = \delta(x)(\alpha)$; and
- if $\delta(x)(\alpha) = (p, x')$, then $\delta(y)(\alpha) = (p, y')$ and $x' R y'$ for some $y' \in X$.

Bisimilarity is a symmetric relation and can be extended to two coalgebras by constructing a coalgebra that has the disjoint union of their state-spaces as state-space.

Using a construction that is reminiscent of Thompson's construction for regular expressions [39], it is possible to efficiently interpret a GKAT expression e as an automaton $\mathscr{X}_e$ that accepts the same language [37]. Alternatively, one can mirror [37] Kozen's syntactic form of Brzozowski's derivatives for KAT [25].

Example 3.2 The Thompson-automaton assigned to the expression $p^{(b)} q \equiv (\texttt{while } b \texttt{ do } p); q$ is depicted in Figure 4. It is normal, but not observable, since the states x and y are bisimilar, $x \simeq y$, thus accept the same language, $[\![x]\!] = [\![y]\!]$. Moreover, it is language equivalent to the expression by which it is generated, that is, it satisfies $[\![\mathscr{X}_{p^{(b)} q}]\!] = [\![p^{(b)} q]\!]$.

4 The minimal representation $m(\mathscr{X})$

The automaton $\mathscr{X}_e$ assigned to an expression e by the Thompson construction is not always the most efficient representation of the language $[\![e]\!]$. For instance, as seen in Theorem 3.2, the Thompson-automaton

$\mathscr{X}_{p^{(b)}q}$ in Figure 4 contains redundant structure, since its states x and y exhibit the same behaviour. In this section, we show that any G-automaton $\mathscr{X}$ admits an equivalent *minimal* representation, $m(\mathscr{X})$.

4.1 Reachability

We begin by formally defining what it means for a state of a G-automaton to be reachable, and show that restricting an automaton to its reachable states preserves important invariants.

Definition 4.1 Let (X, δ) be a G-coalgebra. We write $\to\, \subseteq X \times \mathrm{GS}^- \times X$ for the smallest relation satisfying:

$$\frac{}{x \xrightarrow{\varepsilon} x} \qquad \frac{\delta(x)(\alpha) = (p, y)}{x \xrightarrow{\alpha p} y} \qquad \frac{x \xrightarrow{\alpha_1 p_1 \ldots \alpha_{n-1} p_{n-1}} y \quad , \quad y \xrightarrow{\alpha_n p_n} z}{x \xrightarrow{\alpha_1 p_1 \ldots \alpha_n p_n} z}. \tag{3}$$

The states *reachable* from $x \in X$ are $r(x) := \{y \in X \mid \exists w \in \mathrm{GS}^- : x \xrightarrow{w} y\}$, and their *witnesses* are $R(x) := \{w \in \mathrm{GS}^- \mid \exists x_w \in X : x \xrightarrow{w} x_w\}$.

The following result shows that a state reached by a word is uniquely defined.

Lemma 4.2 *If $x \xrightarrow{w} x_w^1$ and $x \xrightarrow{w} x_w^2$, then $x_w^1 = x_w^2$.*

It is not hard to see that the subset $r(x)$ of reachable states is δ-invariant, i.e. if $y \in r(x)$ and $\delta(y)(\alpha) = (p, z)$, then $z \in r(x)$. We denote the well-defined sub-automaton one obtains by restricting to the states reachable from an initial state as $r(\mathscr{X})$, and call an automaton *reachable*, if $\mathscr{X} = r(\mathscr{X})$. Following [42, Def. 15], we call a normal, reachable, and observable automaton *minimal*.

The set $R(x)$ of words witnessing the reachability of states in $\mathscr{X} = (X, \delta, x)$ can be equipped with a G-automaton structure $R(\mathscr{X}) := (R(x), \partial, \varepsilon)$, where $\partial(w)(\alpha) = (p, w\alpha p)$, if $\delta(x_w)(\alpha) = (p, x_{w\alpha p})$ for some $x_{w\alpha p} \in X$, and $\partial(w)(\alpha) = \delta(x_w)(\alpha)$ otherwise. The automaton $r(\mathscr{X})$ can then be recovered as the image of the automata homomorphism $f : R(\mathscr{X}) \to \mathscr{X}$ defined by $f(w) = x_w$. In other words, there exists an epi-mono factorization $R(\mathscr{X}) \twoheadrightarrow r(\mathscr{X}) \hookrightarrow \mathscr{X}$.

We conclude with a list of important properties preserved by restricting an automaton to its reachable states. *Well-nestedness* and *coequations*, in particular, the *nesting coequation*, have been introduced in [37] and [36], respectively. We refer the reader to the original papers for formal definitions, and to Section 8 for a high-level comparison.

Proposition 4.3 *Let $\mathscr{X}$ be a G-automaton, then $r(\mathscr{X})$ is well-nested, normal, or satisfies the nesting coequation, whenever $\mathscr{X}$ does. Moreover, $r(\mathscr{X})$ accepts the same language as $\mathscr{X}$.*

4.2 Minimality

Recall that the state-space of the minimal DFA for a regular language consists of the equivalence classes of the so-called Myhill-Nerode equivalence relation [32].

Similarly, we define the state-space of the minimization of a GKAT automaton $\mathscr{X}$ as the equivalence classes of the equivalence relation $\equiv_{[\![\mathscr{X}]\!]}$ on GS^- defined for any guarded string language $L \subseteq \mathrm{GS}$ by:

$$v \equiv_L w :\Leftrightarrow \forall u \in \mathrm{GS} : vu \in L \text{ if(f) } wu \in L. \tag{4}$$

Let $v^{-1}L = \{u \in \mathrm{GS} \mid vu \in L\}$, then two words v, w are equivalent with respect to $\equiv_L$ if(f) their derivatives $v^{-1}L$ and $w^{-1}L$ coincide.

Definition 4.4 The *minimization* of a G-automaton $\mathscr{X} = (X, \delta, x)$ is $m(\mathscr{X}) := (\{w^{-1}[\![\mathscr{X}]\!] \mid w \in R(x)\}, \partial, [\![\mathscr{X}]\!])$ with

$$\partial(L)(\alpha) := \begin{cases} (p, (\alpha p)^{-1}L) & \text{if } (\alpha p)^{-1}L \neq \emptyset \\ 1 & \text{if } \alpha \in L \\ 0 & \text{otherwise} \end{cases}, \tag{5}$$

for $L \in \{w^{-1}[\![\mathscr{X}]\!] \mid w \in R(x)\}$.

A few remarks on the well-definedness of above definition are in order. The language accepted by a G-automaton is deterministic, and taking the derivative of a language preserves its deterministic nature. Thus only one of the three cases in (5) occurs. Since $\varepsilon \in R(x)$ and $\varepsilon^{-1}L = L$, the initial state of the minimization is well-defined. Transitioning to a new state is well-defined since $v^{-1}(w^{-1}L) = (wv)^{-1}L$.

It is not hard to see that on a high-level the minimization can be recovered as the image of the final automata homomorphism $[\![-]\!] : R(\mathscr{X}) \to \mathcal{L}$, which, as one verifies, satisfies $[\![w]\!]_{R(\mathscr{X})} = w^{-1}[\![\mathscr{X}]\!]$. In other words, there exists an epi-mono factorization $R(\mathscr{X}) \twoheadrightarrow m(\mathscr{X}) \hookrightarrow \mathcal{L}$.

4.2.1 Properties of $m(\mathscr{X})$

In this section we prove properties of $m(\mathscr{X})$, which one would expect to hold by a minimization construction. We begin by showing that minimizing a normal automaton results in a reachable acceptor.

Lemma 4.5 *Let $\mathscr{X}$ be a normal G-automaton with initial state $x \in X$. Then $[\![\mathscr{X}]\!] \xrightarrow{w} w^{-1}[\![\mathscr{X}]\!]$ in $m(\mathscr{X})$ for all $w \in R(x)$. In particular, $m(\mathscr{X})$ is reachable.*

The next result proves that minimizing an automaton preserves its language semantics.

Lemma 4.6 *Let $\mathscr{X}$ be a G-automaton, then $[\![L]\!] = L$ for all L in $m(\mathscr{X})$. In particular, $[\![m(\mathscr{X})]\!] = [\![\mathscr{X}]\!]$.*

An immediate consequence of above statement is that the states of the minimization can be distinguished by their observable behaviour, that is, different states accept different languages. Another implication of Theorem 4.6 is the normality of the minimization: all states are *live*.

Corollary 4.7 *Let $\mathscr{X}$ be a G-automaton, then $m(\mathscr{X})$ is normal and observable.*

Since $m(\mathscr{X})$ is normal, reachable, and observable, if $\mathscr{X}$ is normal, it is, by our definition, *minimal* (cf. [42, Def. 15]). Its size-minimality among normal automata language equivalent to $\mathscr{X}$ can be derived from the abstract definition, cf. Theorem 4.12.

4.2.2 Identifying $m(\mathscr{X})$

In this section, we identify the minimization of a normal G-automaton with an alternative, but equivalent, construction. In consequence, we are able to derive that the minimization of a normal automaton is size-minimal among language equivalent normal automata and preserves the nesting coequation. We begin by observing its universality in the following sense.

Proposition 4.8 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata with $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$, and $y \in Y$ the initial state of $\mathscr{Y}$. Then $\pi : r(\mathscr{Y}) \to m(\mathscr{X})$ with $\pi(z) = w_z^{-1}[\![\mathscr{X}]\!]$, for $y \xrightarrow{w_z} z$ in $\mathscr{Y}$, is a (surjective) G-automata homomorphism, uniquely defined.*

The next result shows that the minimization of a normal G-automaton is isomorphic to the automaton that arises by identifying semantically equivalent pairs among reachable states.

Lemma 4.9 *Let $\mathscr{X}$ be a normal G-automaton with initial state $x \in X$ and $\pi : r(\mathscr{X}) \twoheadrightarrow m(\mathscr{X})$ as in Theorem 4.8, then $y \simeq z$ if(f) $\pi(y) = \pi(z)$ for all $y, z \in r(x)$. Consequently, $m(\mathscr{X})$ is isomorphic to $r(\mathscr{X})/\simeq$.*

$$\begin{tikzcd}
R(\mathscr{X}) \arrow[r, two heads] \arrow[dd, two heads] & r(\mathscr{X}) \arrow[d, hook] \arrow[ddl, dashed, two heads, "\pi"] \\
& \mathscr{X} \arrow[d] \\
m(\mathscr{X}) \arrow[r, hook] & \mathcal{L}
\end{tikzcd}$$

(a) The morphism π as unique diagonal.

$$\begin{tikzcd}
e \arrow[d] & f \arrow[d] \\
\mathscr{X}_e \arrow[d] & \mathscr{X}_e \arrow[d] \\
\widehat{\mathscr{X}_e} \arrow[d] & \widehat{\mathscr{X}_f} \arrow[d] \\
m(\widehat{\mathscr{X}_e}) \arrow[r, leftrightarrow, "\cong"] & m(\widehat{\mathscr{X}_f})
\end{tikzcd}$$

(b) $[\![e]\!] = [\![f]\!]$ if(f) $m(\widehat{\mathscr{X}_e})$ and $m(\widehat{\mathscr{X}_f})$ are isomorphic.

Fig. 5. A high-level view of the notions introduced in Section 4.2.2.

On a high level, the automata homomorphism π can be recovered as the unique (surjective) diagonal making the diagram in Figure 5a commute.

In Theorem 4.3 it was noted that the reachable subautomaton $r(\mathscr{X})$ satisfies the nesting coequation, whenever $\mathscr{X}$ does. By Theorem 4.8 there exists an epimorphism $\pi : r(\mathscr{X}) \twoheadrightarrow m(\mathscr{X})$, if $\mathscr{X}$ is normal. Since coalgebras satisfying a coequation form a covariety, which is closed under homomorphic images [8,36], we thus can deduce the following result.

Corollary 4.10 *Let $\mathscr{X}$ be a normal G-automaton, then $m(\mathscr{X})$ satisfies the nesting coequation, whenever $\mathscr{X}$ does.*

We continue with the observation that two normal G-automata are language equivalent if and only if their minimizations are isomorphic. As depicted in Figure 5b, this implies that two expressions e and f are language equivalent if and only if the minimizations of their normalized Thompson automata are isomorphic. A similar idea occurs in Kozen's completeness proof for Kleene Algebra [22, Theorem 19].

Corollary 4.11 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata, then $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$ if(f) $m(\mathscr{X}) \cong m(\mathscr{Y})$.*

We conclude with the size-minimality of the minimization of a normal automaton among language equivalent normal automata.

Corollary 4.12 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata with $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$. Then $|m(\mathscr{X})| \leq |\mathscr{Y}|$, where $|m(\mathscr{X})| = |\mathscr{Y}|$ if(f) $m(\mathscr{X}) \cong \mathscr{Y}$.*

5 Learning $m(\mathscr{X})$

In this section we formally investigate the correctness of GL^* (Algorithm 2). Our main result is Theorem 5.9, which shows that if the oracle is instantiated with a deterministic language accepted by a finite normal G-automaton $\mathscr{X}$, then GL^* terminates with a hypothesis isomorphic to $m(\mathscr{X})$.

For calculations, it will be convenient to use the following definition of an observation table. One can show that if the oracle is instantiated with a finite normal G-automaton, then one has a well-defined observation table at every step.

Definition 5.1 An *observation table* $T = (S, E, row)$ consists of subsets $S \subseteq \mathrm{GS}^-$, $E \subseteq \mathrm{GS}$ and a function $row : S \cup S \cdot (\mathrm{At} \cdot \Sigma) \to 2^E$, such that:

- $\varepsilon \in S$ and $\mathrm{At} \subseteq E$
- $\alpha p e \in E$ implies $e \in E$ (suffix-closed)
- $s \alpha p \in S$ implies $s \in S$ (prefix-closed)
- $s \neq t$ implies $row(s) \neq row(t)$ for $s, t \in S$
- $\varepsilon \neq s \in S$ implies $row(s)(e) = 1$ for some $e \in E$
- $row(s\alpha p)(e) = row(s)(\alpha p e)$, if $\alpha p e \in E$

Not every table induces a well-defined G-automaton. To ensure correctness, we have to restrict ourselves to a subclass of tables that satisfies two important properties. We call an observation table *deterministic* if the guarded string language $row(s) \subseteq \mathrm{GS}$ is deterministic for all $s \in S$. An observation table is *closed*, if for all $t \in S \cdot (\mathrm{At} \cdot \Sigma)$ with $row(t)(e) = 1$ for some $e \in E$, there exists an $s \in S$ such that $row(s) = row(t)$.

