BRICS

Basic Research in Computer Science

A Fully Equational Proof of Parikh's Theorem

Luca Aceto
Zoltán Ésik
Anna Ingólfsdóttir

See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:

> BRICS
> Department of Computer Science
> University of Aarhus
> Ny Munkegade, building 540
> DK–8000 Aarhus C
> Denmark
> Telephone: +45 8942 3360
> Telefax: +45 8942 3255
> Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide
Web and anonymous FTP through these URLs:

> `http://www.brics.dk`
> `ftp://ftp.brics.dk`
> **This document in subdirectory** `RS/01/28/`

A Fully Equational Proof of Parikh's Theorem

Luca Aceto   Zoltán Ésik[*]   Anna Ingólfsdóttir
BRICS[†]
Department of Computer Science
University of Aalborg
Fredrik Bajers Vej 7E
DK-9220 Aalborg

Abstract

We show that the validity of Parikh's theorem for context-free languages depends only on a few equational properties of least pre-fixed points. Moreover, we exhibit an infinite basis of μ-term equations of continuous commutative idempotent semirings.

AMS SUBJECT CLASSIFICATION (2000): 03C05, 16Y60, 68Q42, 68Q45, 68Q70.
KEYWORDS AND PHRASES: Parikh's theorem, commutative context-free languages, commutative rational languages, equational logic, varieties, complete axiomatizations, commutative idempotent semirings, algebraically complete commutative idempotent semirings.

1 Introduction

A classic result of the theory of context-free languages is Parikh's theorem [25] that asserts that the letter occurrence vectors (Parikh vectors) corresponding to the words of a context-free language on a k-letter alphabet form a semilinear subset of $\mathbb{N}^k$, the free commutative monoid of k-dimensional

vectors over the naturals. The theorem is usually proved by combinatorial arguments on the derivation trees of the context-free grammar, and is regarded as one of the most fundamental, yet subtly difficult to prove, in the theory of context-free languages. However, as Pilling [27] observed, Parikh's theorem may be formulated as an assertion about "rational functions" on the (free) continuous commutative idempotent semiring of all subsets of $\mathbb{N}^k$. Subsequently, Kuich [20] generalized Parikh's result to all continuous commutative idempotent semirings (l-semirings). (See also [30] for a related treatment.) In fact, by introducing rational terms that denote rational functions, or more generally, recursion terms or μ-terms denoting functions that arise as least solutions of systems of polynomial fixed point equations, Parikh's theorem can be translated into a statement about the equational theory of continuous commutative idempotent semirings:

> For every μ-term t there exists a rational term r such that the equation $t = r$ holds in all continuous commutative idempotent semirings.

Alternatively, one may just consider rational terms and prove that for each rational term $t(x, y_1, \ldots, y_n)$ in the variables $x, y_1, \ldots, y_n$, there is a rational term $r(y_1, \ldots, y_n)$ containing no occurrence of x that provides least solution to the fixed point equation $x = t(x, y_1, \ldots, y_n)$ over *all* continuous commutative idempotent semirings. This approach has been pursued by Hopkins and Kozen in [14], in their argument lifting Parikh's theorem to all commutative idempotent semirings with enough least fixed points to provide solutions to recursion equations. By proving this more general result, Hopkins and Kozen have shown how to replace the analytic arguments of Pilling and Kuich by arguments based only on the least (pre-)fixed point rule (also known as the Park induction rule [26]), the fixed point equation, and the algebraic laws of the sum and product operations. But since Parikh's theorem is a claim about equational theories, one would eventually like to have a fully equational proof of it. In this paper, we derive Parikh's theorem from a small set of purely equational axioms involving fixed points.

Parikh's theorem is not the only result of automata and language theory that can be derived by simple *equational reasoning* from the algebraic properties of fixed points. Other applications of the equational logic of fixed points include proofs of Kleene's theorem and its generalizations [4] (see also [20, 21, 5], where the presentation is not fully based on equational reasoning), and of Greibach's normal form theorem for context-free grammars

[9]. The methods employed in the papers [19, 8] even indicate that one can embed the proof of the Krohn-Rhodes decomposition theorem [11] for finite automata and semigroups within equational logic. Further applications of fixed point theory include an equational proof of the soundness and relative completeness of Hoare's logic [2, 3]. (See also [18], and [23] for a not fully equational treatment.)

We will consider *terms*, or *μ-terms*, defined by the following (abstract) syntax, where x ranges over a fixed countable set X of variables:

$$T \quad ::= \quad x \mid T + T \mid T \cdot T \mid 0 \mid 1 \mid \mu x.T \ .$$

Thus, if t is a term and x is a variable, then $\mu x.t$ is a term. Such terms t may be interpreted as continuous functions $t_S : S^X \to S$ over continuous semirings S, and continuous idempotent semirings in particular. Such a semiring $S = (S, +, \cdot, 0, 1)$ has an idempotent additive structure, and equipped with the order $\leq$ induced by the additive structure it has all suprema. Moreover, the $\cdot$ operation preserves all suprema. (It is clear that the $+$ operation also preserves all suprema.) A prime example of such a semiring is the semiring L_{Σ^*} of all languages in Σ^*, where Σ is a finite or infinite alphabet, equipped with the union and concatenation operations as sum and product, and the empty set and the set whose unique element is the empty word as 0 and 1, respectively. More generally, if M is any monoid, then $P(M)$, the set of all subsets of M, equipped with the operations of set union and complex product as sum and product is a continuous idempotent semiring. In fact, one can easily show that the semiring L_{Σ^*} is freely generated by Σ in the category of continuous idempotent semirings and continuous semiring homomorphisms. In continuous semirings, terms of the form $\mu x.t$ are interpreted by least (pre-)fixed points.

As the semirings L_{Σ^*} are the free continuous idempotent semirings, an equation $t = t'$ between μ-terms with free variables in $Y = \{y_1, \ldots, y_n\}$ holds in all continuous idempotent semirings if and only if $t_{L_{Y^*}}(\{y_1\}, \ldots, \{y_n\}) = t'_{L_{Y^*}}(\{y_1\}, \ldots, \{y_n\})$, i.e., when t and t', viewed as context-free grammars, generate the same language in Y^*. Since the equivalence of context-free grammars is undecidable (see, e.g., [13]), it follows that, for μ-terms, the equational theory of continuous idempotent semirings is undecidable. Moreover, since the inequivalence of context free grammars is semidecidable, the equational theory of continuous idempotent semirings is not recursively enumerable. Thus, the equational theory of continuous idempotent semirings has no recursively enumerable basis. The same holds for continuous semirings, since the free continuous semirings are the semirings of power series

3

with coefficients in the semiring of naturals equipped with a top element, and since the equality of such algebraic series is also not semidecidable.

