A Probabilistic Kleene Theorem
Benedikt Bollig, Paul Gastin, Benjamin Monmege, Marc Zeitoun

To cite this version:

Benedikt Bollig, Paul Gastin, Benjamin Monmege, Marc Zeitoun. A Probabilistic Kleene Theorem. Automated Technology for Verification and Analysis (ATVA’12), Oct 2012, Thiruvananthapuram, India. pp.400-415, 10.1007/978-3-642-33386-6_31 . hal-00909042

HAL Id: hal-00909042
https://hal.archives-ouvertes.fr/hal-00909042
Submitted on 26 Nov 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A Probabilistic Kleene Theorem

Benedikt Bollig¹, Paul Gastin¹, Benjamin Monmege¹, and Marc Zeitoun²

¹ LSV, ENS Cachan, CNRS & Inria, France, firstname.lastname@lsv.ens-cachan.fr
² LaBRI, Univ. Bordeaux & CNRS, France, mz@labri.fr

Abstract. We provide a Kleene Theorem for (Rabin) probabilistic automata over finite words. Probabilistic automata generalize deterministic finite automata and assign to a word an acceptance probability. We provide probabilistic expressions with probabilistic choice, guarded choice, concatenation, and a star operator. We prove that probabilistic expressions and probabilistic automata are expressively equivalent. Our result actually extends to two-way probabilistic automata with pebbles and corresponding expressions.

1 Introduction

Kleene’s Theorem states the equivalence of rational and recognizable languages in the free monoids. Naturally, this fundamental result has been generalized to various settings and in particular to quantitative extensions of classical languages, called formal power series [24,23,4].

The present paper aims at a probabilistic counterpart of Kleene’s Theorem. There are actually a variety of models for probabilistic systems, comprising Segala systems, generative systems, stratified systems, Markov chains, etc. (see [29,25] for overviews). Those models may involve non-determinism and generate some behavior according to probability distributions over states. Alternatively, they may make a probabilistic decision depending on the input letter, like (reactive) probabilistic automata [20]. The latter go back to Rabin [21] and are an object of ongoing research considering decision problems such as emptiness, language equivalence [24,28,9,10,18], and the value 1 problem [17].

Our starting point of view is that expressions and automata shall represent quantitative properties of words. In particular, rather than at bisimulation equivalence, we are looking at language equivalence in terms of formal power series (i.e., mappings from strings to elements from the real-valued interval [0, 1]). This actually has an immediate impact on the choice of both the automaton model and the syntax of expressions that are supposed to characterize it. On the automata side, a probabilistic decision should depend on the given input. Therefore, we consider probabilistic automata. On the specification side, we would like to adopt concepts from rational expressions. In this paper, we actually provide a simple fragment of classical weighted rational expressions over the

* Supported by ANR 2010 BLAN 0202 01 FREC, LIA InForMéL.
nonnegative real numbers, including a star operator and concatenation. The star operator has to be handled with care, though. It comes with a subtle restriction to make sure that an expression associates with every word a probability. In this way, we obtain a class of probabilistic expressions that have the same expressive power as probabilistic automata. Translations forth and back are effective so that decidability results for automata directly carry over to expressions.

Actually, we prove a more general result. Expressions are extended in such a way that they capture two-way probabilistic automata \cite{14,22} and automata with pebbles (similar to two-way word automata and tree-walking automata). Our expressions can then be considered as a probabilistic generalization of XPath \cite{19,27}. Note that (non-probabilistic) two-way automata are in fact an appropriate machine model for compiling XPath queries \cite{5}. The concept presented in this paper may therefore constitute a first step towards probabilistic database query languages: an expression is considered as a query, and an equivalent automaton can be used as a tool for evaluating queries efficiently (see \cite{16} for recent developments on weighted query evaluation).

**Related Work.** It has to be noted that there have been numerous approaches to characterizing probabilistic systems in terms of algebraic expressions and process calculi \cite{29,7,12,11}. A unifying framework is due to Silva et al. \cite{26}, who consider probabilistic systems in a general coalgebraic setting. This allows them to derive algebraic expressions and a corresponding Kleene Theorem, as well as full axiomatizations for many of those (and even for weighted automata over arbitrary semirings). Their and above-mentioned works are mainly aiming at axiomatization of probabilistic-system behaviors in terms of bisimulation equivalence, so their focus is on system models including non-determinism and generative probability distributions. In this paper, we consider probabilistic automata, which are a more appropriate machine model for our purpose, i.e., for evaluating queries. Moreover, while the syntax of process-algebraic expressions is tailored to modeling probabilistic systems and uses action prefixing, fixed points, and process variables, we provide expressions with concatenation and a proper Kleene star. Thus, our expressions are closer to language-theoretic operations and more convenient to use in query languages. So far, there have been only few attempts to define quantitative query languages. In \cite{15}, Flesca et al. introduce a weighted XPath. Their approach, however, does not extend to probabilistic automata. Note that the fact that we also consider two-way devices distinguishes our work from all above-mentioned references. To the best of our knowledge, we present the first Kleene-Schützenberger correspondence for probabilistic two-way automata.

**Outline.** In Section 2, after some motivating example, we recall the definition of (reactive) probabilistic automata, introduce our probabilistic regular expressions, and present a corresponding Kleene Theorem. A part of the proof of this theorem is postponed to Section 4, where a more general result is shown for two-way probabilistic automata and corresponding generalized expressions (which are introduced in Section 3): automata and expressions are expressively equivalent and can be transformed effectively into each other.
Fig. 1. A probabilistic automaton equivalent to \( \left( \frac{1}{6}a + \frac{1}{2}b \right)^* \cdot \frac{1}{3}a + b \)

2 Probabilistic Automata and Expressions

Preliminaries. We fix a finite alphabet \( A \). We restrict our attention to nonempty words over \( A \), i.e., sequences \( w = a_0 \cdots a_{n-1} \in A^+ \) with \( n \geq 1 \) and \( a_i \in A \) for every \( i \). The length \( n \) of \( w \) is denoted \( |w| \), and \( \text{pos}(w) = \{0, \ldots, |w|\} \) is the set of positions of \( w \). The last position of index \( n \) is added to facilitate the definition of runs in two-way automata. To be able to deal with infinite sums over the non-negative real numbers, we extend \( \mathbb{R}_{\geq 0} \) to \( \mathbb{R}_{\geq 0}^\infty = \mathbb{R}_{\geq 0} \cup \{\infty\} \). In other words, we consider the continuous semiring \((\mathbb{R}_{\geq 0}^\infty, +, \cdot, 0, 1)\) where \( \infty \) is assigned to any infinite sum that does not converge.

2.1 Probabilistic Automata

We consider classical probabilistic finite automata (PFA) \([21,20]\). A PFA over alphabet \( A \) is a tuple \( A = (Q, \iota, \text{Acc}, \mathbb{P}) \) where \( Q \) is the finite set of states, \( \iota \in Q \) is the initial state, and \( \text{Acc} \subseteq Q \) is the set of final states. Moreover, \( \mathbb{P} : Q \times A \times Q \to [0,1] \) is a function that assigns a probability to each transition. PFA are reactive automata, whose probabilistic choice depends on the current input letter. Thus, we require that \( \sum_{q' \in Q} \mathbb{P}(q, a, q') \leq 1 \) for all \( (q, a) \in Q \times A \). We will moreover assume that a final state has no outgoing transitions with positive probability: \( \mathbb{P}(q, a, q') > 0 \) implies \( q \notin \text{Acc} \). An example PFA is depicted in Fig. 1 where 1 is the initial state and 3 is the only final state. Transitions with probability 0 are omitted.

An accepting run of \( A \) over \( w = a_0 \cdots a_{n-1} \in A^+ \) is a sequence of transitions \( \rho = \delta_1 \cdots \delta_n \) such that \( \delta_i = (q_{i-1}, a_{i-1}, q_i) \) with \( q_0 = \iota \) and \( q_n \in \text{Acc} \). Given a run \( \rho \), we set \( \mathbb{P}(\rho) = \prod_{i=1}^n \mathbb{P}(\delta_i) \). The semantics of the PFA \( A \) is the mapping (series) \( \llbracket A \rrbracket : A^+ \to [0,1] \) given by \( \llbracket A \rrbracket(w) = \sum_{\rho} \mathbb{P}(\rho) \), where the sum ranges over all accepting runs \( \rho \) over \( w \). For instance, given the automaton of Fig. 1, we have \( \llbracket A \rrbracket(aab) = \frac{1}{4} + \frac{1}{6} = \frac{5}{12} \).