Definition 5.2 Given a closed deterministic observation table $T = (S, E, row)$, let $m(T) := (\{row(s) \mid s \in S\}, \delta, row(\varepsilon))$ be the G-automaton with

$$\delta(L)(\alpha) = \begin{cases} (p, (\alpha p)^{-1}L) & \text{if } (\alpha p)^{-1}L \neq \emptyset \\ 1 & \text{if } \alpha \in L \\ 0 & \text{otherwise} \end{cases}, \quad (6)$$

where $L \in \{row(s) \mid s \in S\}$ and $(\alpha p)^{-1}row(s) = row(s\alpha p)$.

A few remarks on the well-definedness of above definition are in order. By Theorem 5.1 the upper-rows of an observation table are disjoint. Since T is deterministic, precisely one of the three cases in (6) occurs. If $(\alpha p)^{-1}row(s)$ is non-empty, there exists, because T is closed, some $t \in S$ with $(\alpha p)^{-1}row(s) = row(t)$. This shows that $m(T)$ is closed under transitions.

5.1 Properties of $m(T)$

In what follows, let T be a closed deterministic observation table, unless states otherwise. We will establish a few basic properties of $m(T)$. First, we observe its reachability, which is implied by a stronger statement.

Lemma 5.3 *It holds $row(s) \xrightarrow{t} row(st)$ in $m(T)$ for all $s \in S$ and $t \in \mathrm{GS}^-$, such that $st \in S$. In particular, $m(T)$ is reachable.*

We call a G-automaton $(\mathscr{Y}, y)$ *consistent with* T, if $S \subseteq R(y)$ and $[\![y_s]\!](e) = row(s)(e)$ for all $s \in S$, $e \in E$, and $y_s \in Y$ with $y \xrightarrow{s} y_s$. By Theorem 5.3, the automaton $m(T)$ is consistent with T if and only if $[\![row(s)]\!](e) = row(s)(e)$ for all $s \in S$ and $e \in E$. The consistency of $m(T)$ with T should not be confused with the consistency of T itself. Both terminologies appear frequently in the literature [3]. We show that $m(T)$ is not only consistent with T, but has in fact the fewest number of states among all automata consistent with T.

Lemma 5.4 *$m(T)$ is size-minimal among automata consistent with T.*

From the consistency of $m(T)$ with T it is straightforward to derive its normality and observability.

Lemma 5.5 *$m(T)$ is normal and observable.*

5.2 Relationship between $m(T)$ and $m(\mathscr{X})$

We will next deduce the correctness of GL^*, that is, its termination with an automaton isomorphic to $m(\mathscr{X})$, if the teacher is instantiated with the language accepted by a finite normal automaton $\mathscr{X}$.

In a first step we establish that any hypothesis admits an injective function from its state-space into the state-space of $m(\mathscr{X})$. The result below does not necessarily require the observation table to be deterministic or closed.

Lemma 5.6 *Let $T = (S, E, row)$ be an observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$, and let $x \in X$ be the initial state of $\mathscr{X}$. Then $\pi : \{row(s) \mid s \in S\} \to \{w^{-1}[\![\mathscr{X}]\!] \mid w \in R(x)\}$, $row(s) \mapsto s^{-1}[\![\mathscr{X}]\!]$ is a well-defined injective function.*

If the algorithm terminates with a hypothesis $m(T)$, the latter is, by definition, language equivalent to $\mathscr{X}$, and thus to the minimization $m(\mathscr{X})$, by Theorem 4.6. The next result implies a stronger statement: in case of termination, the hypothesis $m(T)$ is *isomorphic* to $m(\mathscr{X})$, via the function π of Theorem 5.6.

Proposition 5.7 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let π be the injection of Theorem 5.6, and $\mathscr{X}$ normal. The following are equivalent:*

(i) $\pi : m(T) \simeq m(\mathscr{X})$ *is a G-automata isomorphism;*

(ii) $[\![m(T)]\!] = [\![m(\mathscr{X})]\!]$.

The main argument in the proof of Theorem 5.9 is the result below. It shows that if the oracle replies *no* to an equivalence query and provides us with a counterexample z, then the table extended with the suffixes of z can immediately be closed only if it is the first time such a situation occurs.

Proposition 5.8 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let $[\![m(T)]\!](z) \neq [\![\mathscr{X}]\!](z)$ for some $z \in \mathrm{GS}$, and $T' = (S, E \cup \mathtt{suf}(z), row')$ with $row'(t)(e) = [\![\mathscr{X}]\!](te)$. If T' is closed, then $row'(\varepsilon)(e) = 0$ for all $e \in E$, but $row'(\varepsilon)(z') = 1$ for some $z' \in \mathtt{suf}(z)$.*

In consequence, an infinite chain of negative equivalence queries and immediately closed extended tables is impossible. Since fixing a closedness defect increases the size of $m(T)$, which by Theorem 5.6 is bounded by the finite number of states in $m(\mathscr{X})$, we can deduce the correctness of Algorithm 2.

Theorem 5.9 *If Algorithm 2 is instantiated with the language accepted by a finite normal automaton $\mathscr{X}$, then it terminates with a hypothesis isomorphic to $m(\mathscr{X})$.*

6 Comparison with Moore automata

How are the minimal GKAT automaton (Figure 2e) and the minimal Moore automaton (Figure 1f) representing the language (1) related? Why should we learn the former, and not the latter? Are there optimizations for L^* that we could adapt for GL^*? Those are the questions this section seeks to answer.

6.1 Embedding of GKAT automata

Comparing the GKAT automaton in Figure 2e with the Moore automaton (with input $\mathrm{At} \cdot \Sigma$ and output 2^{At}, short *M-automaton*) in Figure 1f suggests that the latter can be recovered from the former by adding a sink-state with which halting transitions can be made explicit. The result below formalises this idea. The language semantics of Moore automata is defined as usual.

Lemma 6.1 *Given a G-automaton $\mathscr{X} = (X, \delta, x)$, let $f(\mathscr{X}) := (X + \{\star\}, \langle \partial, \varepsilon \rangle, x)$ be the M-automaton with*

$$\partial(x)(\alpha p) := \begin{cases} y & \text{if } x \in X,\ \delta(x)(\alpha) = (p, y) \\ \star & \text{otherwise} \end{cases} \qquad \varepsilon(x)(\alpha) := \begin{cases} 1 & \text{if } x \in X,\ \delta(x)(\alpha) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then $[\![x]\!]_{\mathscr{X}} = [\![x]\!]_{f(\mathscr{X})}$ for all $x \in X$, and $[\![\star]\!]_{f(\mathscr{X})} = \emptyset$. In particular, $[\![f(\mathscr{X})]\!]_{f(\mathscr{X})} = [\![\mathscr{X}]\!]_{\mathscr{X}}$.

As one would hope for, above construction maps, up to isomorphism, the minimal GKAT automaton $m(\mathscr{X})$ to the minimal Moore automaton accepting the same language as $\mathscr{X}$.

Corollary 6.2 *Let $\mathscr{X}$ be a normal G-automaton, then $f(m(\mathscr{X})) \cong m(f(\mathscr{X}))$ as M-automata.*

6.2 Complexity analysis

We now compare the worst-case complexities of L^* (Algorithm 1) and GL^* (Algorithm 2) for learning automata representations of GKAT programs e. We are mainly interested in a bound to the number of membership queries to $[\![e]\!]$. The example runs in Figure 1 and Figure 2 seem to indicate that with respect to this aspect, GL^* performs better than L^*. The result below confirms this intuition.

Proposition 6.3 *Algorithm 1 requires at most $O(a * (|\mathrm{At}| * b))$ many membership queries to $[\![e]\!]$ for learning a M-automaton representation of e, whereas Algorithm 2 requires at most $O(a * (|\mathrm{At}| + b))$ many membership queries to $[\![e]\!]$ for learning a G-automaton representation of e, for some*[11] *integers $a, b \in \mathbb{N}$.*

One can show that for all integers x, y greater than 2, the product $x * y$ is strictly greater than the sum $x + y$. Moreover, the difference between $x * y$ and $x + y$ increases with the sizes of x and y. The advantage of GL^* over L^* for learning deterministic guarded string languages in terms of membership queries thus increases with the size of the set At, which is exponential in the number of primitive tests, $\mathrm{At} \cong 2^T$. In applications to network verification, the number of tests, thus atoms, is typically quite large [2]. The difference between GL^* and L^* described in Theorem 6.3 is mainly due to a subtle play with the table indices, based on currying. It can be further increased by avoiding querying certain rows all together, taking into account the deterministic nature of the target language, as indicated in Section 2.2.1.

6.3 Optimized counterexamples

In this section we present an optimization of GL^* that is based on a subtle refinement of Theorem 5.8. We show that, while Algorithm 2 reacts to a negative equivalence query with counterexample $z \in \mathrm{GS}$ by adding columns for *all* suffixes in $\mathtt{suf}(z)$, it is in fact enough to add columns for a smaller subset of suffixes $\mathtt{suf}(z') \subseteq \mathtt{suf}(z)$, for some $z' \in \mathtt{suf}(z)$ of minimal length. Our approach is inspired by the optimized counterexample handling method of Rivest and Schapire for L^* [34].

Lemma 6.4 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let $[\![m(T)]\!](z) \neq [\![\mathscr{X}]\!](z)$ for some $z \in \mathrm{GS}$, and $z' := \min(A_z)$*[12]*. If $T' = (S, E \cup \mathtt{suf}(z'), row')$ with $row'(t)(e) = [\![\mathscr{X}]\!](te)$ is closed, then $row'(\varepsilon)(e) = 0$ for all $e \in E$, but $row'(\varepsilon)(z') = 1$.*

Let z_0 be the shortest suffix of z and z_i the suffix of z of length $|z_{i-1}| + 1$. The suffix $\min(A_z)$ can easily be computed in at most $|\mathtt{suf}(z)| - 1$ steps: verify whether $z_i \in A_z$, beginning with z_0; if positive, break and set $\min(A_z) := z_i$, otherwise loop with z_{i+1}.

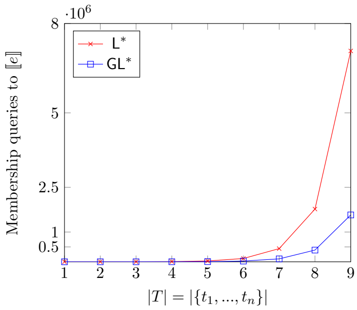
For example, if T is the closed table in Figure 2b with the corresponding hypothesis $m(T)$ in Figure 2c and counterexample $z = bp\bar{b}qb$, then $z' = \min(A_z) = \bar{b}qb$, since $b \not\in A_z$. Theorem 6.4 shows that, instead of adding columns for the two non-present suffixes $bp\bar{b}qb$ and $\bar{b}qb$ of z, it is sufficient to add only one column for the single non-present suffix $\bar{b}qb$ of z'. In this case, the counterexample z is relatively short, thus the number of avoided columns small; in general, however, the advantage can be more significant.

7 Implementation

We have implemented both GL^* and L^* in OCaml; the code is available on GitHub[13]. The implementation allows one to compare, for any GKAT expression $e \in \mathrm{Exp}_{\Sigma,T}$, the number of membership queries to $[\![e]\!]$ required by GL^* for learning a G-automaton representation of e, with the number of membership queries to $[\![e]\!]$ required by L^* for learning a M-automaton representation of e. For each run, we output, for both algorithms, a trace of the involved hypotheses as tables in the `.csv` format and graphs in the `.dot` format, as well as an overview of the numbers of involved queries in the `.csv` format.

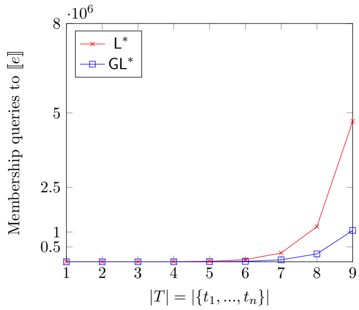
In Figure 6a we present the results for the expression $e = \mathtt{if}\ t_1\ \mathtt{then\ do}\ p_1\ \mathtt{else\ do}\ p_2$, the primitive actions $\Sigma = \{p_1, p_2, p_3\}$, and primitive tests $T = \{t_1, ..., t_n\}$ parametric in $n = 1, ..., 9$. We find that GL^* outperforms L^* for all choices of n. The difference in the number of membership queries increases with the size of n, as suggested by Theorem 6.3. For $n = 9$ the number of atoms is 2^9, resulting in an already relatively large number of queries for both algorithms. The picture is similar in Figure 6b, where we

[11] Let m be the maximum length of a counterexample and n the size of the minimal Moore automaton accepting $[\![e]\!]$, then $a = n * |\mathrm{At}| * |\Sigma|$ and $b = m * n$. As Figure 6 shows, GL^* can be more efficient than L^* even for small $|\mathrm{At}|$.
[12] $A_z := \{z' \in \mathtt{suf}(z) \mid z = v\alpha p z',\ row(\varepsilon) \xrightarrow{v} row(s_v),\ x \xrightarrow{s_v} x_{s_v},\ [\![row(s_v)]\!](\alpha p z') \neq [\![x_{s_v}]\!](\alpha p z')\}$
[13] https://github.com/zetzschest/gkat-automata-learning



$\|T\|$	GL*	L*
1	26	114
2	100	444
3	392	1.752
4	1.552	6.960
5	6.176	27.744
6	24.640	110.784
7	98.432	442.752
8	393.472	1.770.240
9	1.573.376	7.079.424

(a) $e = \texttt{if}\ t_1\ \texttt{then do}\ p_1\ \texttt{else do}\ p_2$



$\|T\|$	GL*	L*
1	36	78
2	102	300
3	330	1.176
4	1.170	4.656
5	4.386	18.528
6	16.962	73.920
7	66.690	295.296
8	264.450	1.180.416
9	1.053.186	4.720.128

(b) $e = (\texttt{while}\ t_1\ \texttt{do}\ p_1); \texttt{do}\ p_2$

Fig. 6. A comparison between GL^* and L^* with respect to membership queries.

choose the expression $e = (\texttt{while}\ t_1\ \texttt{do}\ p_1); \texttt{do}\ p_2$, the primitive actions $\Sigma = \{p_1, p_2\}$, and primitive tests $T = \{t_1, ..., t_n\}$ parametric in $n = 1, ..., 9$. Again, GL^* requires significantly less queries in all cases of n, and the difference increases with the size of n.

Our implementation generates an oracle for L^* from a GKAT expression e in the following way. First, we interpret e as a KAT expression $\iota(e)$ via the standard embedding of GKAT into KAT. Next, we generate from the latter a Moore automaton $\mathscr{X}_{\iota(e)}$ accepting $[\![e]\!]$, by using Kozen's syntactic Brzozowksi derivatives for KAT [25]. Finally, we answer an equivalence query from a Moore automaton $\mathscr{Y}$ by running a bisimulation between $\mathscr{X}_{\iota(e)}$ and $\mathscr{Y}$, similarly to [33, Fig. 1], and a membership query from $w\alpha \in \mathrm{GS}$ by returning the value of α at the output of the state in $\mathscr{X}_{\iota(e)}$ reached by w, that is, $[\![e]\!](w\alpha)$. A membership query from $w \in \mathrm{GS}^-$ is answered by querying $w\alpha \in \mathrm{GS}$ for all $\alpha \in \mathrm{At}$.