For continuous *commutative* idempotent semirings, however, the situation is completely different. The free continuous commutative idempotent semirings are the semirings of commutative languages, i.e., the semirings $L_{\Sigma^\oplus} = P(\Sigma^\oplus)$, where $\Sigma^\oplus$ is the free commutative monoid of commutative words generated by Σ. (When Σ is finite and has k elements, $L_{\Sigma^\oplus}$ is isomorphic to $P(\mathbb{N}^k)$.) By Parikh's theorem [25], the context-free sets included in $\Sigma^\oplus$ are the same as the rational sets, or the semilinear sets, and equality of semilinear sets is decidable and is logspace complete for Π_2^p, the second level of the polynomial time hierarchy [15]. It follows that the equivalence problem of commutative context-free grammars is decidable, see also [10]. In fact, as shown in [16], the equivalence problem for both commutative context-free grammars and commutative rational expressions are solvable in nondeterministic exponential time. Thus, the equational theory of continuous idempotent commutative semirings is also decidable in nondeterministic exponential time. An infinite basis of the rational identities for commutative languages was given by Redko [28] (see also the treatments by Salomaa [29] and Conway [6]). The language of rational terms is a sublanguage of the language of μ-terms. As a corollary of our equational proof of Parikh's theorem, and of Redko's axiomatization, we give a basis of identities of commutative languages and thus of continuous commutative idempotent semirings for the *full* language of μ-terms.

The paper is organized as follows. Section 2 is devoted to preliminary results on *-semirings that will be used throughout the paper, and culminates in a well-known normal form theorem for commutative rational expressions. We then introduce μ-semirings as a suitable class of models for the language of μ-terms, and present the collection of equations from which Parikh's theorem will be proven (Section 3). Our equational proof of Parikh's theorem is given in Section 4, together with other intermediate results of independent interest. Section 5 offers results on derivatives of rational terms. Algebraically complete commutative idempotent semirings are introduced in Section 6, where we show that these structures are models of the equations upon which our equational proof of Parikh's theorem is based. There we also prove that a very weak form of the least pre-fixed point rule suffices to prove Parikh's theorem. The last section of the paper (Section 7) uses our equational proof of Parikh's theorem, and Redko's axiomatization for commutative rational languages, to give a basis of identities of commutative

4

languages and thus of continuous commutative idempotent semirings for the language of μ-terms.

2 *-semirings

Recall that a (unitary) *semiring* [22, 12] is an algebra $S = (S, +, \cdot, 0, 1)$ such that $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid, and such that product distributes over all finite sums. In particular, 0 is an absorbing zero. A semiring is *commutative* if the product operation $\cdot$ is commutative, and *idempotent* if the sum operation $+$ is idempotent. Note that any idempotent semiring S is partially ordered by the *semilattice order* $\leq$ defined by $a \leq b$ iff $a + b = b$, and the constant 0 is least with respect to this partial order. A *ci-semiring* is a commutative idempotent semiring. A morphism of semirings is a function that preserves the operations and constants.

A *-*semiring* is a semiring S equipped with a star operation $^* : S \to S$. This operation is not required to satisfy any particular conditions. A *ci-*-semiring* is a ci-semiring which is a *-semiring. A morphism of *-semirings also preserves the star operation.

A *rational term* is any term built up in the usual way from variables and the symbols 0 and 1 using the operations $+, \cdot$ and *. The following classic equations between rational terms will be important in our treatment:

$$(x + y)^* = (x^* y)^* x^* \tag{1}$$
$$1 + xx^* = x^* \tag{2}$$
$$0^* = 1 \tag{3}$$
$$1^* = 1 \tag{4}$$
$$x + x = x \tag{5}$$
$$x^{**} = x^* \tag{6}$$
$$x^* x^* = x^* \tag{7}$$
$$(x + y)^* = x^* y^* \tag{8}$$
$$(xy^*)^* = 1 + xx^* y^* \ . \tag{9}$$

The following lemmas give a summary of those interrelations among the above equations that will be used in the sequel. Most of these facts are known, and can be found in the references, in particular in [6, 29]. We have included them in order to make the paper self-contained.

LEMMA 2.1 *In *-semirings (9) implies (2), which in turn implies (3).*

Proof. When x is 0, both (2) and (9) reduce to (3). Given that this holds, by substituting 0 for y, (9) reduces to (2). □

LEMMA 2.2 *In *-semirings, (2) and (4) imply (5).*

Indeed, if (2) and (4) hold, then $1 + 1 = 1 \cdot 1^* + 1 = 1^* = 1$, and the result follows by multiplying both sides of the equation $1 + 1 = 1$ by x.

Below, when (5) is implied by the assumptions, for any rational terms t, t' we will write $t \le t'$ as an abbreviation for the equation $t + t' = t'$. Note that modulo (5) and the defining equations of semirings, $t = t'$ holds iff both $t \le t'$ and $t' \le t$ do. Moreover, if $t \le t'$ holds, then so do the equations $t + s \le t' + s$, $ts \le t's$ and $st \le st'$. And if (1) and (2) also hold, then by $1 \le (x^*y)^* = 1 + x^*y(x^*y)^*$, whenever $x \le y$ we have that

$$x^* \ \le \ (x^*y)^*x^* \ = \ (x+y)^* \ = \ y^* \ .$$

Thus, if $t \le s$ holds, then so does $t^* \le s^*$. It follows that in *-semirings satisfying (1), (2) and (4) all the operations are monotonic with respect to $\le$.

LEMMA 2.3 *In *-semirings, equations (1), (2) and (4) jointly imply the equations (6) and (7).*

Proof. First note that $1 \le x^*$ holds, so that $x \le xx^* \le xx^* + 1 = x^*$ and thus $x^* \le x^{**}$, since * is monotonic. Moreover, using (1) and (4), we have

$$\begin{aligned} (x+1)^* \ &= \ x^{**}x^* \\ (1+x)^* \ &= \ (1^*x)^*1^* \\ &= \ x^* \ . \end{aligned}$$

Thus,

$$x^* \ \le \ x^{**} \ \le \ x^{**}x^* \ = \ x^* \ ,$$

proving (6) and (7). □

6

LEMMA 2.4 *In commutative $*$-semirings, equations (1), (7) and (9) imply equation (8).*

Proof. Since by Lemma 2.1 also (2) holds, we have

$$
\begin{aligned}
(x + y)^* &= y^*(xy^*)^* \\
&= y^*(1 + xx^*y^*) \\
&= y^* + xx^*y^* \\
&= (1 + xx^*)y^* \\
&= x^*y^* \ . \quad \square
\end{aligned}
$$

LEMMA 2.5 *In commutative $*$-semirings, equations (7), (8) and (9) imply equation (1).*

Proof. As in the previous argument, we can derive

$$
y^*(xy^*)^* = x^*y^* \ .
$$

But $x^*y^* = (x + y)^*$, by assumption, so that $y^*(xy^*)^* = (x + y)^*$. $\quad \square$

The following result summarizes the consequences of Lemmas 2.1–2.5.