2.2 Probabilistic Expressions

While PFAs are a machine model, we are aiming at denotational probabilistic regular expressions with the same expressiveness as PFAs. We start with the definition of classical weighted expressions (WEs) given by the syntax

\[
E ::= s \mid a \mid E + E \mid E \cdot E \mid E^*
\]
with \( s \in \mathbb{R}_{\geq 0}^\infty \) and \( a \in A \). In the following, we often simply write \( EF \) instead of \( E \cdot F \). Also, we let \( E^0 \triangleq 1 \) and \( E^{m+1} = EE^m \) for \( m \geq 0 \). The semantics of a \( WE \) \( E \) is a mapping \([E] : A^+ \to \mathbb{R}_{\geq 0}^\infty \) which is defined inductively by

\[
[s](w) = \begin{cases} 
  s & \text{if } w = \varepsilon \\
  0 & \text{otherwise} 
\end{cases} \\
[a](w) = \begin{cases} 
  1 & \text{if } w = a \\
  0 & \text{otherwise} 
\end{cases} \\
\[E_1 + E_2\](w) = \[E_1\](w) + \[E_2\](w) \\
\[E^*\](w) = \sum_{m \in \mathbb{N}} \[E^m\](w) \\
\[E_1 \cdot E_2\](w) = \sum_{w = uv} [E_1](u) \cdot [E_2](v) .
\]

In the following, we consider expressions modulo the following trivial identities:

\[
0 + E \equiv E + 0 \equiv E \\
E \cdot 0 \equiv 0 \cdot E \equiv 0 \\
E \cdot 1 \equiv 1 \cdot E \equiv E \\
0^* \equiv 1
\]

We introduce below probabilistic regular expressions (PREs) as a fragment of WE. We have to restrict WE since otherwise values greater than 1 could be obtained. For instance, the WE \((a + ab)(ba + a)\) should not be a PRE since it evaluates to 2 on the word \(aba\). The restriction will be both on sum and star. Since we aim at PREs which are equivalent to PFA, let us examine first which type of WE are obtained from PFA. A transition \( \delta = (q, a, q') \) with probability \( P(\delta) = s \) could be denoted by the expression \( sa \). Applying classical algorithms to build a regular expression from finite-state automata, we then obtain, for the automaton in Fig. 1, the expression \( \llbracket \frac{1}{2}a(a+b) + \frac{1}{2}a \rrbracket^* \cdot (\frac{1}{2}a + b) \). Now, the expression \( \llbracket \frac{1}{2}a(a+b) + \frac{1}{2}a \rrbracket^* \cdot (a + b) \), obtained by changing the subexpression \( \frac{1}{2}a \) into \( a \), should be disallowed, because it corresponds to an automaton violating condition \( \sum_{q'' \in Q} P(q, a, q') \leq 1 \). On the other hand, \( \llbracket \frac{1}{2}a(a+b) + \frac{1}{2}a \rrbracket^* \cdot (\frac{1}{2}a + \frac{1}{4}b) \) would be acceptable: we obtain a corresponding PFA from the automaton depicted in Fig. 1 by setting \( P(1, b, 3) = \frac{1}{2} \).

**Definition 1.** Probabilistic regular expressions (PREs) is the fragment of WE built inductively as follows:

- **Atoms** \( s \in [0, 1] \) and \( a \in A \) are PREs.
- \((+a)\) If \( (E_a)_{a \in A} \) are PREs, then \( \sum_{a \in A} a \cdot E_a \) is a PRE.
- \((+s)\) If \( E \) and \( F \) are PREs and \( s \in [0, 1] \), then \( s \cdot E + (1 - s) \cdot F \) is a PRE.
- \((\cdot)\) If \( E \) and \( F \) are PREs, then \( E \cdot F \) is a PRE.
- \((*)\) If \( E + F \) is a PRE, then \( E^* \cdot F \) is a PRE.
- **ACD** Every WE that is obtained from a PRE by applying commutativity of +, associativity of + or ·, or distributivity of · over + is a PRE.

There are two guarded sums. The first one \((+a)\) is deterministic and guarded by the next letter to be read. The second one \((+s)\) is probabilistic. Also, the star operation contains an implicit choice which is either to iterate again the expression or to exit the loop. This choice also has to be guarded which is the reason for the precondition \( E + F \in \text{PRE} \) in the rule \((*)\). The guard could be deterministic as in \((ab)^*b\) or probabilistic as in \((\frac{1}{2}(aa + bb))^*\frac{1}{2}(a + b)\). Finally, with the above restrictions, we lose the classical ACD identities, hence we enforce
these properties explicitly with the ACD-rules which allow to rewrite a PRE in order to apply the star rule as needed.

Since PREs form a fragment of WEs, the semantics is inherited. From Theorem 1 below, PREs are equivalent to PFAs. We deduce that the semantics of $E \in \text{PRE}$ takes values in $[0, 1]$, so that one can interpret $[E](w)$ as a probability.

**Example 1.** A simple PRE is $(\frac{1}{3}a)^* \cdot \frac{2}{3}b$, which assigns to a word $a^mb$ the probability $(\frac{1}{3})^m \cdot \frac{2}{3}$, and 0 to words not in $a^*b$. Moreover, $E = [\frac{1}{6}a(a + b) + \frac{1}{2}a]^*(\frac{1}{3}a + b)$ is indeed a PRE for the automaton from Fig. 1. To show that $E$ is a PRE, we use some semantical equivalences such as $sa \equiv as$ or $\frac{2}{3} \equiv \frac{1}{2} + \frac{1}{6}$. The expression $a(\frac{1}{6}(a + b) + \frac{2}{3}) + b$ uses two deterministic sums (first and third) and a probabilistic sum. Using the above semantical equivalences and ACD-rules, we deduce that $\frac{1}{6}a(a + b) + \frac{1}{2}a + \frac{1}{3}a + b$ is a PRE and it remains to apply the star rule to get $E$.

In order to construct a PRE which is equivalent to a PFA, we need to be able to concatenate a PRE after an arbitrary term of another PRE. This is possible thanks to the following result.

**Proposition 1.** If $E + F$ and $G$ are PREs, then $E + F \cdot G$ is also a PRE.

For a PFA, we can always find an equivalent PRE, and vice versa. This first theorem, which is non-trivial even in the one-way setting, is generalized in the next sections allowing two-way moves and pebbles.

**Theorem 1.** PFAs and PREs are effectively equivalent.

**Proof.** We only prove the translation from automata to expressions. The other direction will be proved in a more general setting in Section 3.

Let $A = (Q, \iota, \text{Acc}, \mathbb{P})$ be a PFA. For each $q \in Q \setminus \text{Acc}$ we construct a PRE $E_q = \sum_{q' \in \text{Acc}} E_{q,q'}$ where $[E_{q,q'}](w)$ computes the sum of the probabilities of nonempty runs over $w$ starting from state $q$, ending in state $q'$. Hence, we will obtain the PRE $E_q$, which computes exactly the behavior of $A$.

We follow usual procedures to translate automata into expressions. For $q' \in Q$ and $X \subseteq Q \setminus \text{Acc}$, we define $f^X_{q'} = 0$ if $q' \in X$ and 1 otherwise. For $q \in Q \setminus \text{Acc}$ and $X \subseteq Q \setminus \text{Acc}$, we construct by induction on $X$ a PRE $E^X_q = \sum_{q' \in X} E^X_{q,q'} f^X_{q'}$ where $E^X_{q,q'}$ is a PRE such that $[E^X_{q,q'}](w)$ is the sum of the probabilities of nonempty runs over $w$ starting from state $q$, ending in state $q'$ and using only intermediary states in $X$. Hence, we have $E_q = E^Q_{q,\text{Acc}}$ and $E_{q,q'} = E^Q_{q,q'}$.