With the oracle for L^*, we can derive an oracle for GL^* as follows. Membership queries $w\alpha \in \mathrm{GS}$ are delegated and answered by the oracle for L^* as explained above. An equivalence query from a GKAT automaton $\mathscr{Y}$ is answered by posing an equivalence query to the oracle for L^* with the Moore automaton $f(\mathscr{Y})$ obtained via the embedding defined in Theorem 6.1. If the oracle for L^* replies with a counterexample $z \in \mathrm{GS}^-$, we extend z with an $\alpha \in \mathrm{At}$ such that $[\![\mathscr{Y}]\!](z\alpha) \neq [\![e]\!](z\alpha)$.

8 Related work

GKAT is a variation on KAT [26] that one obtains by restricting the union and iteration operations from KAT to guarded versions. While GKAT is less expressive than KAT, term equivalence is notably more efficiently decidable [37,26], making it a candidate for the foundations of network-programming [38,2,13]

GKAT automata appear in the literature already prior to [37], e.g. in the work of Kozen [27] under the name *strictly deterministic automata*. In the latter, Kozen states that GKAT automata correspond to a limited class of *automata with guarded strings (AGS)* [24], for which he gives determinization and minimization constructions. In a different paper [25] Kozen introduces a second definition of (deterministic) AGS as Moore automata, and states the difference to the definition of AGS in [24] is inessential.

Recently, a new perspective on the semantics and coalgebraic theory of GKAT has been given in terms of coequations [36,8]. Using the Thompson construction, it is possible to construct for every expression e a language equivalent automaton $\mathscr{X}_e$. In [27] it was shown that the inverse does generally not hold: there exists a GKAT automaton that is inequivalent to $\mathscr{X}_e$ for all expressions e. In consequence, [37] proposed a subclass of *well-nested* automata and showed that every finite well-nested automaton is bisimilar to $\mathscr{X}_e$ for some e. In [36] it was shown that well-nestedness is in fact too restrictive: there exists an automaton that is bisimilar to $\mathscr{X}_e$ for some e, but not well-nested. To capture the *full* class of automata exhibiting the behaviour of expressions, one has to extend the class of well-nested automata to the class of automata satisfying the *nesting coequation*, which forms a *covariety* [8].

Active automata learning is a technique used for deriving a model from a black-box by interacting with it via observations. The seminal algorithm L^*[3] learns deterministic finite automata, but since then has been extended to other classes of automata [4,1,30], including Moore automata. Typically, algorithms such as L^* are designed to output for a given language a unique minimal acceptor. Not all classes admit a canonical minimal acceptor, for instance, learning non-deterministic models is a challenge [10,6,44,43].

9 Discussion and future work

We have presented GL^*, an algorithm for learning the GKAT automaton representation of a black-box, by observing its behaviour via queries to an oracle. We have shown that for every normal GKAT automaton there exists a unique size-minimal normal automaton, accepting the same language: its minimization. We have identified the minimization with an alternative but equivalent construction, and derived its preservation of the nesting coequation. A central result showed that if the oracle in GL^* is instantiated with the language accepted by a finite normal automaton, then GL^* terminates with its minimization. A complexity analysis showed the advantage of GL^* over L^* for learning automata representations of GKAT programs in terms of membership queries. We discussed additional optimizations, and implemented GL^* and L^* in OCaml to compare their performances on example programs.

There are numerous directions in which the present work could be further explored. In Section 6.3 we introduced an optimization for GL^* which is inspired by Rivest and Schapire's counterexample handling method for L^* [34]. The *oberservation pack* algorithm for L^* [17] has successfully combined Rivest and Schapire's method with an efficient *discrimination tree* data structure [20]. The state-of-the-art *TTT*-algorithm [19] for L^* extends the former with discriminator finalization techniques. It thus is natural to ask whether for GL^* there exist similarly efficient data structures, potentially exploiting the deterministic nature of the languages accepted by GKAT automata.

While L^* has seen major improvements over the years and has inspired numerous variations for different types of transition systems, all approaches remain in common their focus on the *equivalence* of observations. The recently presented $\mathsf{L}^\sharp$ algorithm [41] takes a different perspective: it instead focuses on *apartness*, a constructive form of inequality. $\mathsf{L}^\sharp$ does not require data-structures such as observation tables or discrimination trees, instead operating directly on tree-shaped automata. It remains open whether a similar shift in perspective is feasible for GL^*.

There exist various domain-specific extensions of KAT (e.g. KAT+B! [14], NetKAT [2], ProbNetKAT [12]), and similar directions have been proposed for GKAT. In particular, it has been noted that GKAT is better fit for probabilistic domains than KAT, as it avoids mixing non-determinism with probabilities [38]. We expect that in the future, for such extensions of GKAT, there will be interest in developing the corresponding automata (learning) theories.

References

[1] Aarts, F. and F. Vaandrager, *Learning i/o automata*, in: *International Conference on Concurrency Theory*, pages 71–85, Springer (2010).

[2] Anderson, C. J., N. Foster, A. Guha, J.-B. Jeannin, D. Kozen, C. Schlesinger and D. Walker, *Netkat: Semantic foundations for networks*, Acm sigplan notices **49**, pages 113–126 (2014).

[3] Angluin, D., *Learning regular sets from queries and counterexamples*, Information and computation **75**, pages 87–106 (1987).
https://doi.org/10.1016/0890-5401(87)90052-6

[4] Angluin, D. and M. Csűrös, *Learning markov chains with variable memory length from noisy output*, in: *Proceedings of the tenth annual conference on Computational learning theory*, pages 298–308 (1997).

[5] Baltag, A., *A logic for coalgebraic simulation*, Electronic Notes in Theoretical Computer Science **33**, pages 42–60 (2000).

[6] Bollig, B., P. Habermehl, C. Kern and M. Leucker, *Angluin-style learning of nfa*, in: *Twenty-First International Joint Conference on Artificial Intelligence* (2009).

[7] Chalupar, G., S. Peherstorfer, E. Poll and J. De Ruiter, *Automated reverse engineering using lego®*, in: *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)* (2014).

[8] Dahlqvist, F. and T. Schmid, *How to write a coequation ((co) algebraic pearls)*, in: *9th Conference on Algebra and Coalgebra in Computer Science (CALCO 2021)*, Schloss Dagstuhl-Leibniz-Zentrum für Informatik (2021).

[9] De Ruiter, J. and E. Poll, *Protocol state fuzzing of {TLS} implementations*, in: *24th USENIX Security Symposium (USENIX Security 15)*, pages 193–206 (2015).

[10] Denis, F., A. Lemay and A. Terlutte, *Residual finite state automata*, in: *Annual Symposium on Theoretical Aspects of Computer Science*, pages 144–157, Springer (2001).

[11] Feamster, N., J. Rexford and E. Zegura, *The road to sdn: an intellectual history of programmable networks*, ACM SIGCOMM Computer Communication Review **44**, pages 87–98 (2014).

[12] Foster, N., D. Kozen, K. Mamouras, M. Reitblatt and A. Silva, *Probabilistic netkat*, in: *European Symposium on Programming*, pages 282–309, Springer (2016).

[13] Foster, N., D. Kozen, M. Milano, A. Silva and L. Thompson, *A coalgebraic decision procedure for netkat*, in: *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 343–355 (2015).

[14] Grathwohl, N. B. B., D. Kozen and K. Mamouras, *Kat+ b!*, in: *Proceedings of the joint meeting of the twenty-third eacsl annual conference on computer science logic (csl) and the twenty-ninth annual acm/ieee symposium on logic in computer science (lics)*, pages 1–10 (2014).

[15] Hagerer, A., H. Hungar, O. Niese and B. Steffen, *Model generation by moderated regular extrapolation*, in: *International Conference on Fundamental Approaches to Software Engineering*, pages 80–95, Springer (2002).

[16] Hesselink, W. H. and A. Thijs, *Fixpoint semantics and simulation*, Theoretical Computer Science **238**, pages 275–311 (2000).

[17] Howar, F., *Active learning of interface programs.*, Ph.D. thesis, Dortmund University of Technology (2012).

[18] Hughes, J. and B. Jacobs, *Simulations in coalgebra*, Theoretical Computer Science **327**, pages 71–108 (2004).

[19] Isberner, M., F. Howar and B. Steffen, *The TTT algorithm: a redundancy-free approach to active automata learning*, in: *International Conference on Runtime Verification*, pages 307–322, Springer (2014).

[20] Kearns, M. J., U. V. Vazirani and U. Vazirani, *An introduction to computational learning theory*, MIT press (1994).

[21] Kleene, S., *Representation of events in nerve nets and finite automata*, Automata studies **3**, page 41 (1951).

[22] Kozen, D., *A completeness theorem for Kleene algebras and the algebra of regular events*, Information and computation **110**, pages 366–390 (1994).

[23] Kozen, D., *Kleene algebra with tests*, ACM Transactions on Programming Languages and Systems (TOPLAS) **19**, pages 427–443 (1997).

[24] Kozen, D., *Automata on guarded strings and applications*, Technical report, Cornell University (2001).

[25] Kozen, D., *On the coalgebraic theory of kleene algebra with tests*, in: *Rohit Parikh on Logic, Language and Society*, pages 279–298, Springer (2017).

[26] Kozen, D. and F. Smith, *Kleene algebra with tests: Completeness and decidability*, in: *International Workshop on Computer Science Logic*, pages 244–259, Springer (1996).

[27] Kozen, D. and W.-L. D. Tseng, *The böhm–jacopini theorem is false, propositionally*, in: *International Conference on Mathematics of Program Construction*, pages 177–192, Springer (2008).

[28] Levy, P. B., *Similarity quotients as final coalgebras*, in: *International Conference on Foundations of Software Science and Computational Structures*, pages 27–41, Springer (2011).

[29] Maler, O. and A. Pnueli, *On the learnability of infinitary regular sets*, Information and Computation **118**, pages 316–326 (1995).

[30] Moerman, J., M. Sammartino, A. Silva, B. Klin and M. Szynwelski, *Learning nominal automata*, in: *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, pages 613–625 (2017).

[31] Moore, T., *Gedanken–experiments on*, in: *Sequential Machines, Automata Studies, Annals of Mathematical Studies, no. 34*, Citeseer (1956).

[32] Nerode, A., *Linear automaton transformations*, Proceedings of the American Mathematical Society **9**, pages 541–544 (1958).

[33] Pous, D., *Symbolic algorithms for language equivalence and kleene algebra with tests*, in: *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 357–368 (2015).

[34] Rivest, R. L. and R. E. Schapire, *Inference of finite automata using homing sequences*, Information and Computation **103**, pages 299–347 (1993).

[35] Rutten, J. J., *Universal coalgebra: a theory of systems*, Theoretical computer science **249**, pages 3–80 (2000).

[36] Schmid, T., T. Kappé, D. Kozen and A. Silva, *Guarded kleene algebra with tests: Coequations, coinduction, and completeness*, arXiv preprint arXiv:2102.08286 (2021).

[37] Smolka, S., N. Foster, J. Hsu, T. Kappé, D. Kozen and A. Silva, *Guarded kleene algebra with tests: verification of uninterpreted programs in nearly linear time*, Proceedings of the ACM on Programming Languages **4**, pages 1–28 (2019).

[38] Smolka, S., P. Kumar, D. M. Kahn, N. Foster, J. Hsu, D. Kozen and A. Silva, *Scalable verification of probabilistic networks*, in: *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 190–203 (2019).

[39] Thompson, K., *Programming techniques: Regular expression search algorithm*, Communications of the ACM **11**, pages 419–422 (1968).

[40] Vaandrager, F., *Model learning*, Communications of the ACM **60**, pages 86–95 (2017).

[41] Vaandrager, F., B. Garhewal, J. Rot and T. Wißmann, *A new approach for active automata learning based on apartness*, arXiv preprint arXiv:2107.05419 (2021).

[42] van Heerdt, G., M. Sammartino and A. Silva, *Calf: Categorical automata learning framework*, Computer Science Logic 2017 (2017).

[43] van Heerdt, G., M. Sammartino and A. Silva, *Learning automata with side-effects*, in: *International Workshop on Coalgebraic Methods in Computer Science*, pages 68–89, Springer (2020).

[44] Zetzsche, S., G. van Heerdt, M. Sammartino and A. Silva, *Canonical automata via distributive law homomorphisms*, Electronic Proceedings in Theoretical Computer Science **351**, page 296–313 (2021), ISSN 2075-2180. https://doi.org/10.4204/eptcs.351.18

A Definitions

Definition A.1 [[37]] Let $\mathscr{X} = (X, \delta)$ be a G-coalgebra. The *uniform continuation* of $A \subseteq X$ by $h \in G(X)$ is the G-coalgebra $\mathscr{X}[A, h] = (X, \delta[A, h])$, where

$$\delta[A,h](x)(\alpha) = \begin{cases} h(\alpha) & \text{if } x \in A, \delta(x)(\alpha) = 1 \\ \delta(x)(\alpha) & \text{else} \end{cases}.$$

In the following let $\mathscr{X} + \mathscr{Y} := (X + Y, \delta^{\mathscr{X}} + \delta^{\mathscr{Y}})$, where $\delta^{\mathscr{X}} + \delta^{\mathscr{Y}}(x)(\alpha) = \delta^{\mathscr{X}}(x)(\alpha)$, if $x \in X$, and $\delta^{\mathscr{Y}}(x)(\alpha)$ otherwise.

Definition A.2 [[37]] The class of *well-nested* G-coalgebras is defined as follows:

- If $\mathscr{X} = (X, \delta)$ has no transitions, i.e. if $\delta : X \to 2^{\mathrm{At}}$, then $\mathscr{X}$ is well-nested.
- If $\mathscr{X}$ and $\mathscr{Y}$ are well-nested and $h \in G(X + Y)$, then $(\mathscr{X} + \mathscr{Y})[X, h]$ is well-nested.