COROLLARY 2.6 *In commutative $*$-semirings, the system of equations (1), (4), (9) and the system consisting of (4), (8), (9) are equivalent. Moreover, in commutative $*$-semirings either of them implies all of the equations (1)–(9).*

Proof. Indeed, in commutative semirings, we have by Lemma 2.1 that (9) implies (2) and (3), which together with (1) and (4) imply (5), (6) and (7) (Lemmas 2.2 and 2.3), and finally, (1), (7) and (9) jointly imply (8) (Lemma 2.4).

For the converse, note that in $*$-semirings, (8) and (5) imply (7), so that we may apply Lemma 2.5 to derive (1). $\quad \square$

We let Ax denote the system of equations consisting of (1), (4) and (9). Note that every semiring satisfying all of the equations in Ax is idempotent.

The following corollary offers generalizations of equations (8) and (9).

7

COROLLARY 2.7 *In commutative *-semirings satisfying Ax we have*

$$\begin{aligned}
(y_1 + \ldots + y_k)^* &= y_1^* \ldots y_k^* \\
(xy_1^* \ldots y_k^*)^* &= 1 + xx^* y_1^* \ldots y_k^* ,
\end{aligned}$$

for all $k \geq 0$.

Of course, the empty sum is 0 and the empty product is 1.

Call a rational term a *monomial* if it is a commutative word, i.e., a product of variables, where we take advantage of the associativity and commutativity of the product. A nonempty monomial is a monomial which is a nonempty product. A *star monomial* is a term of the form $uv_1^* \ldots v_k^*$, where $k \geq 0$, and $u, v_1, \ldots, v_k$ are monomials such that no v_i is empty.

PROPOSITION 2.8 (SALOMAA [29], CONWAY [6]) *In commutative *-semirings satisfying Ax, each rational term is equivalent to a finite sum of star monomials.*

Proof. This can be proven by induction on the structure of the rational term making use of Corollary 2.7. □

Rational terms that are sums of star monomials are called *terms in normal form*. Again, we take advantage of the associativity and commutativity of $+$. By (5) and (7), we may also require that the summands of each normal form term be pairwise different, and that in each star monomial $uv_1^* \ldots v_k^*$ which is a summand, the words v_i be pairwise different. Note that the term 0, i.e., the empty sum of star monomials, is in normal form.

COROLLARY 2.9 *For each rational term t and variable x there exist rational terms r and s such that s does not contain x and $t = rx + s$ holds in all commutative *-semirings satisfying Ax.*

Proof. Either by structural induction or by Proposition 2.8. □

3 μ-semirings

Recall the definition of μ-terms from the introduction. The variable x is *bound* in the term $\mu x.t$. The set of *free variables* in a term is defined as

usual. We call a term *finite* if it contains no subterm of the form $\mu x.t$. Below we will sometimes write $t(x_1, \ldots, x_n)$ or $t(\vec{x})$, where $\vec{x} = (x_1, \ldots, x_n)$ is a vector of different variables, to indicate that the free variables of term t belong to the set $\{x_1, \ldots, x_n\}$. We identify any two terms that only differ in the bound variables. *Substitution* $t[t'/x]$ and *simultaneous substitution* $t[(t_1, \ldots, t_n)/(x_1, \ldots, x_n)]$ are defined as usual. When $t = t(x_1, \ldots, x_n)$, we also write $t(t_1, \ldots, t_n)$ for $t[(t_1, \ldots, t_n)/(x_1, \ldots, x_n)]$.

A *μ-semiring* is a semiring A together with an interpretation of the μ-terms t as functions $t_A : A^X \to A$, where X denotes the set of all variables, such that the following hold:

1. When t is a variable x, then t_A is the corresponding projection $A^X \to A$, i.e., $t_A(\rho) = \rho(x)$, for all $\rho : X \to A$. Moreover, 0_A and 1_A are the corresponding constants in the semiring, and $(t + s)_A(\rho) = t_A(\rho) + s_A(\rho)$ and $(t \cdot s)_A(\rho) = t_A(\rho) \cdot s_A(\rho)$, the sum and product of $t_A(\rho)$ and $s_A(\rho)$ in the underlying semiring of A, for all μ-terms t and s, and for all $\rho : X \to A$.

2. For any μ-terms t, t' and variable x, the function $(t[t'/x])_A$ is the "composite" of the functions t_A and t'_A, so that

$$(t[t'/x])_A(\rho) \quad = \quad t_A(\rho[x \mapsto t'_A(\rho)]) \ ,$$

   where for any $\rho : X \to A$ and $b \in A$, the function $\rho[x \mapsto b]$ is the same as ρ except that it maps x to b.

3. If t, t' are μ-terms with $t_A = t'_A$, then for all variables x, it also holds that $(\mu x.t)_A = (\mu x.t')_A$.

It follows that t_A depends at most on those arguments that correspond to the variables with at least one free occurrence in t. Indeed, if x has no free occurrence in t and y does not occur in t, then we have

$$
\begin{aligned}
t_A(\rho) &= (t[y/x])_A(\rho) \\
&= t_A(\rho[x \mapsto \rho(y)]) \ ,
\end{aligned}
$$

for all $\rho : X \to A$. Thus, for all $a, b \in A$ and $\rho : X \to A$,

$$
\begin{aligned}
t_A(\rho[x \mapsto a]) &= t_A(\rho[x \mapsto \rho(y)]) \\
&= t_A(\rho[x \mapsto b]) \ .
\end{aligned}
$$

When the underlying semiring of A is commutative, or idempotent, we call A a commutative, or idempotent, μ-semiring. A ci-μ-semiring is both commutative and idempotent. Morphism of μ-semirings commute with the functions induced by the μ-terms. It is clear that any such morphism is a semiring morphism.

Suppose that $t = t(x_1, \ldots, x_n)$ is a μ-term and A is a μ-semiring. When $\rho : X \to A$ with $x_i \mapsto a_i$, $i = 1, \ldots, n$, below we will write $t_A(a_1, \ldots, a_n)$, or just $t(a_1, \ldots, a_n)$ for $t_A(\rho)$. Note that for finite terms t, the function t_A is just the function induced by t over the underlying semiring of A.

Suppose that t and t' are μ-terms. We say that an *equation* or *identity* $t = t'$ *holds in a μ-semiring* A, or *is satisfied by* A, if t and t' induce equal functions in A, i.e., when $t_A = t'_A$ holds. Note that if $t = t'$ holds in A, then so does any equation $t[(t_1, \ldots, t_n)/(x_1, \ldots, x_n)] = t'[(t_1, \ldots, t_n)/(x_1, \ldots, x_n)]$ as does $\mu x.t = \mu x.t'$, for all variables x.