The base of the induction is when $X = \emptyset$. For each state $q \in Q \setminus \text{Acc}$ and letter $a \in A$, by definition of PFAs we have $\sum_{q' \in Q} \mathbb{P}(q, a, q') \leq 1$. Hence, using rules $(+_a)$ and $(+_s)$ we obtain the PRE

$$E^\emptyset_q = \sum_{a \in A} a \cdot \sum_{q' \in Q} \mathbb{P}(q, a, q') = \sum_{q' \in Q} E^\emptyset_{q,q'} f^\emptyset_{q'}$$

where the last equality is obtained using ACD-rules and $f^\emptyset_{q'} = 1$.

For the induction step, let $X \cup \{r\} \subseteq Q \setminus \text{Acc}$ with $r \notin X$. By induction, we assume that PREs $E^X_q$ have been constructed for all $q \in Q \setminus \text{Acc}$, and we
construct $E^X_{q'^{(r)}}$. We have $E^X_q = \sum_{q'\in Q} E^X_{q',q'q'} \in \text{PRE}$ and $f^X_q = 1$ since $r \notin X$. Using rule (s), we get $G^X_r = (E^X_r)^* \cdot (\sum_{q'\in Q\setminus\{r\}} E^X_{r,q'q'}) \in \text{PRE}$. Now, $E^X_q = \sum_{q'\in Q} E^X_{q',q'} \cdot f^X_q \in \text{PRE}$ and $f^X_q = 1$. Using Proposition 1, we can plug $G^X_r$ after $E^X_q r$ and we obtain the PRE

$E^X_{q'^{(r)}} = E^X_q \cdot G^X_r + \sum_{q'\in Q\setminus\{r\}} E^X_{q',q'} \cdot f^X_q$

$= \sum_{q'\in Q\setminus\{r\}} (E^X_{q',q'} + E^X_{q',q'} \cdot (E^X_{r,q'})^* E^X_{r,q'}) \cdot f^X_q$ (ACD-rules)

$= \sum_{q'\in Q\setminus\{r\}} E^X_{q',q'} \cdot f^X_{q'^{(r)}}$

using $f^X_{q'^{(r)}} = 0$ and $f^X_{q'^{(r)}} = f^X_{q'}$ if $q' \in Q\setminus\{r\}$. 

With Theorem 1, decidability of the equivalence problem for PFAs carries over to PREs (provided the probabilities in an expression are rational numbers), whereas their threshold problem is undecidable.

Corollary 1.

1. The equivalence problem for PREs is decidable: given PREs $E$ and $F$, does $[E] = [F]$ hold?

2. The threshold problem for PREs is undecidable: given an alphabet $A$, a PRE $E$ over $A$ and $0 < s < 1$, is there a word $w \in A^+$ such that $[E](w) \geq s$?

Note that PFAs cannot recognize all series recognized by usual Rabin automata, i.e., PFAs without the blocking assumption over accepting states. For example, the map $g: A^+ \to [0,1]$, defined by $g(a^n) = 1$ if $n > 0$ and $g(w) = 0$ for all other words $w$, is not recognizable by a PFA (note that $a^*a$ is not a PRE). However, $g$ is recognized by a Rabin automaton with a single state. To deal with this issue, we can add a fresh symbol $<$ at the end of a word. For a function $f: A^+ \to [0,1]$, we define $f_\prec: (A \cup \{<\})^+ \to [0,1]$ by $f_\prec(w<) = f(w)$ if $w \in A^+$, and 0 otherwise. For example, the series $g_\prec$ is defined by $a(a^*<)$, which is a PRE since $a + < \in \text{PRE}$. More generally, we can prove the following:

Proposition 2. Let $f: A^+ \to [0,1]$. The function $f_\prec$ is recognizable by a PFA (or equivalently by a PRE) iff $f$ is recognizable by a Rabin automaton.

3 Adding Two-Way Navigation and Pebbles

In this section, we extend probabilistic automata and expressions such that they allow us to navigate in a given word and place pebbles that can be recovered later. Before we extend PFAs and PREs accordingly, let us give a motivating example.

Example 2. Using pebbles in probabilistic expressions or automata is a natural and powerful way to deal with nesting in LTL formulas. Indeed, temporal logics implicitly use a free variable to denote the position where a formula has to be
evaluated. We will mark this position with a pebble, say \( x \), in expressions \( E_{\varphi}(x) \) or automata \( A_{\varphi}(x) \) associated with LTL formulas \( \varphi \).

Consider an LTL formula \( F_{\varphi} \), for Finally \( \varphi \). Given a word \( w \) and a position \( i \) in \( w \), we are interested in the probability \( \mathbb{P}(F_{\varphi}, w, i) \) that \( \varphi \) holds in \( w \) at position \( i \). For instance, for \( \varphi = \frac{1}{2}a \), we should obtain \( \mathbb{P}(F_{\varphi}, abba, 0) = \frac{1}{2} + \frac{2}{3}(0 + \frac{2}{3}(0 + \frac{2}{3}(\frac{1}{4} + 0))) \); either \( \varphi \) is satisfied immediately with probability \( \frac{1}{2} \), or it is not (probability \( \frac{2}{3} \)) so that (product) it has to be satisfied later. More generally, we have

\[
\mathbb{P}(F_{\varphi}, w, i) = \mathbb{P}(\varphi, w, i) + \mathbb{P}(\neg \varphi, w, i) \times \mathbb{P}(F_{\varphi}, w, i + 1)
\]

\[
= \sum_{k \geq i} \mathbb{P}(\varphi, w, k) \times \prod_{i \leq j < k} \mathbb{P}(\neg \varphi, w, j)
\]

For every LTL formula \( \varphi \), we are aiming at an equivalent expression \( E_{\varphi}(x) \) which evaluates to \( \mathbb{P}(\varphi, w, i) \) over word \( w \) when pebble \( x \) marks position \( i \). For this, we use a new construct, \( y!E_{\varphi}(y) \), which marks the current position with pebble \( y \), and computes \( \varphi \) on the whole word (from beginning to end) with this position marked (this is a non-progressing construct). Let us illustrate this inductive construction for LTL formulas. For Finally \( \varphi \), we set

\[
E_{F_{\varphi}}(x) = \triangleright ? \rightarrow^{*} x ? (y!E_{\neg \varphi}(y) \rightarrow^{*} y!E_{\varphi}(y)) \rightarrow^{*} ?.
\]

The expression starts at the beginning of the word (\( \triangleright ? \)), and moves to the right (\( \rightarrow^{*} \)) until it discovers the marked position (\( x ? \)). Then, for each \( n \geq 0 \), it iterates \( n \) times the computation of \( \neg \varphi \) with the current position marked by \( y \) \((y!E_{\neg \varphi}(y))\), moving to the right (\( \rightarrow \)) between two computations. Finally, it computes \( \varphi \) with \( y!E_{\varphi}(y) \) before moving to the last position of the word (\( \rightarrow^{*} ? \)).

Similarly, for Globally \( \varphi \) (\( G_{\varphi} \)), we have \( \mathbb{P}(G_{\varphi}, w, i) = \prod_{j \geq i} \mathbb{P}(\varphi, w, j) \), leading to the simpler expression

\[
E_{G_{\varphi}}(x) = \triangleright ? \rightarrow^{*} x ? (y!E_{\varphi}(y) \rightarrow^{*} ?.
\]

The last test (\( \leftarrow \)) is useful to enforce the preceding star operation to capture the whole suffix of the word from the position marked by \( x \).