Definition A.3 Let $\mathscr{X} = (X, \langle \delta, \varepsilon \rangle)$ be a M-coalgebra, where $MX = X^A \times B$. We define a function $[\![-]\!] : X \to B^{A^*}$ as follows:

$$[\![x]\!](\varepsilon) = \varepsilon(x);$$
$$[\![x]\!](av) = [\![\delta(x)(a)]\!](v).$$

In particular, if $A = (\mathrm{At} \cdot \Sigma)$ and $B = 2^{\mathrm{At}}$ for finite sets At and Σ, then Theorem A.3 induces a function $[\![-]\!] : X \to (2^{\mathrm{At}})^{(\mathrm{At} \cdot \Sigma)^*} \cong \mathcal{P}((\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At})$ via currying by

$$\alpha \in [\![x]\!] \Leftrightarrow \varepsilon(x)(\alpha) = 1;$$
$$\alpha p v \in [\![x]\!] \Leftrightarrow \delta(x)(\alpha p) = y \text{ and } v \in [\![y]\!].$$

B Proofs

Lemma B.1 *If $x \xrightarrow{w} x_w^1$ and $x \xrightarrow{w} x_w^2$, then $x_w^1 = x_w^2$.*

Proof. We show the statement by induction on the length of $w \in \mathrm{GS}^-$:

- The induction base $w = \varepsilon$ follows from the base case of (3): $x \xrightarrow{\varepsilon} x_w^i$ if(f) $x_w^i = x$ for $i = 1, 2$.
- For the induction step let $w = v\alpha p$ for some $v \in \mathrm{GS}^-$. By (3) there exist $x_v^1, x_v^2 \in X$ such that $x \xrightarrow{v} x_v^1 \xrightarrow{\alpha p} x_w^1$ and $x \xrightarrow{v} x_v^2 \xrightarrow{\alpha p} x_w^2$. From the induction hypothesis it follows $x_v^1 = x_v^2$. Thus, by (3), $(p, x_w^1) = \delta(x_v^1)(\alpha) = \delta(x_v^2)(\alpha) = (p, x_w^2)$, which yields $x_w^1 = x_w^2$.

$\square$

Lemma B.2 *Let $\mathscr{X}^A = (A, \delta^A)$ be the restriction of a G-coalgebra $\mathscr{X} = (X, \delta)$ to a δ-invariant subset $A \subseteq X$. Then $[\![a]\!]_{\mathscr{X}} = [\![a]\!]_{\mathscr{X}^A}$ for all $a \in A$.*

Proof. We show $w \in [\![a]\!]_{\mathscr{X}}$ if(f) $w \in [\![a]\!]_{\mathscr{X}^A}$ for all $a \in A$ and $w \in \mathrm{GS}$ by induction on the length of w.

- For the induction base assume $w = \alpha$, then we deduce:

$$\begin{aligned}
\alpha \in [\![a]\!]_{\mathscr{X}} &\Leftrightarrow \delta(a)(\alpha) = 1 && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \delta^A(a)(\alpha) = 1 && (a \in A) \\
&\Leftrightarrow \alpha \in [\![a]\!]_{\mathscr{X}^A} && \text{(Definition of } [\![-]\!]).
\end{aligned}$$

- For the induction step let $w = \alpha p v$, then we find:

$$\begin{aligned}
\alpha p v \in [\![a]\!]_{\mathscr{X}} &\Leftrightarrow \exists x \in X : \delta(a)(\alpha) = (p, x),\ v \in [\![x]\!]_{\mathscr{X}} && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \exists b \in A : \delta(a)(\alpha) = (p, b),\ v \in [\![b]\!]_{\mathscr{X}} && (a \in A,\ \delta\text{-inv}) \\
&\Leftrightarrow \exists b \in A : \delta^A(a)(\alpha) = (p, b),\ v \in [\![b]\!]_{\mathscr{X}^A} && (a, b \in A,\ \mathrm{IH}) \\
&\Leftrightarrow \alpha p v \in [\![a]\!]_{\mathscr{X}^A} && \text{(Definition of } [\![-]\!]).
\end{aligned}$$

$\square$

Lemma B.3 *The restriction of a normal G-coalgebra to a δ-invariant subset is normal.*

Proof. Let $\mathscr{X} = (X, \delta)$ be a normal G-coalgebra and $A \subseteq X$ a δ-invariant subset. We write $\mathscr{X}^A = (A, \delta^A)$ for the well-defined restriction of $\mathscr{X}$ to A. Assume for $a, b \in A$ we have $\delta^A(a)(\alpha) = (p, b)$. Since $a \in A$, we have $\delta(a)(\alpha) = (p, b)$, which by normality of $\mathscr{X}$ implies $\emptyset \neq [\![b]\!]_{\mathscr{X}}$. From $b \in A$ and Theorem B.2 we thus can deduce $\emptyset \neq [\![b]\!]_{\mathscr{X}^A}$. $\square$

Lemma B.4 *The restriction of a well-nested G-coalgebra to a δ-invariant subset is well-nested.*

Proof. We show the statement by induction on the well-nested structure of $\mathscr{X}$. As before, we write $\mathscr{X}^A = (A, \delta^A)$ for the well-defined restriction of $\mathscr{X} = (X, \delta)$ to a δ-invariant subset $A \subseteq X$.

- For the induction base assume that $\mathscr{X} = (X, \delta)$ satisfies $\delta : X \to 2^{\mathrm{At}}$, and $A \subseteq X$ is a δ-invariant set. Then clearly the restriction is of type $\delta^A : A \to 2^{\mathrm{At}}$, i.e. $\mathscr{X}^A = (A, \delta^A)$ is well-nested.
- For the induction step let $\mathscr{Y} = (Y, \delta^{\mathscr{Y}})$ and $\mathscr{Z} = (Z, \delta^{\mathscr{Z}})$ be well-nested G-coalgebras, $h \in G(Y + Z)$, and $\mathscr{X} = (Y + Z, (\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h])$. Moreover let $A \subseteq Y + Z$ be a $(\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h]$-invariant set. We would like to show that $\mathscr{X}^A$ is well-nested.

  The induction hypothesis reads:
  - for all $\delta^{\mathscr{Y}}$-invariant sets $B \subseteq Y$, the subcoalgebra $\mathscr{Y}^B = (B, (\delta^{\mathscr{Y}})^B)$ is well-nested;
  - for all $\delta^{\mathscr{Z}}$-invariant sets $C \subseteq Z$, the subcoalgebra $\mathscr{Z}^C = (C, (\delta^{\mathscr{Z}})^C)$ is well-nested.

  We begin by showing that $A \cap Y \subseteq Y$ and $A \cap Z \subseteq Z$ are $\delta^{\mathscr{Y}}$- and $\delta^{\mathscr{Z}}$-invariant sets, respectively. Let $\delta^{\mathscr{Y}}(x)(\alpha) = (p, y)$ for $x \in A \cap Y$ and $y \in Y$. Then by definition

$$(\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h](x)(\alpha) = \delta^{\mathscr{Y}}(x)(\alpha) = (p, y),$$

which by $(\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h]$-invariance of A implies $y \in A$. It hence follows $y \in A \cap Y$. Analogously one dedues that $A \cap Z$ is $\delta^{\mathscr{Z}}$-invariant.

Thus $\mathscr{Y}^{A\cap Y} = (A \cap Y, (\delta^{\mathscr{Y}})^{A\cap Y})$ and $\mathscr{Z}^{A\cap Z} = (A \cap Z, (\delta^{\mathscr{Z}})^{A\cap Z})$ are well-defined, and moreover, by the induction hypothesis they are well-nested.

We observe the equality $A = A \cap Y + A \cap Z$, which follows from $A \subseteq Y + Z$, and define $\overline{h} \in G(A \cap Y + A \cap Z) = G(A)$ by:

$$\overline{h}(\alpha) = \begin{cases} 1 & \text{if } h(\alpha) = 1 \\ (p, x) & \text{if } h(\alpha) = (p, x),\ x \in A \\ 0 & \text{else} \end{cases} \tag{B.1}$$

It follows $\mathscr{X}^A = (A \cap Y + A \cap Z, ((\delta^{\mathscr{Y}})^{A\cap Y} + (\delta^{\mathscr{Z}})^{A\cap Z})[A \cap Y, \overline{h}])$, since for any $x \in A$ it holds:

$$\begin{aligned}
&((\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h])^A(x)(\alpha) \\
&= \begin{cases} \delta^{\mathscr{Y}}(x)(\alpha) & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) \neq 1 \\ h(\alpha) & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1 \\ \delta^{\mathscr{Z}}(x)(\alpha) & x \in A \cap Z \end{cases} \\
&= \begin{cases} \delta^{\mathscr{Y}}(x)(\alpha) & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) \neq 1 \\ 1 & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1,\ h(\alpha) = 1 \\ 0 & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1,\ h(\alpha) = 0 \\ (p, x') & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1,\ h(\alpha) = (p, x') \\ \delta^{\mathscr{Z}}(x)(\alpha) & x \in A \cap Z \end{cases} \\
&\overset{(\star)}{=} \begin{cases} \delta^{\mathscr{Y}}(x)(\alpha) & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) \neq 1 \\ 1 & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1, \overline{h}(\alpha) = 1 \\ 0 & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1, \overline{h}(\alpha) = 0 \\ (p, x') & x \in A \cap Y,\ \delta^{\mathscr{Y}}(x)(\alpha) = 1, \overline{h}(\alpha) = (p, x') \\ \delta^{\mathscr{Z}}(x)(\alpha) & x \in A \cap Z \end{cases} \\
&= \begin{cases} (\delta^{\mathscr{Y}})^{A\cap Y}(x)(\alpha) & x \in A \cap Y,\ (\delta^{\mathscr{Y}})^{A\cap Y}(x)(\alpha) \neq 1 \\ \overline{h}(\alpha) & x \in A \cap Y,\ (\delta^{\mathscr{Y}})^{A\cap Y}(x)(\alpha) = 1 \\ (\delta^{\mathscr{Z}})^{A\cap Z}(x)(\alpha) & x \in A \cap Z \end{cases} \\
&= ((\delta^{\mathscr{Y}})^{A\cap Y} + (\delta^{\mathscr{Z}})^{A\cap Z})[A \cap Y, \overline{h}](x)(\alpha),
\end{aligned}$$

where we use for $(\star)$ that $((\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h])^A(x)(\alpha) = (p, x')$ for $x \in A$, implies $x' \in A$, as A is $(\delta^{\mathscr{Y}} + \delta^{\mathscr{Z}})[Y, h]$-invariant.

□

Proposition B.5 *Let $\mathscr{X}$ be a G-automaton, then $r(\mathscr{X})$ is well-nested, normal, or satisfies the nesting coequation, whenever $\mathscr{X}$ does. Moreover, $r(\mathscr{X})$ accepts the same language as $\mathscr{X}$.*

Proof. Let us write $\mathscr{X} = (X, \delta, x)$. From (3) it is immediate that $r(x) \subseteq X$ is δ-invariant. Thus, Theorem B.4 and Theorem B.3, respectively, imply that $r(\mathscr{X}) = (r(x), \delta^{r(x)}, x)$ is well-nested, or normal, whenever $\mathscr{X}$ is. From Theorem B.2 it further follows

$$[\![r(\mathscr{X})]\!] = [\![x]\!]_{r(\mathscr{X})} = [\![x]\!]_{\mathscr{X}} = [\![\mathscr{X}]\!].$$

Coalgebras satisfying the nesting coequation form a covariety, which in particular is closed under subcoalgebras [8,36]. Since there exists an epi-mono factorization

$$R(\mathscr{X}) \twoheadrightarrow r(\mathscr{X}) \hookrightarrow \mathscr{X}$$

the automaton $r(\mathscr{X})$ thus satisfies the nesting coequation, whenever $\mathscr{X}$ does.

□

Lemma B.6 *Let $\mathscr{X}$ be a G-automaton with initial state x. Then $[\![w]\!]_{R(\mathscr{X})} = w^{-1}[\![\mathscr{X}]\!]$ for all $w \in R(x)$.*

Proof. We prove $u \in [\![w]\!]_{R(\mathscr{X})}$ if(f) $u \in w^{-1}[\![\mathscr{X}]\!]$ for all $u \in \mathrm{GS}$ and $w \in R(x)$ by induction on the length of u.

- For the induction base assume $u = \alpha$, then we find:

$$\begin{aligned}
\alpha \in [\![w]\!]_{R(\mathscr{X})} &\Leftrightarrow \partial(w)(\alpha) = 1 && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \delta(x_w)(\alpha) = 1 && \text{(Definition of } \partial) \\
&\Leftrightarrow \alpha \in [\![x_w]\!]_{\mathscr{X}} && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow w\alpha \in [\![\mathscr{X}]\!] && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \alpha \in w^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } w^{-1}[\![\mathscr{X}]\!]).
\end{aligned}$$

- For the induction base let $u = \alpha p v$, then it follows:

$$\begin{aligned}
\alpha p v \in [\![w]\!]_{R(\mathscr{X})} &\Leftrightarrow \partial(w)(\alpha) = (p, w\alpha p),\ v \in [\![w\alpha p]\!]_{R(\mathscr{X})} && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \delta(x_w)(\alpha) = (p, x_{w\alpha p}),\ v \in (w\alpha p)^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } \partial,\ \text{IH}) \\
&\Leftrightarrow \delta(x_w)(\alpha) = (p, x_{w\alpha p}),\ v \in [\![x_{w\alpha p}]\!]_{\mathscr{X}} && \text{(Definition of } (w\alpha p)^{-1}[\![\mathscr{X}]\!]) \\
&\Leftrightarrow \alpha p v \in [\![x_w]\!]_{\mathscr{X}} && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \alpha p v \in w^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } w^{-1}[\![\mathscr{X}]\!]).
\end{aligned}$$

□

Lemma B.7 *Let $\mathscr{X}$ be a normal G-automaton with initial state $x \in X$. Then $[\![\mathscr{X}]\!] \xrightarrow{w} w^{-1}[\![\mathscr{X}]\!]$ in $m(\mathscr{X})$ for all $w \in R(x)$. In particular, $m(\mathscr{X})$ is reachable.*

Proof. We prove the statement by induction on the length of $w \in R(x)$:

- For the induction base, let $w = \varepsilon$, then $[\![\mathscr{X}]\!] \xrightarrow{\varepsilon} [\![\mathscr{X}]\!] = \varepsilon^{-1}[\![\mathscr{X}]\!]$ by the base case of (3).
- In the induction step, let $w = v\alpha p$ with $v \in \mathrm{GS}^-$. By the definition of reachability, $v \in R(x)$. From the induction hypothesis we deduce $[\![\mathscr{X}]\!] \xrightarrow{v} v^{-1}[\![\mathscr{X}]\!]$ in $m(\mathscr{X})$. The normality of $\mathscr{X}$ implies the inequality $(\alpha p)^{-1}(v^{-1}[\![\mathscr{X}]\!]) \neq \emptyset$. From (5) it thus follows $v^{-1}[\![\mathscr{X}]\!] \xrightarrow{\alpha p} (\alpha p)^{-1}(v^{-1}[\![\mathscr{X}]\!]) = w^{-1}[\![\mathscr{X}]\!]$. We conclude $[\![\mathscr{X}]\!] \xrightarrow{w = v\alpha p} w^{-1}[\![\mathscr{X}]\!]$ by (3).