We will be interested in interpretations where $\mu x.t$ provides solution to the fixed point equation $x = t$. In such interpretations, fixed points usually satisfy several equational properties, cf. [4]. Below, in addition to the *fixed point identity*

$$\mu x.t = t[\mu x.t/x] \ , \tag{10}$$

we will need the *diagonal identity*

$$\mu x.\mu y.t = \mu x.t[x/y] \tag{11}$$

and the *parameter identity*

$$(\mu z.xz + 1)y = \mu z.xz + y \ . \tag{12}$$

Each rational term r may be identified with a μ-term. When r is 0, 1, or a variable, then r is also a μ-term. Moreover, when r is the sum or product of rational terms r_1 and r_2, then the μ-term corresponding to r is just the sum or product of the μ-terms corresponding to the r_i, $i = 1, 2$. Finally, if r is s^*, then the μ-term corresponding to r is $\mu x.tx + 1$, where x is a fresh variable and t is the μ-term corresponding to s. *Below we will identify any rational term with the corresponding μ-term.* Note that this identification does not conflict with term substitution. Thus, the parameter identity (12) may be reformulated as

$$x^*y = \mu z.xz + y \ .$$

10

Note also that any μ-semiring A is automatically a *-semiring with star operation $a \mapsto t_A(a)$, where t is the term $x^* = \mu z.xz + 1$. Moreover, μ-semiring morphisms preserve star.

One can also prove that any μ-semiring satisfying (10) and (12) satisfies (2).

3.1 Lemmas for μ-terms

Our aim in the remainder of this paper will be to offer a purely equational proof of Parikh's classic theorem [25]. In our formulation, Parikh's theorem takes the form of a "normal form" theorem for μ-terms. We now present some lemmas that will be useful in the proof of our main result.

LEMMA 3.1 *Any μ-semiring satisfying (11) and (12) also satisfies (1).*

Proof.

$$
\begin{aligned}
(x + y)^* &= \mu z.(x + y)z + 1 \\
&= \mu z.xz + yz + 1 \\
&= \mu z_1.\mu z_2.xz_2 + yz_1 + 1 \\
&= \mu z_1.x^*(yz_1 + 1) \\
&= \mu z_1.(x^*y)z_1 + x^* \\
&= (x^*y)^*x^* . \quad \square
\end{aligned}
$$

The next technical lemma introduces an equation (see equation (13) below) that, together with the diagonal and parameter identities, will allow us to eliminate every occurrence of μ in terms. This will be crucial in our promised equational proof of Parikh's theorem.

LEMMA 3.2 *Suppose that*

$$
\mu x.(yx)^*z + u = (y(z + u))^*z + u \tag{13}
$$

holds in a commutative μ-semiring satisfying the diagonal identity (11) and the parameter identity (12). Then so does the equation

$$
\mu x.(yx^k)^*z + u = (y(z + u)^k)^*z + u , \tag{14}
$$

for every $k \geq 1$.

Proof. We prove the claim by induction on k. The basis case $k = 1$ holds by assumption. For the induction step we argue thus:

$$
\begin{aligned}
\mu x.(yx^{k+1})^* z + u &= \mu v.\mu x.(yvx^k)^* z + u \\
&= \mu v.(yv(z + u)^k)^* z + u \\
&= \mu v.(y(z + u)^k v)^* z + u \\
&= (y(z + u)^k (z + u))^* z + u \\
&= (y(z + u)^{k+1})^* z + u \ . \quad \square
\end{aligned}
$$

LEMMA 3.3 *If (13) holds in a commutative μ-semiring satisfying the diagonal identity (11) and the parameter identity (12), then so does*

$$
\mu x.yx^k + z = (yz^{k-1})^* z \ ,
$$

for each $k \geq 1$.

Proof. This is clear for $k = 1$. Assume that $k > 1$. Then, by (11), (12) and (14),

$$
\begin{aligned}
\mu x.yx^k + z &= \mu x.\mu u.yx^{k-1} u + z \\
&= \mu x.(yx^{k-1})^* z \\
&= (yz^{k-1})^* z \ . \quad \square
\end{aligned}
$$

4   Normal form

We let μAx denote the system of equations consisting of the diagonal identity (11), the parameter identity (12), equation (13), and the equations (4), (9). Note that in commutative μ-semirings, these equations imply (1) (Lemma 3.1), so that in such semirings, all of the equations (1)–(9) hold. In particular, all of the equations in Ax hold. Moreover, any commutative μ-semiring satisfying μAx is idempotent and is thus a ci-μ-semiring.

Below we will write $\mu Ax \models t = t'$ to denote that the equation $t = t'$ between the μ-terms t and t' holds in all *commutative μ-semirings* satisfying μAx (or, equivalently, that $t = t'$ is provable from μAx using the rules of equational logic for μ-terms [4]). In the same way, we write $Ax \models r = r'$, for rational terms r and r', to denote that any *commutative *-semiring* satisfying Ax also satisfies the equation $r = r'$.

THEOREM 4.1 (PARIKH'S THEOREM) *In commutative μ-semirings satisfying μAx, any μ-term is equivalent to a rational term in normal form.*

The remainder of this section will be devoted to the proof of this theorem. In fact, as will be clear in what follows, Theorem 4.1 will be a corollary of a result to the effect that any fixed point equation

$$x \;=\; t(x, y_1, \ldots, y_n) \;,$$

where $t(x, y_1, \ldots, y_n)$ is a rational term, has a canonical rational solution $r(y_1, \ldots, y_n)$ (cf. Theorem 4.5 and Proposition 4.6 to follow). The following Proposition 4.2 and Lemmas 4.3 and 4.4 are stepping stones in the proof of this result.

PROPOSITION 4.2 *For every rational term $r(x, \vec{y})$ and variables u, v, it holds that*

$$\mathrm{Ax} \;\models\; r(u^*v, \vec{y}) \cdot u^* = r(v, \vec{y}) \cdot u^* \;.$$

Proof. Below we will write just $r(x)$ for $r(x, \vec{y})$.

First we establish the claim for star monomials which are of the form $r(x) = a_0 x^{k_0}(a_1 x^{k_1})^* \ldots (a_n x^{k_n})^*$, where the a_i do not contain any occurrence of x. We have:

$$
\begin{aligned}
r(u^*v) \cdot u^* \;&=\; a_0(u^*v)^{k_0}(a_1(u^*v)^{k_1})^* \ldots (a_n(u^*v)^{k_n})^* u^* \\
&=\; a_0 v^{k_0}(a_1 v^{k_1} u^*)^* \ldots (a_n v^{k_n} u^*)^* u^* \\
&=\; a_0 v^{k_0} u^*(a_1 v^{k_1} u^*)^* \ldots u^*(a_n v^{k_n} u^*)^* u^* \\
&=\; a_0 v^{k_0} u^*(a_1 v^{k_1})^* \ldots u^*(a_n v^{k_n})^* u^* \\
&=\; a_0 v^{k_0}(a_1 v^{k_1})^* \ldots (a_n v^{k_n})^* u^* \\
&=\; r(v) \cdot u^* \;.
\end{aligned}
$$