Finally, based on the equivalence \( \varphi \cup \psi \equiv (\neg \psi \land \varphi) \cup \psi \), the expression for the Until modality is

\[
E_{\varphi \cup \psi}(x) = \triangleright ? \rightarrow^{*} x ? (y!E_{\neg \psi}(y) \rightarrow^{*} y!E_{\varphi}(y)) \rightarrow^{*} y!E_{\psi}(y) \rightarrow^{*} ?.
\]

In terms of automata, let us assume that, for every formula \( \varphi \), there is an automaton \( A_{\varphi} \) with two designated terminal states, OK and KO, such that runs ending in OK (and at the end of the word) compute expression \( E_{\varphi} \) and those ending in KO compute expression \( E_{\neg \varphi} \). These automata are 2-way, and can drop and lift pebbles on word positions. Dropping a pebble resets the control at the beginning. Lifting a pebble can be performed anywhere and resets the control to the position of the last dropped pebble (which then gets removed). The figure below depicts automata for the modalities Finally and Globally.
3.1 Probabilistic Pebble Automata

Our extended automata navigate (just like extended expressions defined below) inside a word in both directions, denoted $\rightarrow$ and $\leftarrow$. Motivated by Example 2, we moreover equip automata with $p \in \mathbb{N}$ pebbles, $1, \ldots, p$. Naturally, two-way automata can check if the current position carries some particular letter or pebble, or if it is a border (i.e., the first or last) position of the input word. Thus, they make their probabilistic choice depending on the type of the current position, which is a set containing the letter and pebbles that can be found at the current position. Formally, a $p$-type is a set $t \subseteq A \cup \{\top, \bot\} \cup \{1, \ldots, p\}$ such that (i) $\top \in t$ implies $t = \{\top\}$, and (ii) $\bot \notin t$ implies $|t \cap A| = 1$. In other words, $t$ indicates the current letter from $A$, unless the control is beyond the word ($\top \in t$). Moreover, it reveals if the current position is the first ($\top \in t$), or the last one ($\bot \in t$), or neither of them ($t \cap \{\top, \bot\} = \emptyset$). Let $T_p$ be the set of $p$-types, and let $T = \bigcup_{p \in \mathbb{N}} T_p$ denote the set of types. The current state and type of a configuration will give rise to a probability function, which triggers a move of the automaton, taken from the set $\mathcal{M} = \{\rightarrow, \leftarrow, \text{drop, lift, stay}\}$.

Let us formally define pebble probabilistic automata, which generalize PFAs.

**Definition 2.** A pebble probabilistic automaton (PPA) over $A$ is a tuple $\mathcal{A} = (p, Q, \iota, \text{Acc}, \mathbb{P})$ where $p \in \mathbb{N}$ is the number of pebbles, $Q$ is a finite set of states, $\iota \in Q$ is the initial state, and $\text{Acc} \subseteq Q \setminus \{\iota\}$ is the set of final states. Moreover, $\mathbb{P} : Q \times T_p \times \mathcal{M} \times Q \rightarrow [0, 1]$ is a transition probability function such that:

- For all $\delta = (q, t, d, q')$, if $\mathbb{P}(\delta) > 0$ then $q \notin \text{Acc}$ and $\top \in t$ implies $d \neq \leftarrow$ and $\bot \in t$ implies $d \notin \{\rightarrow, \text{drop}\}$.
- For all $q \in Q \setminus \text{Acc}$ and all types $t \in T_p$, we have $\sum_{(d, q') \in \mathcal{M} \times Q} \mathbb{P}(q, t, d, q') \leq 1$.

Next, we define the behavior of PPAs. Fix a word $w = a_0 \cdots a_{n-1}$ and a PPA $\mathcal{A}$ with $p$ pebbles. A *configuration* of $\mathcal{A}$ over $w$ is a triple $\kappa = (q, i, \pi)$ with $q \in Q$, $i \in \text{pos}(w) = \{0, \ldots, n\}$, and $\pi \in \{0, \ldots, n-1\}^{\leq p}$, where $X^{\leq p}$ is the set of words over $X$ of length at most $p$. Intuitively, $q$ is the current state, $i$ is the current position, and $\pi$ represents a stack recording the $k = |\pi| \leq p$ positions of the currently dropped pebbles: $\pi = i_1 \cdots i_k$ means that pebble $\ell \in \{1, \ldots, k\}$ is currently at position $i_\ell$ and pebbles $k+1, \ldots, p$ are currently not dropped. Pebbles are dropped and lifted using a stack policy: if $\pi = i_1 \cdots i_k$, only pebble $k+1$ can be dropped (provided $k+1 \leq p$), and only pebble $k$ can be lifted (provided $k \geq 1$).
Let $\kappa = (q, i, \pi)$ be a configuration with $\pi = i_1 \cdots i_k$. We call $\kappa$ \textit{initial} if $q = \iota$, $i = 0$, and $\pi = \varepsilon$. It is said to be \textit{final} if $q \in \text{Acc}$, $i = n$, and $\pi = \varepsilon$. Moreover, the type of $\kappa$ is denoted by $\text{type}(\kappa)$ and defined as $\{a_i \mid i < n\} \cup \{> \mid i = 0\} \cup \{< \mid i = n\} \cup \{\ell \in \{1, \ldots, k\} \mid i_{\ell} = i\}$.

Given $\delta = (q, t, d, q') \in Q \times T_p \times A \times Q$ as well as configurations $\kappa = (q, i, \pi)$ and $\kappa' = (q', i', \pi')$, we write $\kappa \xrightarrow{\delta} \kappa'$ if $t = \text{type}(\kappa)$ and the following hold:

1. if $d = \to$ then $i' = i + 1$ and $\pi' = \pi$
2. if $d = \leftarrow$ then $i' = i - 1$ and $\pi' = \pi$
3. if $d = \text{stay}$ then $i' = i$ and $\pi' = \pi$
4. if $d = \text{drop}$ then $i' = 0$ and $\pi' = \pi i$ and $i < n$
5. if $d = \text{lift}$ then $\pi' i' = \pi$.

In other words, drop saves the current position on the stack of pebbles ($\pi' = \pi i$ in 4) and resets the head to the first position ($i' = 0$ in 4). Moreover, $\pi' i' = \pi$ in 5 means that lift pops the last dropped pebble and resets the control to the position where this pebble was dropped.

A \textit{run} of $A$ over $w$ is a finite sequence $\rho = (\kappa_0, \delta_1, \kappa_1, \ldots, \delta_h, \kappa_h)$ ($h \geq 0$) of configurations and transitions such that, for all $0 < m \leq h$, we have $\mathbb{P}(\delta_m) > 0$ and $\kappa_{m-1} \xrightarrow{\delta_m} \kappa_m$. We say that $\rho$ is \textit{accepting} if $\kappa_0$ is an initial configuration and $\kappa_h$ is final. The probability of this run is the product of the probabilities of the transitions all along the run: $\mathbb{P}(\rho) = \prod_{m=1}^{h} \mathbb{P}(\delta_m)$. Now, let $[A](w)$ be the sum $\sum_{\rho} \mathbb{P}(\rho)$, where $\rho$ ranges over the accepting runs of $A$ over $w$. Note that the number of accepting runs over a given word may be infinite so that, a priori, $[A]$ is a mapping $A^+ \to \mathbb{R}_{\geq 0}$. However, one can show the following:

\textbf{Proposition 3. For every PPA $A$ and every $w \in A^+$, we have $[A](w) \in [0, 1]$.}

\textit{Proof.} Let us define, for every $w \in A^+$, a probability space $(\Omega^w, \mathcal{E}^w, \mathbb{P}^w)$. The set $\Omega^w$ of outcomes is the set of maximal runs of $A$ over $w$, starting in the initial configuration (for technical reasons, we have to include infinite ones). Moreover, the set $\mathcal{E}^w$ of events is the smallest $\sigma$-algebra containing, for all finite runs $\rho$, the cylinder set $\text{Cyl}(\rho) \overset{\text{def}}{=} \{\rho' \mid \rho'$ is a maximal run with prefix $\rho\}$. With this, there is a unique probability measure $\mathbb{P}^w$ for $\Omega^w$ and $\mathcal{E}^w$, which is given by $\mathbb{P}^w(\text{Cyl}(\rho)) = 1 \cdot \mathbb{P}(\delta_1) \cdots \cdot \mathbb{P}(\delta_h)$ for all finite runs $\rho = (\kappa_0, \delta_1, \kappa_1, \ldots, \delta_h, \kappa_h)$. As the set $\text{AR}(w)$ of accepting runs over $w$ is countable, it is measurable in the probability space, and its probability is $\mathbb{P}^w(\text{AR}(w)) = \sum_{\rho \in \text{AR}(w)} \mathbb{P}^w(\text{Cyl}(\rho))$. Note that the latter equals $[A](w)$ and that $\text{Cyl}(\rho) = \{\rho\}$ for all $\rho \in \text{AR}(w)$. $\square$

The proof above establishes a strong connection between PPAs and Markov chains. This connection also provides an algorithm for evaluating a PPA wrt. a given word, which reduces to computing the probability of reaching a final configuration in the \textit{synchronized} Markov chain (see, for example, [3]).