□

Lemma B.8 *Let $\mathscr{X}$ be a G-automaton, then $[\![L]\!] = L$ for all L in $m(\mathscr{X})$. In particular, $[\![m(\mathscr{X})]\!] = [\![\mathscr{X}]\!]$.*

Proof. We show $v \in [\![w^{-1}[\![\mathscr{X}]\!]]\!]$ if and only if $v \in w^{-1}[\![\mathscr{X}]\!]$ for all $v \in \mathrm{GS}$, $w \in R(x)$ by induction on the length of v:

- For the induction base, let $v = \alpha$. Then we can compute:

$$\begin{aligned}
\alpha \in [\![w^{-1}[\![\mathscr{X}]\!]]\!] &\Leftrightarrow \partial(w^{-1}[\![\mathscr{X}]\!])(\alpha) = 1 && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow \alpha \in w^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } \partial).
\end{aligned}$$

- In the induction step, let $v = \alpha p u$. Then we have the following equivalences:

$$\begin{aligned}
\alpha p u \in [\![w^{-1}[\![\mathscr{X}]\!]]\!] &\Leftrightarrow u \in [\![(w\alpha p)^{-1}[\![\mathscr{X}]\!]]\!] && \text{(Definition of } [\![-]\!], (5)) \\
&\Leftrightarrow u \in (w\alpha p)^{-1}[\![\mathscr{X}]\!] && \text{(IH)} \\
&\Leftrightarrow w\alpha p u \in [\![\mathscr{X}]\!] && \text{(Definition of } (-)^{-1}[\![\mathscr{X}]\!]) \\
&\Leftrightarrow \alpha p u \in w^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } (-)^{-1}[\![\mathscr{X}]\!]).
\end{aligned}$$

In particular,

$$[\![m(\mathscr{X})]\!] = [\![[\![\mathscr{X}]\!]]\!] = [\![\varepsilon^{-1}[\![\mathscr{X}]\!]]\!] = \varepsilon^{-1}[\![\mathscr{X}]\!] = [\![\mathscr{X}]\!].$$

□

Corollary B.9 *Let $\mathscr{X}$ be a G-automaton, then $m(\mathscr{X})$ is observable.*

Proof. By Theorem 4.6, $[\![L_1]\!] = [\![L_2]\!]$ implies $L_1 = L_2$, which shows that $[\![-]\!]$ is injective. By definition, this proves that $m(\mathscr{X})$ is observable. □

Corollary B.10 *Let $\mathscr{X}$ be a G-automaton, then $m(\mathscr{X})$ is normal.*

Proof. Assume $\partial(L_1)(\alpha) = (p, L_2)$, then $L_2 = (\alpha p)^{-1}L_1 \neq \emptyset$ by (5). From Theorem 4.6 it follows $[\![L_2]\!] = L_2 \neq \emptyset$, which shows that $m(\mathscr{X})$ is normal. □

Corollary B.11 *Let $\mathscr{X}$ be a G-automaton, then $m(\mathscr{X})$ is normal and observable.*

Proof. Follows immediately from Theorem B.10 and Theorem B.9. □

Proposition B.12 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata with $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$, and $y \in Y$ the initial state of $\mathscr{Y}$. Then $\pi : r(\mathscr{Y}) \to m(\mathscr{X})$ with $\pi(z) = w_z^{-1}[\![\mathscr{X}]\!]$, for $y \xrightarrow{w_z} z$ in $\mathscr{Y}$, is a (surjective) G-automata homomorphism, uniquely defined.*

Proof. We have to show that π is well-defined, surjective, preserves initial states, is a G-coalgebra homomorphism, and is unique. In this order:

- Let $z \in r(y)$, then by definition there exists at least one $w_1 \in R(y)$ such that $y \xrightarrow{w_1} z$ in $\mathscr{Y}$. Since $\mathscr{Y}$ is normal, we have $w_1^{-1}[\![\mathscr{X}]\!] = w_1^{-1}[\![\mathscr{Y}]\!] \neq \emptyset$. Hence there exists some $z' \in X$, such that $x \xrightarrow{w_1} z'$ in $\mathscr{X}$, that is, $w_1 \in R(x)$, where $x \in X$ is the initial state of $\mathscr{X}$. Assume there exists a second $w_2 \in R(y)$, such that $y \xrightarrow{w_2} z$ in $\mathscr{Y}$. Then we have:

$$\begin{aligned}
w_1 u \in [\![\mathscr{X}]\!] &\Leftrightarrow w_1 u \in [\![\mathscr{Y}]\!] && ([\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]) \\
&\Leftrightarrow u \in [\![z]\!] && (\text{Definition of } [\![-]\!]) \\
&\Leftrightarrow w_2 u \in [\![\mathscr{Y}]\!] && (\text{Definition of } [\![-]\!]) \\
&\Leftrightarrow w_2 u \in [\![\mathscr{X}]\!] && ([\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!])
\end{aligned}$$

  for all $u \in \mathrm{GS}$. In other words, $w_1 \equiv_{[\![\mathscr{X}]\!]} w_2$, or, equivalently, $w_1^{-1}[\![\mathscr{X}]\!] = w_2^{-1}[\![\mathscr{X}]\!]$. Thus π is a well-defined function.
- Let $w \in R(x)$, then by definition there exists some $x_w \in X$ with $x \xrightarrow{w} x_w$ in $\mathscr{X}$. Since $\mathscr{X}$ is normal, $w^{-1}[\![\mathscr{Y}]\!] = w^{-1}[\![\mathscr{X}]\!] \neq \emptyset$, i.e. $y \xrightarrow{w} y_w$ in $\mathscr{Y}$, for some $y_w \in Y$. Thus, by construction, $\pi(y_w) = w^{-1}[\![\mathscr{X}]\!]$, which shows that π is surjective.
- Initial states are preserved since $y \xrightarrow{\varepsilon} y$ by (3), which by definition of π implies $\pi(y) = \varepsilon^{-1}[\![\mathscr{X}]\!] = [\![\mathscr{X}]\!]$.
- π is a G-coalgebra homomorphism in the (compact, equivalent) sense of [37][Definition of 5.7.]:
  - Let $\delta^{\mathscr{Y}}(z)(\alpha) = 0$, then $\delta^{m(\mathscr{X})}(\pi(z))(\alpha) \neq 1$, since otherwise $w_z\alpha \in [\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$ by the definition of $\delta^{m(\mathscr{X})}$, which would imply the contradiction $1 = \delta^{\mathscr{Y}}(z)(\alpha) = 0$. Assume $\delta^{m(\mathscr{X})}(\pi(z))(\alpha) = (p, (w_z\alpha p)^{-1}[\![\mathscr{X}]\!])$. By definition of $\delta^{m(\mathscr{X})}$ there exists some $v \in \mathrm{GS}$, such that $w_z\alpha p v \in [\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$. Hence it follows $\delta^{\mathscr{Y}}(z)(\alpha) \neq 0$ by the definition of $[\![-]\!]$, which is a contradiction. We can thus conclude $\delta^{m(\mathscr{X})}(\pi(z))(\alpha) = 0$
  - Let $\delta^{\mathscr{Y}}(z)(\alpha) = 1$, then $w_z\alpha \in [\![\mathscr{Y}]\!] = [\![\mathscr{X}]\!]$ by the definition of $[\![-]\!]$. From the definition of $\delta^{m(\mathscr{X})}$, it follows $\delta^{m(\mathscr{X})}(\pi(z))(\alpha) = 1$.
  - Let $\delta^{\mathscr{Y}}(z)(\alpha) = (p, z')$, then, by normality of $\mathscr{Y}$, there exists some $v \in [\![z']\!] \neq \emptyset$. The latter implies $w_z\alpha p v \in [\![\mathscr{Y}]\!] = [\![\mathscr{X}]\!]$. By the definitions of $\delta^{m(\mathscr{X})}$ and $w_{z'}$, it follows $\delta^{m(\mathscr{X})}(\pi(z))(\alpha) = (p, (w_z\alpha p)^{-1}[\![\mathscr{X}]\!]) = (p, \pi(z'))$.

- Let $g : r(\mathscr{Y}) \to m(\mathscr{X})$ be any G-automata homomorphism. Let $z \in r(y)$, then by definition there exists $w_z \in R(y)$, such that $y \xrightarrow{w_z} z$ in $\mathscr{Y}$, and thus in $r(\mathscr{Y})$. Since g is a G-automata homomorphism, it follows $[\![\mathscr{X}]\!] = g(y) \xrightarrow{w_z} g(z)$ in $m(\mathscr{X})$. By Theorem 4.5, on the other hand, we have $[\![\mathscr{X}]\!] \xrightarrow{w_z} w_z^{-1}[\![\mathscr{X}]\!]$ in $m(\mathscr{X})$. From Theorem 4.2 it thus follows $g(z) = w_z^{-1}[\![\mathscr{X}]\!] = \pi(z)$.

□

Lemma B.13 *Let $\mathscr{X}$ be a normal G-automaton with initial state $x \in X$ and $\pi : r(\mathscr{X}) \twoheadrightarrow m(\mathscr{X})$ as in Theorem 4.8, then $y \simeq z$ if(f) $\pi(y) = \pi(z)$ for all $y, z \in r(x)$. Consequently, $m(\mathscr{X})$ is isomorphic to $r(\mathscr{X})/\simeq$.*

Proof. The statement follows from the following chain of equivalences:

$$\begin{aligned} \pi(y) = \pi(z) &\Leftrightarrow (w_y)^{-1}[\![\mathscr{X}]\!] = (w_z)^{-1}[\![\mathscr{X}]\!] && \text{(Definition of } \pi) \\ &\Leftrightarrow [\![y]\!] = [\![z]\!] && \text{(Definition of } (-)^{-1}[\![\mathscr{X}]\!]) \\ &\Leftrightarrow y \simeq z && (\mathscr{X} \text{ normal}). \end{aligned}$$

□

Corollary B.14 *Let $\mathscr{X}$ be a normal G-automaton, then $m(\mathscr{X})$ satisfies the nesting coequation, whenever $\mathscr{X}$ does.*

Proof. In Theorem 4.3 it was noted that the reachable subcoalgebra $r(\mathscr{X})$ satisfies the nesting coequation, whenever $\mathscr{X}$ does. By Theorem 4.8 there exists an epimorphism $\pi : r(\mathscr{X}) \twoheadrightarrow m(\mathscr{X})$ for any normal automaton $\mathscr{X}$. The claim follows since coalgebras satisfying a coequation form a covariety, which is in particular closed under homomorphic images [8,36]. □

Corollary B.15 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata, then $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$ if(f) $m(\mathscr{X}) \cong m(\mathscr{Y})$.*

Proof. We begin by assuming $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$. From Theorem 4.6 and Theorem 4.7 we know that $m(\mathscr{X})$ and $m(\mathscr{Y})$ are normal and accept the same language as $\mathscr{X}$ and $\mathscr{Y}$. From Theorem 4.5 it follows that $m(\mathscr{X})$ and $m(\mathscr{Y})$ are reachable. Theorem 4.8 thus implies that there exist G-automata homomorphisms $\pi_1 : m(\mathscr{Y}) \to m(\mathscr{X})$ and $\pi_2 : m(\mathscr{X}) \to m(\mathscr{Y})$. From the uniqueness property in Theorem 4.8 we deduce $\pi_1\pi_2 = \mathrm{id}_{m(\mathscr{X})}$ and $\pi_2\pi_1 = \mathrm{id}_{m(\mathscr{Y})}$. Hence $\pi_2 : m(\mathscr{X}) \to m(\mathscr{Y})$ is an isomorphism with inverse π_1.

Conversely, assume $m(\mathscr{X})$ is isomorphic to $m(\mathscr{Y})$. Then it immediately follows $[\![m(\mathscr{X})]\!] = [\![m(\mathscr{Y})]\!]$, which implies $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$ by Theorem 4.6. □

Corollary B.16 *Let $\mathscr{X}$ and $\mathscr{Y}$ be normal G-automata with $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$. Then $|m(\mathscr{X})| \leq |\mathscr{Y}|$, where $|m(\mathscr{X})| = |\mathscr{Y}|$ if(f) $m(\mathscr{X}) \cong \mathscr{Y}$.*

Proof. From Theorem 4.11 it immediately follows $m(\mathscr{X}) \cong m(\mathscr{Y})$. We additionally observe Figure 5a to derive

$$|m(\mathscr{X})| = |m(\mathscr{Y})| \leq |r(\mathscr{Y})| \leq |\mathscr{Y}|.$$

We next show $|m(\mathscr{X})| = |\mathscr{Y}|$ if(f) $m(\mathscr{X}) \cong \mathscr{Y}$:

- Assume $m(\mathscr{X}) \cong \mathscr{Y}$, then immediately $|m(\mathscr{X})| = |\mathscr{Y}|$.
- Assume $|m(\mathscr{X})| = |\mathscr{Y}|$, then Theorem 4.8 and Figure 5a imply:

$$|r(\mathscr{Y})| \geq |m(\mathscr{X})| = |\mathscr{Y}| \geq |r(\mathscr{Y})|.$$

  It thus follows $|m(\mathscr{X})| = |r(\mathscr{Y})| = |\mathscr{Y}|$. From the second equality and the definition of $r(\mathscr{Y})$ it immediately follows $\mathscr{Y} \cong r(\mathscr{Y})$. The first equality implies that the epimorphism $\pi : r(\mathscr{Y}) \twoheadrightarrow m(\mathscr{X})$ in Theorem 4.8 is a bijective automata homomorphism. Any bijective coalgebra homomorphism is a coalgebra isomorphism [35, Prop. 2.3]. It is clear that the inverse of an initial state preserving coalgebra isomorphism preserves initial states as well. Thus $\pi : r(\mathscr{Y}) \cong m(\mathscr{X})$ is an G-automata isomorphism.

□

Lemma B.17 *It holds $row(s) \xrightarrow{t} row(st)$ in $m(T)$ for all $s \in S$ and $t \in \mathrm{GS}^-$, such that $st \in S$. In particular, $m(T)$ is reachable.*

Proof. We show the statement by induction on the length of $t \in \mathrm{GS}^-$:

- If $t = \varepsilon$, the statement follows from the base case of (3), i.e. $row(s) \xrightarrow{\varepsilon} row(s)$.
- If $t = v\alpha p$ for $v \in \mathrm{GS}^-$, we have $sv \in S$, since $sv\alpha p = st \in S$ and S is prefix-closed by Theorem 5.1. Thus $row(s) \xrightarrow{v} row(sv)$ by the induction hypothesis. Since $\varepsilon \neq st \in S$, we have $(\alpha p)^{-1} row(sv) = row(st) \neq \emptyset$ by Theorem 5.1. Thus it follows $row(sv) \xrightarrow{\alpha p} row(sv\alpha p)$ by (6). We conclude $row(s) \xrightarrow{v\alpha p = t} row(sv\alpha p) = row(st)$ by (3).