Since any rational term is equivalent to a finite sum of star monomials and the claim clearly holds if $r(x)$ is 0, the proof of the proposition can be completed by showing that if our claim holds for $r_1(x)$ and $r_2(x)$, then it holds for $r(x) = r_1(x) + r_2(x)$. But this is immediate, since in this case,

$$
\begin{aligned}
r(u^*v) \cdot u^* \;&=\; (r_1(u^*v) + r_2(u^*v)) \cdot u^* \\
&=\; r_1(u^*v)u^* + r_2(u^*v)u^* \\
&=\; r_1(v)u^* + r_2(v)u^* \\
&=\; (r_1(v) + r_2(v)) \cdot u^* \\
&=\; r(v) \cdot u^* \;. \quad \square
\end{aligned}
$$

Suppose that $r(x, \vec{y})$ and $s(\vec{y})$ are rational terms. With respect to our axiom system μAx, the equations

$$\mu x.r(x, \vec{y}) \cdot x + s(\vec{y}) \;=\; r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \qquad\qquad (15)$$

and

$$\mu x.r(x, \vec{y})^* \cdot s(\vec{y}) \;=\; r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \qquad\qquad (16)$$

are equivalent. Indeed, by the diagonal identity (11), we have

$$
\begin{aligned}
\mu x.r(x, \vec{y}) \cdot x + s(\vec{y}) &= \mu x.\mu z.r(x, \vec{y}) \cdot z + s(\vec{y}) \\
&= \mu x.r(x, \vec{y})^* \cdot s(\vec{y}) \ .
\end{aligned}
$$

Below we will prove that (15) and (16) always hold under μAx.

LEMMA 4.3 *Suppose that $p(x, \vec{y})$ and $q(x, \vec{y})$ are rational terms such that for all rational terms $a(\vec{y})$ and $c(\vec{y})$ it holds that*

$$
\begin{aligned}
\mu Ax &\models \mu x.a(\vec{y}) \cdot p(x, \vec{y}) \cdot x + c(\vec{y}) = (a(\vec{y}) \cdot p(c(\vec{y}), \vec{y}))^* \cdot c(\vec{y}) \\
\mu Ax &\models \mu x.a(\vec{y}) \cdot q(x, \vec{y}) \cdot x + c(\vec{y}) = (a(\vec{y}) \cdot q(c(\vec{y}), \vec{y}))^* \cdot c(\vec{y}) \ .
\end{aligned}
$$

Then, for the product $r(x, \vec{y}) = p(x, \vec{y}) \cdot q(x, \vec{y})$ and for all rational terms $a(\vec{y})$ and $c(\vec{y})$, we have

$$\mu Ax \;\models\; \mu x.a(\vec{y}) \cdot r(x, \vec{y}) \cdot x + c(\vec{y}) = (a(\vec{y}) \cdot r(c(\vec{y}), \vec{y}))^* \cdot c(\vec{y}) \ .$$

Proof. Below we write $r(x)$ in lieu of $r(x, \vec{y})$, and abbreviate $a(\vec{y})$ and $c(\vec{y})$ to a and c, respectively. We argue thus:

$$
\begin{aligned}
\mu x.a \cdot r(x) \cdot x + c &= \mu x.a \cdot p(x) \cdot q(x) \cdot x + c \\
&= \mu x.\mu z.a \cdot p(x) \cdot q(z) \cdot z + c \\
&= \mu x.(a \cdot p(x) \cdot q(c))^* \cdot c \\
&= \mu x.\mu z.a \cdot q(c) \cdot p(x) \cdot z + c \\
&= \mu x.a \cdot q(c) \cdot p(x) \cdot x + c \\
&= (a \cdot q(c) \cdot p(c))^* \cdot c \\
&= (a \cdot r(c))^* \cdot c \ . \quad \square
\end{aligned}
$$

LEMMA 4.4 *For all star monomials $r(x, \vec{y})$ and rational terms $a(\vec{y})$ and $c(\vec{y})$,*
it holds that

$$\mu Ax \quad \models \quad \mu x . a(\vec{y}) \cdot r(x, \vec{y}) \cdot x + c(\vec{y}) = (a(\vec{y}) \cdot r(c(\vec{y}), \vec{y}))^* \cdot c(\vec{y}) \ .$$

Proof. Below we will write just $r(x)$ for $r(x, \vec{y})$, a for $a(\vec{y})$, etc. We argue
by induction on the "length" of r.

When $r(x)$ is 1, then $\mu x . ax + c = a^* c$ holds by the parameter identity.
In the induction step, we have that $r(x) = p(x)q(x)$ where $q(x)$ is a star
monomial and $p(x) = bx^k$ or $p(x) = (bx^k)^*$. The result follows by the
induction assumption applied to $q(x)$ and Lemmas 4.3, 3.2 and 3.3.   □

We are now ready to prove the promised result to the effect that, over
μ-semirings satisfying μAx, rational fixed point equations have canonical
rational solutions (cf. Proposition 4.6 to follow). Apart from its intrinsic
interest, this theorem will also have application in our proof of Parikh's
theorem.

THEOREM 4.5 *For every rational terms $r(x, \vec{y})$ and $s(\vec{y})$, we have that*

$$\mu Ax \quad \models \quad \mu x . r(x, \vec{y}) \cdot x + s(\vec{y}) = r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \ .$$

Proof. We prove this equation in the equivalent form

$$\mu x . r(x, \vec{y})^* \cdot s(\vec{y}) \quad = \quad r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \ ,$$

i.e., writing just $r(x)$ for $r(x, \vec{y})$ and c for $s(\vec{y})$,

$$\mu x . r(x)^* \cdot c \quad = \quad r(c)^* \cdot c \ .$$

We have already shown in Lemma 4.4 that this holds when $r(x)$ is a star
monomial. Since every rational term is equivalent to a sum of star mono-
mials, and since the claim is obvious for the term 0, to complete the proof
it is sufficient to show that if

$$\mu Ax \quad \models \quad \mu x . r_i(x)^* \cdot c = r_i(c)^* \cdot c, \quad i = 1, 2,$$

then

$$\mu Ax \quad \models \quad \mu x . r(x)^* \cdot c = r(c)^* \cdot c \ ,$$

for $r(x) = r_1(x) + r_2(x)$. Using Proposition 4.2, this is shown as follows:

$$
\begin{aligned}
\mu x.r(x)^* \cdot c &= \mu x.(r_1(x) + r_2(x))^* \cdot c \\
&= \mu x.r_1(x)^* \cdot r_2(x)^* \cdot c \\
&= \mu x.\mu y.r_1(x)^* \cdot r_2(y)^* \cdot c \\
&= \mu x.r_2(r_1(x)^* c)^* \cdot r_1(x)^* \cdot c \\
&= \mu x.r_2(c)^* \cdot r_1(x)^* \cdot c \\
&= r_1(r_2(c)^* c)^* \cdot r_2(c)^* \cdot c \\
&= r_1(c)^* \cdot r_2(c)^* \cdot c \\
&= (r_1(c) + r_2(c))^* \cdot c \\
&= r(c)^* \cdot c \ . \quad \square
\end{aligned}
$$