\textbf{Example 3.} Consider the PPA $A$ (2-way, without pebbles) depicted on the left of Fig. 2 (where $0 < s < 1$) over alphabet $A = \{a\}$. The synchronized Markov chain of $A$ wrt. a word of length $n$ is depicted on the right of the same figure. This Markov chain represents a random walk over a straight line of bounded length.
3.2 Probabilistic Pebble Expressions

Now, we define probabilistic expressions that capture the expressive power of PPAs. Just like PPAs, expressions are equipped with some pebbles from an infinite supply $\mathcal{P} = \{1, 2, \ldots\}$ (though every expression will only employ a finite number thereof). Also, expressions should be able to move left or right and to check if pebbles are dropped on the current position. Hence, we adopt an XPath-like syntax: we explicitly distinguish progression in the word (with $\leftarrow$ or $\rightarrow$) from tests $\varphi \in \text{Tests}$ checking the current type. We define test formulas inductively by

$$\varphi ::= a? \mid x? \mid \triangleright? \mid \triangleleft? \mid \lnot \varphi \mid \varphi \lor \varphi \mid \varphi \land \varphi$$

where $a \in A$ and $x \in \mathcal{P}$. In particular, formulas $\triangleright?$ and $\triangleleft?$ allow an expression to test whether it is at the first or last position of the word. Moreover, $x?$ is true if pebble $x$ is on the current position. Formulas $\varphi \in \text{Tests}$ are interpreted over a type $t \in T$ in a straightforward manner: for $\theta \in A \cup \{\triangleright, \triangleleft\} \cup \mathcal{P}$, we write $t \models \theta$ if $\theta \in t$. The semantics of boolean connectives is defined as expected.

We start with unrestricted weighted pebble expressions (WPEs) defined by

$$E ::= s \mid \varphi \mid \leftarrow \mid \rightarrow \mid E + E \mid E \cdot E \mid E^* \mid x!E$$

with $s \in \mathbb{R}_{\geq 0}^\infty$, $\varphi \in \text{Tests}$ and $x \in \mathcal{P}$. The interpretation of $s$, sum, concatenation, and star does not change wrt. WPEs. The new atomic expressions $\leftarrow$ and $\rightarrow$ perform a step to the left or to the right. The expressions $\varphi$ and $x!E$, on the other hand, perform non-progressing computations (similar to $s$). The atomic WEA is obtained by checking first if the current letter is $a$ and then moving right, hence the abbreviation $a \equiv a?\rightarrow$. The new construct $x!E$ is read “compute $E$ with $x$ assigned to the current position”. The computation of $E$ “rescans” the whole word, from position 0 to position $|w|$.

The set of free pebbles of an expression $E \in \text{WPE}$ is defined in the obvious way; in particular, we set $\text{Free}(x?) = \{x\}$ and $\text{Free}(x!E) = \text{Free}(E) \setminus \{x\}$.

The semantics $[E]$ of an expression $E$ assigns a value from $\mathbb{R}_{\geq 0}^\infty$ to each tuple $(w, \sigma, i, j)$ where $w = a_0a_1 \cdots \in A^+$, $i, j \in \text{pos}(w)$ and $\sigma : \text{Free}(E) \rightarrow \{0, \ldots, |w| - 1\}$. It computes the weight of going from $i$ to $j$ with the pebble assignment $\sigma$. Formally, the semantics is given in Table 1. Hereby, we let $\text{type}(i) \in T$ denote the set $\{a_i \mid i \neq |w|\} \cup \{\triangleright \mid i = 0\} \cup \{\triangleleft \mid i = |w|\} \cup \sigma^{-1}(i)$. Moreover, $\sigma[x \mapsto i]$ stands for the assignment coinciding with $\sigma$ except on $x$, which is
operations to get the associative, i.e., distributivity rules (ACD built inductively as follows: the rule for concatenation. Proof of Proposition associativity and distributivity hence we enforce these properties explicitly. The commutative, concatenation distributes over + by induction:

\[ E_1 + E_2 = [E_1] + [E_2] \]

\[ [E_1 \cdot E_2](w, \sigma, i, j) = \sum_{k \in pos(w)} [E_1](w, \sigma, i, k) \times [E_2](w, \sigma, k, j) \]

\[ [x!E](w, \sigma, i, j) = \begin{cases} [E](w, \sigma[x \mapsto i], 0, |w|) & \text{if } j = i < |w| \\ 0 & \text{otherwise} \end{cases} \]

Table 1. Semantics of WPEs

mapped to i. If \( \text{Free}(E) = \emptyset \), then we let \( [E](w) = [E](w, 0, |w|) \) (omitting \( \sigma \), as it is irrelevant).

One can easily check that concatenation, also called Cauchy product, is associative, i.e., \( ([E_1 \cdot E_2] \cdot E_3) = [E_1 \cdot (E_2 \cdot E_3)] \). Hence, one can define \( E^m \) by induction: \( E^0 = 1 \) and \( E^{m+1} = E \cdot E^m \). Moreover, + is associative and commutative, concatenation distributes over +, and \( x! \) distributes over +.

As for expressions without pebbles, we need to restrict the sum and star operations to get the probabilistic fragment. Doing so, we lose commutativity, associativity and distributivity hence we enforce these properties explicitly. The proof of Proposition 1 cannot be extended to cope with \( x!E \), hence we strengthen the rule for concatenation.

**Definition 3.** Probabilistic pebble expressions (PPEs) is the fragment of WPEs built inductively as follows:

(Atoms) \( s \in [0,1], \varphi \in \text{Tests}, \leftarrow \text{and } \rightarrow \text{ are PPEs.} \)

\[ (+\varphi) \] If \( E \) and \( F \) are PPEs and \( \varphi \in \text{Tests} \), then \( \varphi \cdot E + (\neg \varphi) \cdot F \) is a PPE.

\[ (+s) \] If \( E \) and \( F \) are PPEs and \( s \in [0,1] \), then \( s \cdot E + (1 - s) \cdot F \) is a PPE.

\[ (\cdot) \] If \( E + F \) is a PPE and \( G \) is a PPE, then \( E + F \cdot G \) is a PPE.

\[ (* ) \] If \( E + F \) is a PPE, then \( E^* \cdot F \) is a PPE.

\[ (x!) \] If \( E \) is a PPE, then \( x!E \) is a PPE.

(ACD) PPEs are closed under the following associativity, commutativity and distributivity rules (ACD-rules):

\[
\begin{align*}
A_+ & \quad E + (F + G) \in \text{PPE} \iff (E + F) + G \in \text{PPE} \\
C_+ & \quad E + F \in \text{PPE} \iff F + E \in \text{PPE} \\
A & \quad E \cdot (F + G) \in \text{PPE} \iff (E \cdot F) \cdot G \in \text{PPE} \\
D & \quad E \cdot (F + G) \in \text{PPE} \iff E \cdot F + E \cdot G \in \text{PPE} \\
D_{x!} & \quad x!(E + F) \in \text{PPE} \iff x!E + x!F \in \text{PPE}
\end{align*}
\]
The semantics of PPEs is inherited from WPEs and we will show later that when \( E \in \text{PPE} \) then \( \llbracket E \rrbracket (w, \sigma, i, j) \) actually always belongs to \([0, 1]\).

**Example 4.** We continue Example 3. An equivalent PPE to denote the random walk is given by

\[
E = (\neg \text{?}(s \rightarrow + (1 - s)\neg \text{?}?)^* \text{?}.
\]

Moreover, let \( F = \neg \text{?}(s \rightarrow + (1 - s)\neg \text{?}?) \) so that \( E = F^* \). Notice that \( E \) is indeed an expression in PPE because \( F + ? \in \text{PPE} \). Let \( w \) be a word of length \( m \geq 2 \). We can easily see that, for all \( i, j \in \text{pos}(w) \) and all \( n \geq |j - i| \), the expression \( F^n \) computes a positive value on \((w, i, j)\). Therefore, the expression \( F^s \) computes an infinite sum on \((w, i, j)\). In the present case (0 < \( s < 1 \)), the series \( \sum_{n \geq 0} [F^n](w, i, j) \) converges: with \( \alpha = \frac{1 - s}{s} \), one can show that \( \llbracket E \rrbracket (w, 0, |w|) = 1/(1 + \alpha + \ldots + \alpha^{|w|}) \), and \( \llbracket F^s \rrbracket (w, i, j) \in [0, 1] \).