Since $\epsilon \in S$ by Theorem 5.1, we in particular obtain $row(\varepsilon) \xrightarrow{s} row(s)$ in $m(T)$ for all $s \in S$, which implies the reachability of $m(T)$. ◻

Lemma B.18 *$m(T)$ is size-minimal among automata consistent with T.*

Proof. We begin by showing that $m(T)$ is consistent with T, that is, it satisfies $[\![row(s)]\!](e) = row(s)(e)$ for all $s \in S, e \in E$, by induction on the length of e:

- For the induction base, let $e = \alpha \in \mathrm{At}$, then it immediately follows:

$$
\begin{aligned}
[\![row(s)]\!](e) = 1 &\Leftrightarrow \delta(row(s))(\alpha) = 1 && \text{(Definition of } [\![-]\!]) \\
&\Leftrightarrow row(s)(\alpha) = 1 && (6).
\end{aligned}
$$

- For the induction step, let $e = \alpha p w$ for $w \in \mathrm{GS}$, then Theorem 5.1 implies $w \in E$ and $row(s)(\alpha p w) = row(s\alpha p)(w)$. Thus we can deduce:

$$
\begin{aligned}
& [\![row(s)]\!](\alpha p w) = 1 \\
\Leftrightarrow\ & \exists t \in S : \emptyset \neq row(s\alpha p) = row(t) \text{ and } [\![row(t)]\!](w) = 1 && \text{(Definition of } [\![-]\!]) \\
\Leftrightarrow\ & \exists t \in S : row(s\alpha p) = row(t) \text{ and } row(t)(w) = 1 && (w \in E,\ \text{IH}) \\
\Leftrightarrow\ & row(s\alpha p)(w) = 1 && (T \text{ closed}) \\
\Leftrightarrow\ & row(s)(\alpha p w) = 1 && \text{(Theorem 5.1)}.
\end{aligned}
$$

Let $(\mathscr{Y}, y)$ be any G-automaton consistent with T, i.e. $S \subseteq R(y)$ and $[\![y_s]\!](e) = row(s)(e)$ for all $s \in S, e \in E$, and $y_s \in Y$ with $y \xrightarrow{s} y_s$. We define a function $f : \{row(s) \mid s \in S\} \to Y$ by $f(row(s)) = y_s$. The function is well-defined, since $S \subseteq R(y)$. Assume $f(row(s)) = f(row(t))$, i.e. $y_s = y_t$ for $s, t \in S$. Then we can deduce

$$
row(s)(e) = [\![y_s]\!](e) = [\![y_t]\!](e) = row(t)(e)
$$

for all $e \in E$. Since by Theorem 5.1 rows indexed by S are disjoint, it follows $s = t$. This shows that f is injective, which implies the size-minimality of $m(T)$. ◻

Lemma B.19 *$m(T)$ is normal.*

Proof. Assume $\delta(row(s))(\alpha) = (p, row(t))$ for $s, t \in S$. Then we have

$$
row(t) = row(s\alpha p) = (\alpha p)^{-1} row(s) \neq \emptyset
$$

by (6). Since by Theorem 5.4 $m(T)$ is consistent with T, it follows $[\![row(t)]\!] \neq \emptyset$. ◻

Corollary B.20 *$m(T)$ is observable.*

Proof. Assume $[\![row(s)]\!] = [\![row(t)]\!]$ for $s, t \in S$. Then, by Theorem 5.4, we can immediately deduce $row(s) = row(t)$, which shows that $[\![-]\!]$ is injective, i.e. $m(T)$ is observable. ◻

Lemma B.21 *$m(T)$ is normal and observable.*

Proof. Immediate from Theorem B.19 and Theorem B.20. $\square$

Lemma B.22 *Let $T = (S, E, row)$ be an observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$, and let $x \in X$ be the initial state of $\mathscr{X}$. Then $\pi : \{row(s) \mid s \in S\} \to \{w^{-1}[\![\mathscr{X}]\!] \mid w \in R(x)\}$, $row(s) \mapsto s^{-1}[\![\mathscr{X}]\!]$ is a well-defined injective function.*

Proof. We first show that π is well-defined. To this end, we need to establish that i) $S \subseteq R(x)$; and ii) if $row(s) = row(t)$ for $s, t \in S$, then $s^{-1}[\![\mathscr{X}]\!] = t^{-1}[\![\mathscr{X}]\!]$.

For i) note that if $s = \varepsilon$, then $x \xrightarrow{s} x$ by the base case of (3), i.e. $s \in R(x)$. If $s \neq \varepsilon$, then Theorem 5.1 implies the existence of some $e \in E$, such that $row(s)(e) = 1$. Thus $[\![x]\!](se) = [\![\mathscr{X}]\!](se) = row(s)(e) = 1$, which implies $s \in R(x)$ by the definition of $[\![-]\!]$. For ii) it is enough to observe that by Theorem 5.1 all rows of an observation table are disjoint.

To show that π is injective, assume $\pi(row(s)) = \pi(row(t))$, for $s, t \in S$. By definition of π we thus have an equivalence $s \equiv_{[\![\mathscr{X}]\!]} t$. From the definition of $\equiv_{[\![\mathscr{X}]\!]}$ and the assumptions it thus follows:

$$e \in row(s) \Leftrightarrow se \in [\![\mathscr{X}]\!] \Leftrightarrow te \in [\![\mathscr{X}]\!] \Leftrightarrow e \in row(t)$$

for all $e \in E$. This proves the equality $row(s) = row(t)$. $\square$

Lemma B.23 *Let $T = (S, E, row)$ and $T' = (S, E', row')$ be closed deterministic observation table with $E \subseteq E'$ and $row(t)(e) = row'(t)(e)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let $m(T)$ and $m(T')$ have transition functions δ and δ', respectively, then for all $s, t \in S$:*

- *$\delta'(row'(s))(\alpha) = 1$ if(f) $\delta(row(s))(\alpha) = 1$*
- *$\delta'(row'(s))(\alpha) = (p, row'(t))$ implies $\delta(row(s))(\alpha) = (p, row(t))$ or $\delta(row(s))(\alpha) = 0$.*
- *$\delta'(row'(s))(\alpha) = 0$ implies $\delta(row(s))(\alpha) = 0$.*

Proof.

- For the first point we deduce

$$\begin{aligned} \delta'(row'(s))(\alpha) = 1 &\Leftrightarrow row'(s)(\alpha) = 1 && \text{(Definition of } \delta'\text{)} \\ &\Leftrightarrow row(s)(\alpha) = 1 && (\alpha \in \mathrm{At} \subseteq E) \\ &\Leftrightarrow \delta(row(s))(\alpha) = 1 && \text{(Definition of } \delta\text{).} \end{aligned}$$

- For the second point, assume $\delta'(row'(s))(\alpha) = (p, row'(t))$ for $t \in S$ with $row'(s\alpha p) = row'(t)$. Then by the first point $\delta(row(s))(\alpha) = 0$, or $\delta(row(s))(\alpha) = (p, row(u))$ for some $u \in S$ with $row(s\alpha p) = row(u)$. We further have

$$row(t)(e) = row'(t)(e) = row'(s\alpha p)(e) = row(s\alpha p)(e) = row(u)(e)$$

  for all $e \in E$. In other words, we have derived $row(t) = row(u)$.

- For the last point, assume $\delta'(row'(s))(\alpha) = 0$. Then by the first point $\delta(row(s))(\alpha) = 0$, or $\delta(row(s))(\alpha) = (p, row(t))$ for some $t \in S$ with $row(s\alpha p) = row(t)$. By the definition of δ, the latter case implies

$$row'(s\alpha p)(e) = row(s\alpha p)(e) = 1$$

  for some $e \in E \subseteq E'$. It thus follows $\delta'(row'(s))(\alpha) \notin 2$, which contradicts the assumption $\delta'(row'(s))(\alpha) = 0$. We thus can conclude $\delta(row(s))(\alpha) = 0$.

$\square$

Proposition B.24 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let π be the injection of Theorem 5.6, and $\mathscr{X}$ normal. The following are equivalent:*

(i) $\pi : m(T) \simeq m(\mathscr{X})$ *is a G-automata isomorphism;*
(ii) $[\![m(T)]\!] = [\![m(\mathscr{X})]\!]$.

Proof.

- 1. → 2.: Since π is a homomorphism, it follows $[\![-]\!]_{m(\mathscr{X})} \circ \pi = [\![-]\!]_{m(T)}$ by uniqueness. In particular we have:

$$\begin{aligned} [\![m(T)]\!]_{m(T)} &= [\![row(\varepsilon)]\!]_{m(T)} && (\text{Definition of } [\![-]\!]_{m(T)}) \\ &= [\![\pi(row(\varepsilon))]\!]_{m(\mathscr{X})} && ([\![-]\!]_{m(\mathscr{X})} \circ \pi = [\![-]\!]_{m(T)}) \\ &= [\![\varepsilon^{-1}\mathscr{X}]\!]_{m(\mathscr{X})} && (\text{Definition of } \pi) \\ &= [\![\mathscr{X}]\!]_{m(\mathscr{X})} && (\text{Definition of } [\![-]\!]_{m(\mathscr{X})}). \end{aligned}$$

- 2. → 1. : By Theorem 5.5 and Theorem 5.3 $m(T)$ is normal and reachable. From the assumption and Theorem 4.6 it follows $[\![m(T)]\!] = [\![m(\mathscr{X})]\!] = [\![\mathscr{X}]\!]$. By assumption $\mathscr{X}$ is normal. There thus exists a unique surjective automata homomorphism $f := m(T) = r(m(T)) \to m(\mathscr{X})$ by Theorem 4.8. Using Theorem 5.3, one easily verifies that $\pi = f$. Since by Theorem 5.6 the function $\pi = f$ is injective, it is a bijective coalgebra homomorphism. Any bijective coalgebra homomorphism is a coalgebra isomorphism [35, Prop. 2.3]. It is clear that the inverse of an initial state preserving coalgebra isomorphism preserves initial states as well. It thus follows that $\pi = f$ is a G-automata isomorphism.

□

Lemma B.25 *Let $T = (S, E, row)$ and $T' = (S, E', row')$ be closed deterministic observation table with $E \subseteq E'$ and $row(t)(e) = row'(t)(e)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Then $[\![row(s)]\!]_{m(T)} \subseteq [\![row'(s)]\!]_{m(T')}$ for all $s \in S$.*

Proof. We show $w \in [\![row(s)]\!]_{m(T)}$ implies $w \in [\![row'(s)]\!]_{m(T')}$ for all $s \in S$ and $w \in \mathrm{GS}$ by induction on w. Let $m(T)$ and $m(T')$ have transition functions δ and δ', respectively.

- For the induction base, assume $w = \alpha$. Then we deduce:

$$\begin{aligned} \alpha \in [\![row(s)]\!]_{m(T)} &\Leftrightarrow \delta(row(s))(\alpha) = 1 && (\text{Definition of } [\![-]\!]) \\ &\Leftrightarrow \delta'(row'(s))(\alpha) = 1 && (\text{Theorem B.23}) \\ &\Leftrightarrow \alpha \in [\![row'(s)]\!]_{m(T')} && (\text{Definition of } [\![-]\!]). \end{aligned}$$

- In the induction step, let $w = \alpha p v$. Then we have:

$$\begin{aligned} & \alpha p v \in [\![row(s)]\!]_{m(T)} \\ \Leftrightarrow\ & \exists t \in S : \delta(row(s))(\alpha) = (p, row(t)),\ v \in [\![row(t)]\!]_{m(T)} && (\text{Definition of } [\![-]\!]) \\ \Rightarrow\ & \exists t \in S : \delta'(row'(s))(\alpha) = (p, row'(t)),\ v \in [\![row'(t)]\!]_{m(T')} && (\text{Theorem B.23, IH}) \\ \Leftrightarrow\ & \alpha p v \in [\![row'(s)]\!]_{m(T')} && (\text{Definition of } [\![-]\!]). \end{aligned}$$

□

Proposition B.26 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let $[\![m(T)]\!](z) \neq [\![\mathscr{X}]\!](z)$ for some $z \in \mathrm{GS}$, and $T' = (S, E \cup \mathtt{suf}(z), row')$ with $row'(t)(e) = [\![\mathscr{X}]\!](te)$. If T' is closed, then $row'(\varepsilon)(e) = 0$ for all $e \in E$, but $row'(\varepsilon)(z') = 1$ for some $z' \in \mathtt{suf}(z)$.*

Proof.

- Assume $[\![\mathscr{X}]\!](z) = 0$ and $[\![m(T)]\!](z) = 1$. Since $[\![m(T)]\!] \subseteq [\![m(T')]\!]$ by Theorem B.25, it follows $[\![m(T')]\!](z) = 1$. From Theorem 5.4 and the global assumptions we thus can deduce

$$1 = [\![m(T')]\!](z) = [\![row'(\varepsilon)]\!](z) = row'(\varepsilon)(z) = [\![\mathscr{X}]\!](z),$$

which contradicts $0 = [\![\mathscr{X}]\!](z)$.

- Assume $[\![\mathscr{X}]\!](z) = 1$ and $[\![m(T)]\!](z) = 0$. From Theorem 5.4 and the global assumptions we can deduce

$$1 = [\![\mathscr{X}]\!](z) = row'(\varepsilon)(z) = [\![row'(\varepsilon)]\!](z) = [\![m(T')]\!](z).$$

By Theorem B.23, there exists some decomposition $z = v\alpha p z'$ for $v \in \mathrm{GS}^-, z' \in \mathtt{suf}(z)$, such that for some $t \in S$:
(i) $row'(\varepsilon) \xrightarrow{v} row'(t)$ in $m(T')$ and $row(\varepsilon) \xrightarrow{v} row(t)$ in $m(T)$;
(ii) $\delta'(row'(t))(\alpha) = (p, row'(t'))$ for some $t' \in S$, but $\delta(row(t))(\alpha) = 0$.
For all $e \in E$ it follows

$$0 = row(t\alpha p)(e) = row'(t\alpha p)(e) = row'(t')(e) = row(t')(e),$$

since otherwise $\delta(row(t))(\alpha) \neq 0$ by the definition of δ. From Theorem 5.1 we can deduce $t' = \varepsilon$. Since $(v\alpha p)z' = z \in [\![m(T')]\!] = [\![row'(\varepsilon)]\!]$ and $row'(\varepsilon) \xrightarrow{v\alpha p} row'(t') = row'(\varepsilon)$, it follows $z' \in [\![row'(\varepsilon)]\!]$ by the definition of $[\![-]\!]$. From Theorem 5.4 we can conclude $z' \in row'(\varepsilon)$.