Proof of Theorem 4.1, completed. Recall that we need to show that, in commutative μ-semirings satisfying μAx, each μ-term $t = t(\vec{y})$ is equivalent to a rational term in normal form. Actually, since by Proposition 2.8, with respect to the equations in Ax every rational term is equivalent to a rational term in normal form, it suffices to prove that in commutative μ-semirings satisfying μAx, each μ-term is equivalent to a rational term. We prove this claim by induction on the structure of t. When t is a variable or a constant, our claim is obvious. In the induction step, there are three cases to deal with. The cases that t is the sum or product of two terms are obvious, since rational terms are closed with respect to these operations. The nontrivial case is when t is $\mu x.t'(x, \vec{y})$, for some μ-term $t'(x, \vec{y})$ and variable x. But, by the induction assumption, there is a rational term equivalent to t', and, by Corollary 2.9, we can assume that this term is of the form $r(x, \vec{y}) \cdot x + s(\vec{y})$. But then, by Theorem 4.5, t is equivalent modulo μAx to $r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y})$, which is a rational term. $\qquad\square$

PROPOSITION 4.6 *With respect to the axiom system μAx, the fixed point identity (10) holds for all μ-terms.*

Proof. Suppose that $t(x, \vec{y})$ is a μ-term. By Theorem 4.1 and Corollary 2.9, we know that there exist rational terms $r(x, \vec{y})$ and $s(\vec{y})$ such that, modulo our axioms, $t(x, \vec{y}) = r(x, \vec{y}) \cdot x + s(\vec{y})$. By Theorem 4.5, we have that, with respect to μAx,

$$
\mu x.t(x, \vec{y}) = r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \ .
$$

Thus, using Proposition 4.2,

$$
\begin{aligned}
t(\mu x.t, \vec{y}) &= r(r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}), \vec{y}) \cdot r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) + s(\vec{y}) \\
&= r(s(\vec{y}), \vec{y}) \cdot r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) + s(\vec{y}) \\
&= (r(s(\vec{y}), \vec{y}) \cdot r(s(\vec{y}), \vec{y})^* + 1) \cdot s(\vec{y}) \\
&= r(s(\vec{y}), \vec{y})^* \cdot s(\vec{y}) \\
&= \mu x.t(x, \vec{y}) \ . \quad \square
\end{aligned}
$$

5 Derivatives

The *derivative* t_x of a rational term t with respect to a variable is defined as follows (cf. [14, Sect. 3.2]).

- If t is 0, 1, or a variable other than x, then $t_x = 0$. If t is the variable x, then $t_x = 1$.

- If t is $r + s$, for rational terms r, s, then $t_x = r_x + s_x$.

- If t is rs, for rational terms r, s, then $t_x = r_x s + r s_x$.

- If $t = s^*$, for a rational term s, then $t_x = s^* s_x$.

Intuitively, if we interpret t as a commutative rational language, then t_x denotes the rational language consisting of all the commutative words that can be obtained from those in t by deleting one occurrence of the letter x. We refer the interested reader to [6, Chapter 5] and [14] for more information on derivatives of rational expressions and further applications. Below, we shall use derivatives to offer another characterization of the rational solutions of rational fixed point equations (cf. Theorem 5.5 to follow).

We omit the simple proof of the following fact.

LEMMA 5.1 *If r does not contain any occurrence of x, then $Ax \models r_x = 0$.*

PROPOSITION 5.2 *If $Ax \models r = s$, for rational terms r, s, then $Ax \models r_x = s_x$, for all variables x, i.e., derivation is stable with respect to Ax.*

Proof. By the above definition, we have that for all rational terms r, s, t with $Ax \models r_x = s_x$, also $Ax \models (r + t)_x = (s + t)_x$, $Ax \models (rt)_x = (st)_x$, and

$Ax \models (r^*)_x = (s^*)_x$. Thus, to complete the proof, we only need to show that if $r = s$ is a substitution instance of one of the axioms in Ax, then $Ax \models r_x = s_x$, for all variables x. This is clear for (4), since the derivatives with respect to any variable of both sides of this equation are 0. As for (9), we have, for any rational terms s, t and any variable x,

$$
\begin{aligned}
((st^*)^*)_x &= (st^*)^*(s_x t^* + st^* t_x) \\
&= (1 + ss^* t^*)(s_x t^* + st^* t_x) \\
&= s_x t^* + st_x t^* + s_x ss^* t^* + sst_x s^* t^* \\
&= s_x s^* t^* + st_x s^* t^* \\
&= s_x s^* t^* + ss_x s^* t^* + ss^* t_x t^* \\
&= (1 + ss^* t^*)_x \ \ .
\end{aligned}
$$

Since with respect to the other axioms, (1) is equivalent to (8), the proof can be completed by showing that $Ax \models ((s + t)^*)_x = (s^* t^*)_x$, for all rational terms s, t. But

$$
\begin{aligned}
((s + t)^*)_x &= (s + t)^*(s_x + t_x) \\
&= s^* t^*(s_x + t_x) \\
&= s^* s_x t^* + s^* t^* t_x \\
&= (s^* t^*)_x \ \ . \quad \square
\end{aligned}
$$

LEMMA 5.3 *For all rational terms r and variables x,*

$$
Ax \ \models \ r_x x \le r \ \ .
$$

Proof. We prove this by induction on the structure of r. When r is $0, 1$, or a variable other than x, we have by Ax that $r_x x = 0$. When r is $s + t$, then $r_x x = s_x x + t_x x \le s + t = r$, by the induction assumption. Suppose now that r is of the form st. Then, it holds that

$$
r_x x = s_x tx + st_x x \le st + st = st \ \ ,
$$

by (5) and the induction assumption. Finally, if r is s^*, for some rational term s, then $r_x = s^* s_x$, so that by using the fixed point equation (2), we have that

$$
r_x x = s^* s_x x \le s^* s \le ss^* + 1 = s^* = r \ \ . \quad \square
$$

Thinking of a rational term $t(x, \vec{y})$ as denoting a commutative regular language over letters $x, \vec{y}$, we expect that this language contains all the words

that can be obtained by adding one occurrence of x to those in the language denoted by t_x, and of those in t in which x does not occur. The following proposition shows that the axiom system Ax is strong enough to prove this result.