We define now the multiset \( \text{Terms}(E) \) of terms of an expression \( E \in \text{WPE} \). This will be crucial for the translation from expressions to automata in the next section. Intuitively, if we suppose that summation is pushed up as much as possible by means of ACD-rules, then the multiset of terms consists of all expressions that occur in this big outermost sum. Formally, the definition is by induction over \( E \in \text{WPE} \). When \( E \) is an atom, we let \( \text{Terms}(E) = \llbracket E \rrbracket \) be the singleton multiset containing only the atom itself. Moreover,

\[
\begin{align*}
\text{Terms}(E + F) &= \text{Terms}(E) \cup \text{Terms}(F) \\
\text{Terms}(E \cdot F) &= \llbracket E' \cdot F' \mid E' \in \text{Terms}(E), F' \in \text{Terms}(F) \rrbracket \\
\text{Terms}(E^*) &= \llbracket E^* \rrbracket \\
\text{Terms}(x!E) &= \llbracket x!E' \mid E' \in \text{Terms}(E) \rrbracket .
\end{align*}
\]

Note that, if an expression \( F \) can be obtained from an expression \( E \) through ACD-rules, then we have \( \text{Terms}(E) = \text{Terms}(F) \). The converse also holds as can be seen from the following proposition which can be easily proved by structural induction on the expression.

**Proposition 4.** Let \( E \in \text{WPE} \) with \( \text{Terms}(E) = \llbracket E_i \mid i \in I \rrbracket \). Using ACD-rules, we can rewrite \( E \) into \( \sum_{i \in I} E_i \). In particular, we have \( \llbracket E \rrbracket = \sum_{i \in I} \llbracket E_i \rrbracket \). Hence, we identify \( E \) and \( \sum_{i \in I} E_i \).

## 4 The Probabilistic Kleene Theorem

We prove in this section that PPAs are effectively equivalent to PPEs. We start with the construction of PPAs from PPEs. The problematic cases are concatenation and iteration due to the precondition \( E + F \in \text{PPE} \). To deal with these cases, we construct from PPE \( E \) a PPA \( \mathcal{A} \) which simultaneously recognizes all terms of \( E \).

**Theorem 2.** From any expression \( E \in \text{PPE} \) we can effectively construct an equivalent PPA \( \mathcal{A} = (p, Q, \iota, \text{Acc}, \text{P}) \). More precisely, if \( \text{Terms}(E) = \llbracket E_i \mid i \in I \rrbracket \), the set of accepting states of \( \mathcal{A} \) is \( \text{Acc} = \{ f_i \mid i \in I \} \) and for all \( i \in I \) the expression \( E_i \) is equivalent to the PPA \( \mathcal{A}[f_i] = (p, Q, \iota, \{ f_i \}, \text{P}) \).
Proof. The construction is by structural induction on the expression $E \in \text{PPE}$ which may have free pebbles. As usual, the assignment of free pebbles will be encoded in the alphabet of the word read by the automaton $A \in \text{PPA}$, hence $(w, \sigma)$ will be interpreted as a word over $A \times 2^{\text{Free}(E)}$ in the automata. Then, equivalence $A \approx E$ means that, for all words $w \in A^+$, assignments $\sigma : \text{Free}(E) \to \text{pos}(w) \setminus \{|w|\}$, and positions $i, j \in \text{pos}(w)$, the value $\llbracket E \rrbracket(w, \sigma, i, j)$ is the sum of the probabilities of the runs of $A$ over $(w, \sigma)$ starting in the initial state in position $i$, ending in an accepting state in position $j$.

The cases $s \in \{0, 1\}$, $\varphi \in \text{Tests}$, $\rightarrow$, and $\leftarrow$ are clear. For each atom, the resulting automaton has only two states (it uses stay transitions for $s$ and $\varphi$).

Now let $E, E' \in \text{PPE}$ be such that $\text{Terms}(E) = \{E_i \mid i \in I\}$ and $\text{Terms}(E') = \{E_j' \mid j \in J\}$. By induction hypothesis, we have constructed two suitable PPAs $A = (p, Q, i, \text{Acc}, \mathbb{P})$ and $A' = (p', Q', i', \text{Acc}', \mathbb{P}')$ with $\text{Acc} = \{f_i \mid i \in I\}$ and $\text{Acc}' = \{f_j' \mid j \in J\}$. Without loss of generality, we assume that $p = p'$, $Q \cap Q' = \emptyset$, and that a final state may only be reached when no pebble is dropped (if necessary, this may be enforced by keeping the number of dropped pebbles in the states).

Consider $E'' = \varphi \cdot E + \neg \varphi \cdot E'$. We have $\text{Terms}(E'') = \{\varphi \cdot E_i \mid i \in I\} \cup \{- \varphi \cdot E_j' \mid j \in J\}$. We construct a PPA $A'' = (p, Q \uplus Q' \cup \{i''\}, i'', \text{Acc} \uplus \text{Acc}', \mathbb{P}'')$. From the new initial state $i''$, we add stay transitions with probability 1 going to $i$ for all types $t$ satisfying $\varphi$, and going to $i'$ for all other types.

The construction for $E'' = s \cdot E + (1 - s) \cdot E'$ is similar. We have $\text{Terms}(E'') = \{s \cdot E_i \mid i \in I\} \cup \{(1 - s) \cdot E_j' \mid j \in J\}$. We add stay transitions with probability $s$ from $i''$ to $i$ and stay transitions with probability $1 - s$ from $i$ to $i'$.

For the concatenation, we assume that $E = F \cdot G$ and $E'' = F + G \cdot E'$. We have $I = K \uplus L$ with $\text{Terms}(E) = \{E_i \mid i \in K\}$ and $\text{Terms}(G) = \{E_i \mid i \in L\}$. Hence, we have $\text{Terms}(E'') = \{E_i \mid i \in K\} \cup \{E_i \cdot E_j' \mid (i, j) \in L \times J\}$. The automaton $A''$ for $E''$ consists of one copy of $A$ and each copy $A_i'$ of $A'$ for every $i \in L$. First, $A''$ simulates $A$ until it reaches some final state $f_i$ of $A$. Then, if $i \in L$, a stay transition leads with probability 1 into the initial state of $A_i'$. The final states of $A''$ consist of $\{f_i \mid i \in K\}$ and a copy of $\text{Acc}'$ for each $i \in L$.

For the Kleene star we assume that $E = F \cdot G$ and $E'' = F^* \cdot G$. We have $I = K \uplus L$ with $\text{Terms}(F) = \{E_i \mid i \in K\}$ and $\text{Terms}(G) = \{E_i \mid i \in L\}$. Hence, we have $\text{Terms}(E'') = \{F^* \cdot E_i \mid i \in L\}$. We construct the PPA $A'' = (p, Q, i, \text{Acc}''', \mathbb{P}'')$ with $\text{Acc}''' = \{f_i \mid i \in L\}$ by adding stay transitions with probability 1 from all states $f_i$ for $i \in K$ back to the initial state $i$.

Consider $E'' = x!E$. We have $\text{Terms}(E'') = \{x!E_i \mid i \in I\}$. We construct the PPA $A'' = (p + 1, Q \uplus \{i''\} \cup \text{Acc}'', i'', \text{Acc}''', \mathbb{P}'')$ with $\text{Acc}'''$ a copy of $\text{Acc}$. To this aim, we shift the numbers of pebbles of $A$ to $\{2, \ldots, p + 1\}$ keeping pebble 1 to be the fresh one, used to mark the position of variable $x$. We start by dropping pebble 1 with transitions of the form $(i''', t, \text{drop}, i)$, each with probability 1. At the end of a computation of $A$, pebble 1 is lifted, again with probability 1, using transitions $(q, <\emptyset>, \text{lift}, q'')$ where $q'' \in \text{Acc}''$ is the copy of $q \in \text{Acc}$.