□

Proposition B.27 *If Algorithm 2 is instantiated with the language accepted by a finite normal automaton G-automaton $\mathscr{X}$, then T is a well-defined deterministic observation table at every step.*

Proof.

- Any G-automaton accepts a deterministic language. Since $row(s) \subseteq s^{-1}[\![\mathscr{X}]\!]$, and determinacy is preserved under derivatives, the determinacy of T is thus implied by the determinacy of $[\![\mathscr{X}]\!]$.
- In the initial step we have $S = \{\varepsilon\}$ and $E = \mathrm{At}$. In every step that follows the sets S and E are only extended. We thus have $\varepsilon \in S$ and $\mathrm{At} \subseteq E$ in every step.
- In the initial step $S = \{\varepsilon\}$ and $E = \mathrm{At}$ are clearly prefix- and suffix-closed, respectively. In the following steps S is only extended with strings of the shape $s\alpha p$ for $s \in S$, and E is only extended with the suffixes of some z. Hence S and E are prefix- and suffix-closed in every step.
- In the initial step $S = \{\varepsilon\}$, hence all rows indexed by elements in S are trivially disjoint. In the following steps we only add $s\alpha p$ to S, if $row(s\alpha p) \neq row(t)$ for all $t \in S$. Since disjoint rows do at no point collapse, we can deduce that $s \neq t$ implies $row(s) \neq row(t)$ for all $s, t \in S$ in every step.
- In the initial step we have $S = \{\varepsilon\}$, thus the observation that for all $s \in S$ with $s \neq \varepsilon$ we have $row(s) \neq \emptyset$ is trivially true. In the following steps we only add elements $s\alpha p$ with $row(s\alpha p) \neq \emptyset$ to S.
- Since $row(t)(e) = [\![\mathscr{X}]\!](te)$, the identity $row(s\alpha p)(e) = row(s)(\alpha p e)$, if $\alpha p e \in E$, follows from the associativity of string concatenation.

□

Theorem B.28 *If Algorithm 2 is instantiated with the language accepted by a finite normal automaton $\mathscr{X}$, then it terminates with a hypothesis isomorphic to $m(\mathscr{X})$.*

Proof. By Theorem B.27, T is a well-defined deterministic observation table at every step. We continue by showing that the algorithm yields $m(\mathscr{X})$ in finitely many steps. By Theorem 5.6 we have $|X| \leq |Y|$ for $X = \{row(s) \mid s \in S\}$ and $Y = \{w^{-1}[\![\mathscr{X}]\!] \mid w \in R(x)\}$ at any point of the algorithm. Since $\mathscr{X}$ is finite, the state-space Y of $m(\mathscr{X})$ is finite. At no point of the algorithm does the size of X decrease. Resolving a closedness defect strictly increases the size of X. Hence a closedness defect can only occur finitely many times. The only way the algorithm could not terminate is thus an infinite chain of negative equivalence queries, for which the subsequent suffix-enriched table is immediately closed again. By applying Theorem 5.8 twice, one observes that such a case can not occur. □

Lemma B.29 *Given a G-automaton $\mathscr{X} = (X, \delta, x)$, let $f(\mathscr{X}) := (X + \{\star\}, \langle \partial, \varepsilon \rangle, x)$ be the M-automaton* *with*

$$\partial(x)(\alpha p) := \begin{cases} y & \text{if } x \in X,\ \delta(x)(\alpha) = (p, y) \\ \star & \text{otherwise} \end{cases} \qquad \varepsilon(x)(\alpha) := \begin{cases} 1 & \text{if } x \in X,\ \delta(x)(\alpha) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then $[\![x]\!]_{\mathscr{X}} = [\![x]\!]_{f(\mathscr{X})}$ *for all* $x \in X$, *and* $[\![\star]\!]_{f(\mathscr{X})} = \emptyset$. *In particular,* $[\![f(\mathscr{X})]\!]_{f(\mathscr{X})} = [\![\mathscr{X}]\!]_{\mathscr{X}}$.

Proof. We simultaneously show i) $w \notin [\![\star]\!]_{f(\mathscr{X})}$ and ii) $w \in [\![x]\!]_{f(\mathscr{X})}$ if(f) $w \in [\![x]\!]_{\mathscr{X}}$, for all $w \in \mathrm{GS}$ and $x \in X$ by induction on the length of w.

- For the induction base assume $w = \alpha$, then we observe the following equivalences for i):

$$\begin{aligned} \alpha \in [\![\star]\!]_{f(\mathscr{X})} &\Leftrightarrow \varepsilon(\star)(\alpha) = 1 && (\text{Definition of } [\![-]\!]_{f(\mathscr{X})}) \\ &\Leftrightarrow 0 = 1 && (\text{Definition of } \varepsilon) \\ &\Leftrightarrow \text{false} && (0 \neq 1). \end{aligned}$$

  Similarly, we derive the following chain for ii):

$$\begin{aligned} \alpha \in [\![x]\!]_{f(\mathscr{X})} &\Leftrightarrow \varepsilon(x)(\alpha) = 1 && (\text{Definition of } [\![-]\!]_{f(\mathscr{X})}) \\ &\Leftrightarrow \delta(x)(\alpha) = 1 && (\text{Definition of } \varepsilon,\ x \in X) \\ &\Leftrightarrow \alpha \in [\![x]\!]_{\mathscr{X}} && (\text{Definition of } [\![-]\!]_{\mathscr{X}}). \end{aligned}$$

- For the induction step, let $w = \alpha p v$ for $v \in \mathrm{GS}$, then we observe the following for i):

$$\begin{aligned} \alpha p v \in [\![\star]\!]_{f(\mathscr{X})} &\Leftrightarrow \partial(\star)(\alpha p) = y,\ v \in [\![y]\!]_{f(\mathscr{X})} && (\text{Definition of } [\![-]\!]_{f(\mathscr{X})}) \\ &\Leftrightarrow \partial(\star)(\alpha p) = \star,\ v \in [\![\star]\!]_{f(\mathscr{X})} && (\text{Definition of } \partial) \\ &\Leftrightarrow \text{false} && (\text{IH}). \end{aligned}$$

  Analogously, we deduce for ii):

$$\begin{aligned} &\alpha p v \in [\![x]\!]_{f(\mathscr{X})} \\ \Leftrightarrow\ &\partial(x)(\alpha p) = y,\ v \in [\![y]\!]_{f(\mathscr{X})} && (\text{Definition of } [\![-]\!]_{f(\mathscr{X})}) \\ \Leftrightarrow\ &\delta(x)(\alpha) = (p, y),\ v \in [\![y]\!]_{f(\mathscr{X})} \text{ or } \delta(x)(\alpha) \in 2,\ v \in [\![\star]\!]_{f(\mathscr{X})} && (\text{Definition of } \partial) \\ \Leftrightarrow\ &\delta(x)(\alpha) = (p, y),\ v \in [\![y]\!]_{\mathscr{X}} \text{ or false} && (\text{IH}) \\ \Leftrightarrow\ &\alpha p v \in [\![x]\!]_{\mathscr{X}} && (\text{Definition of } [\![-]\!]_{\mathscr{X}}). \end{aligned}$$

In particular, $[\![f(\mathscr{X})]\!]_{f(\mathscr{X})} = [\![x]\!]_{f(\mathscr{X})} = [\![x]\!]_{\mathscr{X}} = [\![\mathscr{X}]\!]_{\mathscr{X}}$. □

Corollary B.30 *Let* $\mathscr{X}$ *be a normal* G*-automaton, then* $f(m(\mathscr{X})) \cong m(f(\mathscr{X}))$ *as* M*-automata.*

Proof. From Theorem 6.1 and Theorem 4.6 we can deduce that $f(m(\mathscr{X}))$ accepts $[\![\mathscr{X}]\!]$, which is also accepted by $m(f(\mathscr{X}))$.

By Theorem 4.7 $[\![-]\!]_{m(\mathscr{X})}$ is injective. Since by Theorem 4.7 and Theorem 4.5 $m(\mathscr{X})$ is normal and reachable, we know that $[\![-]\!]_{m(\mathscr{X})}$ never evaluates to the empty set. From Theorem 6.1 we thus can deduce that $[\![-]\!]_{f(m(\mathscr{X}))}$ is injective.

It is not hard to see that if a state is reachable in $\mathscr{Y}$, then it is reachable in $f(\mathscr{Y})$. The element $\star$ is reachable in $f(\mathscr{Y})$ in particular if $\mathscr{Y}$ is reachable and normal. Hence, since $m(\mathscr{X})$ is reachable and normal by Theorem 4.5 and Theorem 4.7, respectively, $f(m(\mathscr{X}))$ is reachable.

The automaton $f(m(\mathscr{X}))$ thus accepts the same language as $m(f(\mathscr{X}))$, is observable, and reachable. By uniqueness, $f(m(\mathscr{X}))$ and $m(f(\mathscr{X}))$ are thus isomorphic. □

Lemma B.31 *Let* $a, b \in \mathbb{N}_{\geq 3}$, *then* $a * b > a + b$.

Proof. We prove the statement by induction on $a \in \mathbb{N}_{\geq 3}$.

- For the induction base, assume $a = 3$. We show that $3 * b > 3 + b$ for all $b \in \mathbb{N}_{\geq 3}$ by induction on b. In the induction base, $b = 3$, the statement immediately is implied by $3 * 3 = 9 > 6 = 3 + 3$. Assume the statement is true for some $b \geq 3$. The induction step follows from

$$3 * (b + 1) = 3 * b + 3 > (3 + b) + 3 = 6 + b > 3 + (b + 1).$$

- Assume the statement is true for $a \geq 3$. The induction step follows from

$$(a + 1) * b = (a * b) + b > (a + b) + b > (a + 1) + b.$$

□

Proposition B.32 *Algorithm 1 requires at most $O(a * (|\mathrm{At}| * b))$ many membership queries to $[\![e]\!]$ for learning a M-automaton representation of e, whereas Algorithm 2 requires at most $O(a*(|\mathrm{At}|+b))$ many membership queries to $[\![e]\!]$ for learning a G-automaton representation of e, for some*[14] *integers $a, b \in \mathbb{N}$.*

Proof. We first derive the maximum number of entries a table indexed by S and E can have during a run of L^* for generalised languages with input A and output B. Since we use a suffix-strategy for the handling of counterexamples (opposed to a prefix-strategy), our presentation slightly differs from the one in [3]. Let k denote the cardinality of the alphabet A. The number of states of the minimal Moore automaton accepting the target language is referred to by n, and the maximum length of a counterexample by m. The size of S is bounded by n. In the worst case, the sets S and $S \cdot A$ are disjoint. The cardinality of $S \cup S \cdot A$ is thus bounded by $n + n * k$. The maximum number of strings in E is $1 + m * (n - 1)$. This is because E is instantiated with ε, and only extended with suffixes of counterexamples. Each counterexample has at most m suffixes, and there can only be $n - 1$ counterexamples, since any counterexample leads to a closedness defect, resolving which increases the size of S, which is instantiated with ε, and bounded in size by n. A table can thus have at most $(n + n * k) * (1 + m * (n - 1))$, or $O(m * n^2 * k)$, many entries.

In the case of $A = (\mathrm{At} \cdot \Sigma)$ and $B = 2^{\mathrm{At}}$, each entry requires $|\mathrm{At}|$ many membership queries. Overall Algorithm 1 thus requires at most

$$O(n * |\mathrm{At}| * |\Sigma| * (|\mathrm{At}| * m * n))$$

many membership queries to learn a deterministic guarded string language.

We now derive a bound to the number of membership queries GL^* requires. As before, let m denote the maximum length of a counterexample, and n the number of states of the minimal Moore automaton accepting the target language. The cardinality of the set S is bounded by the number of states in the minimal GKAT automaton accepting the target language, which by Theorem 6.2 is $n-1$. The cardinality of $S \cup S \cdot (\mathrm{At} \cdot \Sigma)$ is thus bounded by $(n-1)+(n-1)*|\mathrm{At}|*|\Sigma|$. The maximum number of strings in E is $|\mathrm{At}|+ m*(n-1)$. This is because E is instantiated with At, and only extended with suffixes of counterexamples. Each counterexample has at most m suffixes, and there can only be $n - 1$ counterexamples. Indeed, assume there are $u > n - 1$ counterexamples. Since resolving a closedness defect increases the size of S, which is instantiated with ε, and in size bounded by $n - 1$, there can be at most $(n - 1) - 1 = n - 2$ counterexamples for which the extended table is not closed. Thus there must be at least $u - (n - 2) = u - n + 2 \geq n - n + 2 = 2$ counterexamples for which the extended table is closed. This is a contradiction, since Theorem 5.8 implies that this can be the case for at most 1 counterexample. A table can thus have at most $((n - 1) + (n - 1) * |\mathrm{At}| * |\Sigma|) * (|\mathrm{At}| + m * (n - 1))$ entries. Each entry requires one membership query. Overall Algorithm 2 requires at most

$$O(n * |\mathrm{At}| * |\Sigma| * (|\mathrm{At}| + m * n))$$

[14] Let m be the maximum length of a counterexample and n the size of the minimal Moore automaton accepting $[\![e]\!]$, then $a = n * |\mathrm{At}| * |\Sigma|$ and $b = m * n$. As Figure 6 shows, GL^* can be more efficient than L^* even for small $|\mathrm{At}|$.

many membership queries to learn a deterministic guarded string language. The statement follows by setting $a := n * |\mathrm{At}| * |\Sigma|$ and $b := m * n$. ☐

Lemma B.33 *Let $T = (S, E, row)$ be a closed deterministic observation table with $row(t)(e) = [\![\mathscr{X}]\!](te)$ for all $t \in S \cup S \cdot (\mathrm{At} \cdot \Sigma)$, $e \in E$. Let $[\![m(T)]\!](z) \neq [\![\mathscr{X}]\!](z)$ for some $z \in \mathrm{GS}$, and $z' := \min(A_z)$* [15]*. If $T' = (S, E \cup \mathtt{suf}(z'), row')$ with $row'(t)(e) = [\![\mathscr{X}]\!](te)$ is closed, then $row'(\varepsilon)(e) = 0$ for all $e \in E$, but $row'(\varepsilon)(z') = 1$.*

Proof. We begin by showing that $z \notin \mathrm{At}$. Let us assume the opposite, $z = \alpha \in \mathrm{At} \subseteq E$. In that case, it follows

$$\begin{aligned}
[\![m(T)]\!](z) &= [\![row(\varepsilon)]\!](\alpha) && (\text{Definition of } [\![-]\!],\ z)\\
&= row(\varepsilon)(\alpha) && (\text{Theorem 5.4})\\
&= [\![\mathscr{X}]\!](\alpha) && (row(t)(e) = [\![\mathscr{X}]\!](te))\\
&= [\![\mathscr{X}]\!](z) && (\text{Definition of } z)
\end{aligned}$$

which is a contradiction. Thus there exists a decomposition $z = \varepsilon\alpha p z'$ for some $z' \in \mathtt{suf}(z)$. The former immediately implies that the set A_z is non-empty. Hence the shortest suffix $z' := \min(A_z)$ is well-defined. By construction, we have $row(\varepsilon) \xrightarrow{v} row(s_v)$, $x \xrightarrow{s_v} x_{s_v}$, and $[\![row(s_v)]\!](\alpha p z') \neq [\![x_{s_v}]\!](\alpha p z')$.