PROPOSITION 5.4 *For all rational terms $t(x, \vec{y})$, it holds that*

$$Ax \ \models \ t(x, \vec{y}) = t_x(x, \vec{y}) \cdot x + t(0, \vec{y}) \ .$$

Proof. We know that for some rational terms $r(x, \vec{y})$ and $s(\vec{y})$, it holds that

$$Ax \ \models \ t(x, \vec{y}) = r(x, \vec{y}) \cdot x + s(\vec{y}) \ .$$

Thus, by substituting 0 for x,

$$Ax \ \models \ t(0, \vec{y}) = s(\vec{y}) \ .$$

By Proposition 5.2, also

$$Ax \ \models \ t_x(x, \vec{y}) = (r(x, \vec{y})x + s(\vec{y}))_x = r_x(x, \vec{y})x + r(x, \vec{y}) \ ,$$

since $s_x(\vec{y}) = 0$ (Lemma 5.1). Since by Lemma 5.3 it holds that

$$Ax \ \models \ r_x(x, \vec{y})x \leq r(x, \vec{y}) \ ,$$

we have that

$$Ax \ \models \ t_x(x, \vec{y}) = r(x, \vec{y}) \ ,$$

completing the proof. $\qquad\square$

THEOREM 5.5 *For each rational term $r(x, \vec{y})$ it holds that*

$$\mu Ax \ \models \ \mu x. r(x, \vec{y}) = r_x(r(0, \vec{y}), \vec{y})^* \cdot r(0, \vec{y}) \ . \tag{17}$$

Proof. From Proposition 5.4 and Theorem 4.5. $\qquad\square$

Hopkins and Kozen in [14] derive Proposition 5.4 and (17) from the axioms of Kozen's semirings [17].

6 Least pre-fixed points

Suppose that A is a ci-μ-semiring. Thus, A is equipped with the semilattice order $a \leq b$ iff $a + b = b$. We call A *algebraically complete* [9] if A satisfies the fixed point and parameter equations (10), (12), and if for all μ-terms t and $\rho : X \to A$, $x \in X$ and $a \in A$,

$$t_A(\rho[x \mapsto a]) \leq a \quad \Rightarrow \quad (\mu x.t)_A(\rho) \leq a \ ,$$

i.e., when A satisfies the *least pre-fixed point rule* (also known as *Park induction rule* [26])

$$t[y/x] \leq y \quad \Rightarrow \quad \mu x.t \leq y \ .$$

Morphisms of algebraically complete ci-semirings are μ-semiring morphisms. Note that any morphism preserves the partial order.

The most important examples of algebraically complete ci-semirings are the *continuous ci-semirings*. Such a semiring is a ci-semiring such that the supremum of every set $B \subseteq A$ exists, with respect to the semilattice order $\leq$. Moreover, the $\cdot$ operation is continuous, i.e., it preserves the supremum of any directed set in each of its arguments. It then follows that the product operation is in fact completely additive, i.e., it preserves all suprema. Morphisms of continuous ci-semirings are continuous semiring morphisms. We may turn any continuous ci-semiring into an algebraically complete ci-semiring by defining $(\mu x.t)_A(\rho)$, for each μ-term t and function $\rho : X \to A$, as the least pre-fixed point of the map $a \mapsto t_A(\rho[x \mapsto a])$, $a \in A$. It follows that any morphism of continuous ci-semirings commutes with the functions induced by the μ-terms and is thus a morphism of algebraically complete semirings. We will return to continuous ci-semirings in Section 7.

The following facts are well-known and in fact do not require that product is commutative. (See, e.g., [4, 24].)

PROPOSITION 6.1 *When A is an algebraically complete ci-semiring, each function t_A, induced by a μ-term t, is monotonic with respect to the pointwise order on A^X.*

LEMMA 6.2 *Every algebraically complete ci-semiring satisfies the diagonal identity (11).*

Our order of business will now be to show that:

PROPOSITION 6.3 *Every algebraically complete ci-semiring satisfies all of the equations in μAx.*

For ease of presentation, and for further reference, we break the proof of the above proposition in several intermediate results. These we now proceed to present.

COROLLARY 6.4 *Every algebraically complete ci-semiring satisfies (1) and (2).*

Proof. It is clear that in μ-semirings, equation (2) is a particular instance of the fixed point identity (10). The fact that (1) holds in all algebraically complete ci-semirings follows from Lemmas 6.2 and 3.1. □

For a μ-term $t(x, \vec{y})$, define the sequence of μ-terms $t^k(x, \vec{y})$, $k \geq 0$, by induction on k:

$$
\begin{aligned}
t^0(x, \vec{y}) &= x \\
t^{k+1}(x, \vec{y}) &= t(t^k(x, \vec{y}), \vec{y}) \ .
\end{aligned}
$$

Below we will make use of the following simple property of algebraically complete ci-semirings A, which is easily proved by using the monotonicity of the term functions (Proposition 6.1): For all μ-terms $t(x, y_1, \ldots, y_n)$ and all $b_1, \ldots, b_n \in A$ and $k \geq 0$, if

$$
t_A^k(0, b_1, \ldots, b_n) = t_A^{k+1}(0, b_1, \ldots, b_n) \ ,
$$

then

$$
(\mu x.t)_A(b_1, \ldots, b_n) = t_A^k(0, b_1, \ldots, b_n) \ .
$$

Thus, any algebraically complete ci-semiring satisfies

$$
t^k(0, \vec{y}) = t^{k+1}(0, \vec{y}) \quad \Rightarrow \quad \mu x.t = t^k(0, \vec{y}) \ , \tag{18}
$$

for all μ-terms t, variables x and for all $k \geq 0$.

LEMMA 6.5 *Every algebraically complete ci-semiring satisfies (4).*

21

Proof. Suppose that A is an algebraically complete ci-semiring. Let $t(x)$ denote the term $x + 1$. Then $t_A(0) = 1 = 1 + 1 = t_A^2(0)$, so that $1^* = (\mu x.t)_A = t_A(0) = 1$, proving that (4) holds in A. $\qquad\square$

COROLLARY 6.6 *Each of the equations (1)–(7) holds in all algebraically complete ci-semirings.*

Proof. First note that (5) holds by assumption in all ci-semirings. Moreover, we already know that (1), (2) and (4) hold in all algebraically complete ci-semirings. But it was shown in Section 2 that in *-semirings, these equations imply (3), (6) and (7), cf. Lemmas 2.1, 2.2 and 2.3. $\qquad\square$

LEMMA 6.7 *Every algebraically complete ci-semiring satisfies (9).*

Proof. By Corollary 6.6 we have that

$$
\begin{aligned}
(xy^*)^* &= xy^*(xy^*)^* + 1 \\
&\geq xy^*x^* + 1 \\
&= 1 + xx^*y^*
\end{aligned}
$$

holds in all algebraically complete semirings. As for the converse, suppose that A is an algebraically complete ci-semiring and $a, b \in A$. We have

$$
\begin{aligned}
ab^*(1 + aa^*b^*) &= ab^* + a^2a^*b^* \\
&= aa^*b^* \\
&\leq 1 + aa^*b^* \ .
\end{aligned}
$$

Thus, $(ab^*)^* \leq 1 + aa^*b^*$ holds, by the least pre-fixed point rule. $\qquad\square$

In light of Corollary 2.6 and of the previous results, we have that:

COROLLARY 6.8 *Every algebraically complete ci-semiring satisfies all of the equations (1)–(9).*

The following result gives the missing ingredient in the proof of Proposition 6.3.