Finally, if $E''$ is obtained from $E$ via ACD-rules, we have $\text{Terms}(E'') = \text{Terms}(E)$ so we can keep the same automaton: $A'' = A$. 
\qed
Note that, even if we start from a PRE, the proof above does not yield a PFA since it adds stay transitions. Hence, this proof has to be adapted to translate PREs into PFAs. By Proposition 3, the semantics of automata only assumes values in $[0,1]$. This carries over to PPE.

**Corollary 2.** For every PPE $E$ and every $w \in A^+$, we have $[E](w) \in [0,1]$.

We turn now to the construction of expressions (PPEs) which are equivalent to automata (PPAs). We follow usual procedures for the translation from automata to expressions, ensuring throughout the proof that we produce expressions in PPE. To this aim, we strongly rely on ACD-rules.

**Theorem 3.** Let $A = (p,Q,\iota,\text{Acc}, \mathbb{P})$ be a PPA with $p$ pebbles. We can effectively construct a PPE $E_\iota = \sum_{q \in \text{Acc}} E_{\iota,q}$ such that $[E_{\iota,q}](w,0,|w|)$ is the sum of the runs from the initial configuration $(\iota,0,\varepsilon)$ to the final configuration $(q,|w|,\varepsilon)$.

5 Conclusion

In this paper, we presented a probabilistic Kleene Theorem, first for classical probabilistic automata and then for extended automata with two-way navigation and pebbles. This constitutes a first step towards probabilistic XPath, so we aim at extending our work to finite trees and probabilistic tree automata. We also raise the question of whether our technique can be used to obtain $\omega$-expressions for probabilistic Büchi automata, which have attracted a lot of attention [2,1,8]. Just like classical finite automata, weighted automata over semirings enjoy characterizations in terms of monadic second-order logic [13,6]. Continuing this line of research, a recent paper establishes a logical characterization of probabilistic automata [30]. It would be interesting to study whether alternative characterizations exist that use, for example, a transitive-closure operator [6].

References

Appendix

Proposition 1. Let $E \in \text{PRE}$ with $\text{Terms}(E) = \{E_i \mid i \in I\}$. Let $F_i \in \text{PRE}$ for each $i \in I$. We have

$$\bar{E} = \sum_{i \in I} E_i \cdot F_i \in \text{PRE}.$$

In particular, any sum of (some) terms of a PRE is also a PRE: if $I' \subseteq I$ we get $\sum_{i \in I'} E_i \in \text{PRE}$ by letting $F_i = 1$ for $i \in I'$ and $F_i = 0$ otherwise.

Proof (of Proposition 1). We proceed by structural induction over $E$. This is trivial for atoms and also for ACD-rules since they preserve the multiset of terms. Let $G, H \in \text{PRE}$ with $\text{Terms}(G) = \{G_j \mid j \in J\}$ and $\text{Terms}(H) = \{H_k \mid k \in K\}$.

Consider $E = sG + (1 - s)H$. Then, $\text{Terms}(E) = \{sG_j \mid j \in J\} \uplus \{(1 - s)H_k \mid k \in K\}$. Hence we have $I = J \uplus K$, $E_i = sG_i$ for $i \in J$ and $E_i = (1 - s)H_i$ for $i \in K$. By induction, we have $\bar{G} = \sum_{i \in J} G_i \cdot F_i \in \text{PRE}$ and $\bar{H} = \sum_{i \in K} H_i \cdot F_i \in \text{PRE}$. Therefore, $\bar{E} = (s\bar{G} + (1 - s)\bar{H}) \in \text{PRE}$. This expression can be rewritten into $\bar{E}$ with ACD-rules.

The proof is similar for $E = \sum_{a \in A} aE_a$.

Consider $E = G \cdot H$ so that $I = J \times K$ and $E_{(j,k)} = G_j \cdot H_k$ for $(j,k) \in I$. By induction, for every $j \in J$, we get $\bar{H}_j = \sum_{k \in K} H_k \cdot F_{(j,k)} \in \text{PRE}$. Again by induction we obtain $\sum_{j \in J} G_j \cdot \bar{H}_j \in \text{PRE}$. This expression can be rewritten into $\bar{E}$ with ACD-rules.

Consider now $E = G^* \cdot H$ assuming $G + H \in \text{PRE}$ instead of $G, H \in \text{PRE}$. We have $I = K$ and $E_i = G^* \cdot H_i$ for $i \in I$. Applying the induction hypothesis to the expression $G + H$ with $F_j = 1$ for $j \in J$, we obtain $\sum_{j \in J} G_j + (\sum_{k \in K} H_k \cdot F_k) \in \text{PRE}$. From the star rule we deduce that $(\sum_{j \in J} G_j)^* \cdot (\sum_{k \in K} H_k \cdot F_k) \in \text{PRE}$. Using ACD-rules, this can be rewritten into $\bar{E} = \sum_{i \in I} G^* \cdot H_i \cdot F_i$. 

From Automata to Expressions.

Let $A = (p, Q, t, \text{Acc}, \mathbb{P})$ be a PPA with $p$ pebbles. Without loss of generality, we assume that the number of dropped pebbles is encoded in the states of $A$. Hence, $Q = \biguplus_{k=0}^{p} Q^{(k)}$ where a state in $Q^{(k)}$ means that $p - k$ pebbles have been dropped and $k$ pebbles may still be dropped. The top level $Q^{(p)}$ of the automaton contains the initial state $\iota \in Q^{(p)}$ and the final states $\text{Acc} \subset Q^{(p)}$. Moreover, a transition of level $k$ may only test pebbles up to $p - k$: for $q \in Q^{(k)}$, if $\mathbb{P}(q, t, d, q') > 0$ then $t \in T_{p-k}$.

We also assume that lift transitions are enabled only at the last position of the input word, i.e., only when the type is $t = \langle \cdot \rangle$. For each state $q \in Q^{(k)}$ ($k < p$) we let $f_q = \sum_{q' \in Q^{(k+1)}} \mathbb{P}(q, \langle \cdot \rangle, \text{lift}, q')$ be the sum of the probabilities of lift transitions starting from $q$. When $q \in Q^{(p)}$, we let $f_q = 1$ if $q \in \text{Acc}$ and $f_q = 0$ otherwise.

For each $q \in Q^{(k)}$ ($k \leq p$) we construct a PPE $E_q = \sum_{q' \in Q^{(k)}} E_{q', q'\langle ? \rangle} f_q$, where $E_{q', q'\langle ? \rangle}$ is a PPE which computes the sum of the probabilities of runs starting from state $q$, ending in state $q'$ and visiting only states in $Q^{(\leq k)} = \biguplus_{\ell \leq k} Q^{(\ell)}$. 

16
This construction is by induction on \( k \in \{0, \ldots, p \} \). Within each level \( k \leq p \), we follow usual procedures to translate automata into expressions.

When \( k < p \) some pebbles were already dropped hence the PPE \( E_q \) will have free pebbles \( \text{Free}(E_q) \subseteq \{1, \ldots, p - k\} \) and we encode with an assignment \( \sigma : \text{Free}(E_q) \to \text{pos}(w) \setminus \{|w|\} \) the positions of the dropped pebbles. We denote by \( \pi_\sigma \in \text{pos}(w)^{p-k} \) the corresponding stack recording the positions of pebbles.

For \( q \in Q^{(k)} \) and \( X \subseteq Q^{(k)} \) we let \( f_q^X = \begin{cases} \angle f_q & \text{if } q \in X \\ 1 & \text{otherwise.} \end{cases} \)

For \( q \in Q^{(k)} \) and \( X \subseteq Q^{(k)} \), we construct by induction on \( X \) a PPE

\[
E_q^X = \angle f_q + \sum_{q' \in Q^{(k)}} E_{q,q'}^{X} f_{q'}^X
\]

where \( E_{q,q'}^{X} \) is a PPE such that \( [E_{q,q'}^{X}](w, \sigma, i, j) \) is the sum of the probabilities of nonempty runs starting from configuration \( (q, i, \pi_\sigma) \), ending in configuration \( (q', j, \pi_\sigma) \) and using only intermediary states in \( X \cup Q^{(\leq k-1)} \).