- Assume $[\![x_{s_v}]\!](\alpha p z') = 0$ and $[\![row(s_v)]\!](\alpha p z') = 1$, then there exists $s_{v\alpha p} \in S$ with $row(\varepsilon) \xrightarrow{v} row(s_v) \xrightarrow{\alpha p} row(s_{v\alpha p})$ such that

$$\begin{aligned}
1 &= [\![row(s_v)]\!](\alpha p z') && (\text{Assumption})\\
&= [\![row(s_{v\alpha p})]\!](z') && (\text{Definition of } [\![-]\!])\\
&= [\![row'(s_{v\alpha p})]\!](z') && (\text{Theorem B.25})\\
&= row'(s_{v\alpha p})(z') && (\text{Theorem 5.4})\\
&= row'(s_v\alpha p)(z') && (\text{Definition of } row')\\
&= [\![\mathscr{X}]\!](s_v\alpha p z') && (row'(t)(e) = [\![\mathscr{X}]\!](te))\\
&= [\![x_{s_v}]\!](\alpha p z') && (\text{Definition of } [\![-]\!])
\end{aligned}$$

  which contradicts $0 = [\![x_{s_v}]\!](\alpha p z')$.

- Assume $[\![x_{s_v}]\!](\alpha p z') = 1$ and $[\![row(s_v)]\!](\alpha p z') = 0$, then there exists $s_{v\alpha p} \in S$ with $row'(\varepsilon) \xrightarrow{v} row'(s_v) \xrightarrow{\alpha p} row'(s_{v\alpha p})$ such that

$$\begin{aligned}
1 &= [\![x_{s_v}]\!](\alpha p z') && (\text{Assumption})\\
&= [\![\mathscr{X}]\!](s_v\alpha p z') && (\text{Definition of } [\![-]\!])\\
&= row'(s_v\alpha p)(z') && (row'(t)(e) = [\![\mathscr{X}]\!](te))\\
&= row'(s_{v\alpha p})(z') && (\text{Definition of } row')\\
&= [\![row'(s_{v\alpha p})]\!](z') && (\text{Theorem 5.4})\\
&= [\![row'(s_v)]\!](\alpha p z') && (\text{Definition of } [\![-]\!])
\end{aligned}$$

  By Theorem B.23 there thus are two possibilities:
  · Assume $row(s_v) \xrightarrow{\alpha p} row(s_{v\alpha p})$, then there are two options:
  If $z' \notin \mathrm{At}$, we can deduce a contradiction to the minimality of z' in A_z.

[15] $A_z := \{z' \in \mathtt{suf}(z) \mid z = v\alpha p z',\ row(\varepsilon) \xrightarrow{v} row(s_v),\ x \xrightarrow{s_v} x_{s_v},\ [\![row(s_v)]\!](\alpha p z') \neq [\![x_{s_v}]\!](\alpha p z')\}$

If $z' \in \mathrm{At} \subseteq E$, then

$$\begin{aligned}
0 &= [\![row(s_v)]\!](\alpha p z') && \text{(Assumption)} \\
&= [\![row(s_{v\alpha p})]\!](z') && (row(s_v) \xrightarrow{\alpha p} row(s_{v\alpha p})) \\
&= row(s_{v\alpha p})(z') && \text{(Theorem 5.4)} \\
&= [\![\mathscr{X}]\!](s_{v\alpha p} z') && (row(t)(e) = [\![\mathscr{X}]\!](te)) \\
&= [\![x_{s_{v\alpha p}}]\!](z') && \text{(Definition of } [\![-]\!]) \\
&= [\![x_{s_v}]\!](\alpha p z') && \text{(Definition of } [\![-]\!])
\end{aligned}$$

which is a contradiction to $[\![x_{s_v}]\!](\alpha p z') = 1$.

· Assume $\delta(row(s_v))(\alpha) = 0$, then we have, for all $e \in E$,

$$\begin{aligned}
0 &= row(s_v \alpha p)(e) && (\delta(row(s_v))(\alpha) = 0) \\
&= row'(s_v \alpha p)(e) && (row(t)(e) = row'(t)(e)) \\
&= row'(s_{v\alpha p})(e) && \text{(Definition of } row') \\
&= row(s_{v\alpha p})(e) && (row(t)(e) = row'(t)(e))
\end{aligned}$$

By Theorem 5.1, it thus must be that $s_{v\alpha p} = \varepsilon$, which implies the claim.

□

C Similarity

The primitive algebraic notion of the original axiomatisation of GKAT [37] is term equivalence, and its coalgebraic analogue is bisimulation. In [37] it has been proposed to replace term equivalence with a partial order between terms. Inspired by this idea, we introduce the notion of similarity, that is to bisimulation, what a partial order is to equality (term equivalence). Similarity has been studied for general coalgebras [5,18,16,28].

Definition C.1 Let $\mathscr{X}$ be a G-coalgebra. A *simulation* is a binary relation $R \subseteq X \times X$, such that if xRy, then:

- if $\delta(x)(\alpha) = 1$, then $\delta(y)(\alpha) = 1$;
- if $\delta(x)(\alpha) = (p, x')$, then $\delta(y)(\alpha) = (p, y')$ and $x'Ry'$ for some $y' \in X$.

States x and y are *similar*, $x \precsim y$, if there exists a simulation relating x to y.

Lemma C.2 *$x \simeq y$ if and only if $x \precsim y$ and $y \precsim x$.*

Proof.

- Assume the bisimilarity $x \simeq y$ is witnessed by some relation R. We show that R witnesses the similarity $x \precsim y$. Clearly xRy by construction. Let $x'Ry'$ for arbitrary $x', y' \in X$, then we find:
  · If $\delta(x')(\alpha) = 1$ it follows $\delta(y') = 1$ since R is a bisimulation.
  · If $\delta(x')(\alpha) = (p, x'')$ it follows $\delta(y')(\alpha) = (p, y'')$ and $x''Ry''$ for some $y'' \in X$, since R is a bisimulation.
  Similarly, we show that the reverse relation R^r witnesses the similarity $y \precsim x$. Clearly yR^rx, since by construction xRy. Let $y'R^rx'$, i.e. $x'Ry'$, for arbitrary $x', y' \in X$, then we find:
  · If $\delta(y')(\alpha) = 1$ it follows $\delta(x')(\alpha) = 1$, since as R is a bisimulation we could otherwise falsely deduce $\delta(y')(\alpha) = 0$ or $\delta(y')(\alpha) \notin 2$.
  · If $\delta(y')(\alpha) = (p, y'')$, it follows $\delta(x')(\alpha) = (p, x'')$ with $y''R^rx''$, i.e. $x''Ry''$. Indeed, since R is a bisimulation, if $\delta(x')(\alpha) \in 2$, it falsely follows $\delta(y')(\alpha) \in 2$, and if $\delta(x')(\alpha) = (q, x'')$, it follows $\delta(y')(\alpha) = (q, y''')$ with $x''Ry'''$, as R is a bisimulation. It remains to observe $(p, y'') = \delta(y')(\alpha) = (q, y''')$, which implies $p = q$ and $y'' = y'''$.

- Assume $x \precsim y$ and $y \precsim x$ are witnessed by relations $R_1 \subseteq X \times X$ and $R_2 \subseteq X \times X$, respectively. We define $R := R_1 \cap R_2^r$, and show that R is a bisimulation witnessing $x \simeq y$. Clearly xR_1y and xR_2^ry, i.e. xRy. Thus let $x'Ry'$ for arbitrary $x', y' \in X$, then we find:
  · If $\delta(x')(\alpha) = 0$ it follows $\delta(y')(\alpha) = 0$. Indeed, if $\delta(y')(\alpha) = 1$ or $\delta(y')(\alpha) \notin 2$, we could falsely deduce $\delta(x')(\alpha) = 1$ or $\delta(x')(\alpha) \notin 2$, as $y'R_2x'$, and R_2 is a simulation.
  · If $\delta(x')(\alpha) = 1$, it follows $\delta(y')(\alpha) = 1$, since $x'R_1y'$, and R_1 is a simulation.
  · If $\delta(x')(\alpha) = (p, x'')$, it follows (i) $\delta(y')(\alpha) = (p, y'')$ with $x''R_1y''$, since $x'R_1y'$, and R_1 is a simulation; and (ii) $y''R_2x''$, since $y'R_2x'$ implies $\delta(x')(\alpha) = (p, x''') = (p, x'')$ for $y''R_2x'''$. Thus we find by definition of R that $x''Ry''$.

□

Lemma C.3 *If $x \precsim y$ then $[\![x]\!] \subseteq [\![y]\!]$.*

Proof. The proof is similar to the one of its bisimilar counterpart [37][Lemma 5.2].
We prove $w \in [\![x]\!]$ implies $w \in [\![y]\!]$ for all $w \in \mathrm{GS}$ by induction on the length of w.

- For the induction base, let $w = \alpha$, then:

$$\begin{aligned}
\alpha \in [\![x]\!] &\Leftrightarrow \delta(x)(\alpha) = 1 && \text{(Definition of } [\![-]\!]) \\
&\Rightarrow \delta(y)(\alpha) = 1 && (x \precsim y) \\
&\Leftrightarrow \alpha \in [\![y]\!] && \text{(Definition of } [\![-]\!])
\end{aligned}$$

- For the induction step, let $w = \alpha p v$, then we derive:

$$\begin{aligned}
\alpha p v \in [\![x]\!] &\Leftrightarrow \delta(x)(\alpha) = (p, x'),\ v \in [\![x']\!] && \text{(Definition of } [\![-]\!]) \\
&\Rightarrow \delta(y)(\alpha) = (p, y'),\ v \in [\![y']\!] && (x \precsim y,\ \text{IH}) \\
&\Leftrightarrow \alpha p v \in [\![y]\!] && \text{(Definition of } [\![-]\!])
\end{aligned}$$

□

Lemma C.4 *Let $L_1, L_2 \in \mathscr{L}$, then $L_1 \subseteq L_2$ if(f) $L_1 \precsim L_2$ in $(\mathscr{L}, \delta^{\mathscr{L}})$.*

Proof. Theorem C.3 shows that $L_1 \precsim L_2$ implies $L_1 = [\![L_1]\!] \subseteq [\![L_2]\!] = L_2$.
Conversely, we show that $\subseteq$ is a simulation. Assume $L_1 \subseteq L_2$, then we compute:

$$\begin{aligned}
\delta^{\mathscr{L}}(L_1)(\alpha) = 1 &\Leftrightarrow \alpha \in L_1 && \text{(Definition of } \delta^{\mathscr{L}}) \\
&\Rightarrow \alpha \in L_2 && (L_1 \subseteq L_2) \\
&\Leftrightarrow \delta^{\mathscr{L}}(L_2)(\alpha) = 1 && \text{(Definition of } \delta^{\mathscr{L}})
\end{aligned}$$

Moreover, we find:

$$\begin{aligned}
\delta^{\mathscr{L}}(L_1)(\alpha) = (p, L^1) &\Leftrightarrow \emptyset \neq L^1 = (\alpha p)^{-1} L_1 && \text{(Definition of } \delta^{\mathscr{L}}) \\
&\Rightarrow \emptyset \neq L^1 = (\alpha p)^{-1} L_1 \subseteq (\alpha p)^{-1} L_2 = L^2 && (L_1 \subseteq L_2) \\
&\Leftrightarrow \delta^{\mathscr{L}}(L_2)(\alpha) = (p, L^2),\ L^1 \subseteq L^2 && \text{(Definition of } \delta^{\mathscr{L}})
\end{aligned}$$

□

Corollary C.5 *Let $\mathscr{X}$ be a normal G-coalgebra, then $x \precsim y$ if(f) $[\![x]\!] \subseteq [\![y]\!]$.*

Proof. The proof is similar to the one of its bisimilar counterpart [37][Corollary 5.9].
From Theorem C.3 it follows that $x \precsim y$ implies $[\![x]\!] \subseteq [\![y]\!]$.
Conversely, assume $[\![x]\!] \subseteq [\![y]\!]$. We define a relation $R := \{(s, t) \in X \times X \mid [\![s]\!] \subseteq [\![t]\!]\}$. In order to show $x \precsim y$ it is sufficient to prove that R is a simulation. Since $\mathscr{X}$ is normal, $[\![-]\!]$ is a G-coalgebra homomorphism.

- Suppose sRt and $\delta(s)(\alpha) = 1$. As $[\![-]\!]$ is a G-coalgebra homomorphism it follows $\delta^{\mathscr{L}}([\![s]\!])(\alpha) = 1$. Since $[\![s]\!] \subseteq [\![t]\!]$ implies $[\![s]\!] \precsim [\![t]\!]$ by Theorem C.4, we thus can deduce $\delta^{\mathscr{L}}([\![t]\!])(\alpha) = 1$. Since $[\![-]\!]$ is a G-coalgebra homomorphism, we can conclude $\delta(t)(\alpha) = 1$.
- Suppose sRt and $\delta(s)(\alpha) = (p, s')$. Since $[\![-]\!]$ is a G-coalgebra homomorphism it follows $\delta^{\mathscr{L}}([\![s]\!])(\alpha) = (p, [\![s']\!])$. Since $[\![s]\!] \subseteq [\![t]\!]$ implies $[\![s]\!] \precsim [\![t]\!]$ by Theorem C.4, we deduce $\delta^{\mathscr{L}}([\![t]\!])(\alpha) = (p, L)$ for some $L \in \mathscr{L}$ with $[\![s']\!] \precsim L$ in $\mathscr{L}$. Since $[\![-]\!]$ is a G-coalgebra homomorphism, it follows $L = [\![t']\!]$ with $\delta(t)(\alpha) = (p, t')$. Thus we have $[\![s']\!] \precsim [\![t']\!]$, or equivalently $[\![s']\!] \subseteq [\![t']\!]$ by Theorem C.4. The latter implies $s'Rt'$ by definition of R. Thus we can summarize as desired $\delta(t)(\alpha) = (p, t')$ and $s'Rt'$.

$\square$