The base of the induction is when \( k = 0 \) and \( X = \emptyset \). For each state \( q \in Q^{(0)} \) and type \( t \in T_p \), by definition of PPAs we have \( \sum_{(d,q') \in M \times Q} \mathbb{P}(q, t, d, q') \leq 1 \). Now, since \( q \in Q^{(0)} \), drop moves are disallowed. Moreover, we have assumed that lift moves are only enabled for type \( t = \{\angle\} \). Hence, when \( t \neq \{\angle\} \), using rule \((+_s)\) we deduce that

\[
F_{q,t} = \sum_{q' \in Q^{(0)}} \mathbb{P}(q, t, \text{stay}, q') + \mathbb{P}(q, t, \leftarrow, q') \cdot \leftarrow + \mathbb{P}(q, t, \rightarrow, q') \cdot \rightarrow
\]

is a PPE. For \( t = \{\angle\} \), using rule \((+_s)\) and the definition of \( f_q \) we deduce that

\[
F_{q,\angle} = f_q + \sum_{q' \in Q^{(0)}} \mathbb{P}(q, \{\angle\}, \text{stay}, q') + \mathbb{P}(q, \{\angle\}, \leftarrow, q') \cdot \leftarrow
\]

is a PPE. Now, using the deterministic sum \((+_\varphi)\) we obtain the PPE

\[
E_q^0 = \sum_{t \in T_p} t? \cdot F_{q,t} = \angle f_q + \sum_{q' \in Q^{(0)}} E_{q,q'}^0 f_{q'}^0
\]

where the last equality is obtained using ACD-rules and \( f_{q'}^0 = 1 \).

We turn now to the induction step on \( X \). This step is the same for all layers \( k \leq p \). So fix \( k \leq p \), \( X \subseteq Q^{(k)} \) and \( r \in Q^{(k)} \setminus X \). By induction, we assume that PPEs \( E_r^X \) have been constructed for all \( q \in Q^{(k)} \). We construct \( E_q^{X \cup \{r\}} \).

We have \( E_r^X = \angle f_r + \sum_{q' \in Q^{(k)}} E_{r,q'}^{X} f_{q'}^X \in \text{PPE} \) and \( f_r^X = 1 \) since \( r \notin X \).

With rule \((*)\) we get

\[
G_r^X = \left( E_{r,r}^X \right)^* \cdot \left( \angle f_r + \sum_{q' \in Q^{(k)} \setminus \{r\}} E_{r,q'}^{X} f_{q'}^X \right) \in \text{PPE}.
\]
Now, \( E^X_q = \preceq f_q + \sum_{q' \in Q^{(k)}} E^X_{q,q'} f^X_{q'} \in \text{PPE} \) and \( f^X_r = 1 \). Using rule (\( \cdot \)) we can plug \( G^X_r \) after \( E^X_{q,r} \) and we obtain the PPE

\[
E^X_{q,r} = \preceq f_q + E^X_{q,r} \cdot G^X_r + \sum_{q' \in Q^{(k)} \setminus \{r\}} E^X_{q,q'} f^X_{q'}
\]

\[
= \preceq f_q + E^X_{q,r} (E^X_r)^* \preceq f_r + \sum_{q' \in Q^{(k)} \setminus \{r\}} (E^X_{q,q'} + E^X_{q,r} (E^X_r)^*) f^X_{q'}
\]

\[
= \preceq f_q + \sum_{q' \in Q^{(k)}} E^X_{q,q'} f^X_{q'}
\]

where the last equality uses \( f^X_{r} = \preceq f_r \) and \( f^X_{q'} = f^X_q \) if \( q' \in Q^{(k)} \setminus \{r\} \).

It remains to deal with \( X = \emptyset \) and \( 0 < k \leq p \). Compared to the case \( X = \emptyset \) and \( k = 0 \) we also have to consider drop transitions which lead to the lower layer. The next pebble to be dropped is \( x = p - k + 1 \). By induction, we have already constructed expressions \( E^X_r \) for all states \( r \in Q^{(k-1)} \) of the lower layer. To lighten the notation, for \( r, r' \in Q^{(k-1)} \), we let \( E_r = E^X_r \) and \( E_{r,r'} = E^X_{r,r'} \). Using distributivity \( \mathbf{D}_{x!} \) we get the PPE

\[
x! E_r = x! (\preceq f_r) + \sum_{r' \in Q^{(k-1)}} x! (E_{r,r'} \preceq f_{r'}) \cdot \sum_{q' \in Q^{(k)}} \sum_{r' \in Q^{(k-1)}} x! (E_{r,r'} \preceq f_{r'}) \frac{P(r', \{\preceq\}, \text{lift}, q')}{f_{r'}}.
\]

The first term is equivalent to 0 since we consider only nonempty words. Using the concatenation rule (\( \cdot \)) we plug after each term \( x! (E_{r,r'} \preceq f_{r'}) \) the PPE \( 1 = \sum_{q' \in Q^{(k)}} P(r', \{\preceq\}, \text{lift}, q') \) and we obtain using ACD-rules the PPE

\[
G_r = \sum_{q' \in Q^{(k)}} \sum_{r' \in Q^{(k-1)}} x! (E_{r,r'} \preceq f_{r'}) \frac{P(r', \{\preceq\}, \text{lift}, q')}{f_{r'}}.
\]

Note that \( \text{Free}(G_r) \subseteq \{1, \ldots, p - k\} \). Now, we proceed as before. For each state \( q \in Q^{(k)} \) and type \( t \in T_{p-k} \) we have \( \sum_{d, q' \in Q} P(q, t, d, q') \leq 1 \). Hence, when \( t \neq \{\preceq\} \), using rule (+x) we deduce that

\[
F_{q,t} = \sum_{q' \in Q^{(k)}} P(q, t, \text{stay}, q') + P(q, t, \leftarrow, q') + P(q, t, \rightarrow, q') + \sum_{r \in Q^{(k-1)}} P(q, t, \text{drop}, r) G_r
\]

\[
= \sum_{q' \in Q^{(k)}} \left( P(q, t, \text{stay}, q') + P(q, t, \leftarrow, q') + P(q, t, \rightarrow, q') + \sum_{r, r' \in Q^{(k-1)}} P(q, t, \text{drop}, r) x! (E_{r,r'} \preceq f_{r'}) \frac{P(r', \{\preceq\}, \text{lift}, q')}{{f}_{r'}} \right)
\]

is a PPE. For \( t = \{\preceq\} \) the drop transition is not possible, hence we get as before the PPE

\[
F_{q,\{\preceq\}} = f_q + \sum_{q' \in Q^{(k)}} P(q, \{\preceq\}, \text{stay}, q') + P(q, \{\preceq\}, \leftarrow, q') \leftarrow.
\]
Now, using the deterministic sum \((+\varphi)\) we obtain the PPE

\[
E_q^\emptyset = \sum_{t \in T_{p-k}} t? \cdot F_{q,t} = \triangleleft ? f_q + \sum_{q' \in Q(k)} E_{q',q} f_{q'}^\emptyset
\]

where the last equality is obtained using ACD-rules and \(f_{q'}^\emptyset = 1\). Note that \(\text{Free}(E_q^\emptyset) \subseteq \{1, \ldots, p-k\}\).

For \(0 < k \leq p\), the induction on \(X\) goes exactly as explained above. Again, for \(q, q' \in Q(k)\), we let \(E_q = E_q^{Q(k)}\) and \(E_{q,q'} = E_{q,q'}^{Q(k)}\). Therefore, for all \(k \leq p\) and \(q \in Q(k)\) we have constructed a PPE \(E_q = \sum_{q' \in Q(k)} E_{q,q'} \triangleleft ? f_{q'}\) as announced at the beginning of the proof.

Finally, the PPE \(E_i\) is equivalent to the automaton \(A\): for each word \(w\), the value \([E_i](w, 0, |w|)\) is the sum of the probabilities of all accepting runs starting from the initial configuration \((\varepsilon, 0, \varepsilon)\) and ending in a final configuration \((q', |w|, \varepsilon)\) with \(q' \in \text{Acc}\).