LEMMA 6.9 *Every algebraically complete ci-semiring satisfies (13).*

Proof. Let a, b, c be elements of an algebraically complete ci-semiring A, and let f denote the function $A \to A$, $x \mapsto (ax)^*b + c$. By Corollary 6.8, we have that:

$$
\begin{aligned}
f(0) &= b + c \\
f^2(0) &= (a(b+c))^*b + c \\
&= (ab)^*(ac)^*b + c \\
f^3(0) &= f^2(0) \ .
\end{aligned}
$$

Indeed,

$$
\begin{aligned}
f^3(0) &= [a((ab)^*(ac)^*b + c)]^*b + c \\
&= [ab(ab)^*(ac)^* + ac]^*b + c \\
&= [ab(ab)^*(ac)^*]^*(ac)^*b + c \\
&= (1 + ab(ab)^*(ac)^*)(ac)^*b + c \\
&= [(ac)^* + ab(ab)^*(ac)^*]b + c \\
&= [1 + ab(ab)^*](ac)^*b + c \\
&= (ab)^*(ac)^*b + c \ .
\end{aligned}
$$

It follows that $f^2(0) = (a(b+c))^*b + c$ is the least pre-fixed point of f, and thus equals $\mu x.(ax)^*b + c$. $\qquad\square$

By Proposition 6.3 and Theorem 4.1, we can derive the following corollary, which was obtained, in the setting of Kozen's semirings, in [14].

COROLLARY 6.10 (HOPKINS AND KOZEN [14]) *For each μ-term t there is a rational term s in normal form such that $t = s$ holds in all algebraically complete ci-semirings, and hence in all continuous ci-semirings.*

In fact, if r is any rational term such that $\mu Ax \models t = r$, then we have that $t = r$ holds in all algebraically complete ci-semirings.

In the proof of Lemma 6.9, in addition to some equations, we only used a weak property of least pre-fixed points, namely (18) for $k = 2$. We thus have:

PROPOSITION 6.11 *For every μ-term t there is a rational term r in normal form such that $t = r$ holds in all commutative μ-semirings satisfying the diagonal and parameter equations (11), (12), the equations (4), (9), and the implication (18) for $k = 2$.*

As a consequence of the above result, we have that a very weak form of the least pre-fixed point rule suffices to establish Parikh's theorem.

7 Completeness

Redko [28] supplied a (necessarily infinite) basis of the rational equations of commutative languages, and hence of ci-*-semirings derived from continuous ci-semirings. However, as pointed out in Conway [6], the proof given in [28] (and the one included in [29]) is incomplete, so that Pilling's proof, reported in [6], completes Redko's argument.

We use Redko's theorem to prove:

THEOREM 7.1 *The commutative semiring equations together with those in μAx and the equations*

$$x^*y^* = (xy)^*(x^* + y^*) \tag{19}$$

$$x^* = (x^p)^*(1 + x + \ldots + x^{p-1}) \ , \tag{20}$$

for all prime numbers p, form an equational basis of the class of (μ-semirings derived from) continuous ci-semirings.

Proof. Let E denote the system of equations given in the statement of the theorem. Suppose that t_1, t_2 are μ-terms such that the equation $t_1 = t_2$ holds in all continuous ci-semirings. We know that there exist rational terms r_1, r_2 with $\mu Ax \models t_i = r_i$, $i = 1, 2$. By Redko's theorem, the rational equations in E are complete for the rational equations that hold in continuous ci-semirings. Hence, E proves $r_1 = r_2$ and thus $t_1 = t_2$. The proof is completed by noting that all of the equations in E hold in all continuous ci-semirings. $\square$

In fact, the system given in the preceding theorem is redundant. As shown in [6], one may omit equation (9).

COROLLARY 7.2 *An equation between μ-terms holds in all continuous ci-semirings iff it holds in all algebraically complete ci-semirings.*

Proof. This follows if we can derive the equations (19) and (20) in all algebraically complete ci-semirings. But this was done in [17]. $\square$

As mentioned in the introduction, for each set Σ, the semiring $L_{\Sigma\oplus}$ of all subsets of $\Sigma^{\oplus}$, the free commutative monoid generated by Σ, is freely generated by Σ (more precisely, by the singleton sets corresponding to the elements of Σ) in the class of all continuous ci-semirings. This means that if S is any continuous ci-semiring and h is a function $\Sigma \to S$, then h extends to a unique continuous semiring morphism $L_{\Sigma\oplus} \to S$. It is well-known that each commutative context-free language over Σ, viz. the image of a context-free language in Σ^{*} under the canonical morphism $\Sigma^{*} \to \Sigma^{\oplus}$, is the first component of the least solution of a system of "polynomial fixed point equations" over $L_{\Sigma\oplus}$. Moreover, one can solve systems of fixed point equations by the method of successive elimination of the variables (also known as Gaussian elimination, cf. [1, 7]). It follows that the commutative context-free languages over Σ are exactly those of the form $L = t_{L_{\Sigma\oplus}}(\{\sigma_1\}, \ldots, \{\sigma_n\})$, where $t(x_1, \ldots, x_n)$ is any μ-term and each σ_i is a letter in Σ. But by Corollary 6.10, any such L can be constructed from the singletons and the constants $0, 1$ by the rational operations of $+, \cdot$ and *. We thus have that every commutative context-free language is rational, a statement that is very close to Parikh's [25] original formulation of this result.

REMARK 7.3 By Corollary 7.2, algebraically complete ci-semirings and continuous ci-semirings satisfy the same equations between μ-terms. Thus, the fact that Parikh's theorem holds in all algebraically complete ci-semirings is no stronger than the result that Parikh's theorem holds in all continuous ci-semirings (cf. Corollary 6.10).

Let $CR_{\Sigma\oplus}$ denote the collection of all commutative context-free, i.e., rational languages in $\Sigma^{\oplus}$. Then $CR_{\Sigma\oplus}$ is closed under the functions induced by the μ-terms. It follows that $CR_{\Sigma\oplus}$ is itself a ci-μ-semiring, in fact an algebraically complete ci-semiring, and thus a ci-*-semiring. As a ci-*-semiring, $CR_{\Sigma\oplus}$ is freely generated by Σ in the class of all ci-*-semirings satisfying Redko's axioms. A *variety* of μ-semirings is any class of μ-semirings containing all μ-semirings that satisfy all of the equations that hold in every member of the variety.

By our previous results we have:

COROLLARY 7.4 *$CR_{\Sigma\oplus}$, as a ci-μ-semiring, is freely generated by Σ in each of the following classes of μ-semirings:*

1. *The class of all ci-μ-semirings satisfying the equations μAx and (19) and (20).*

2. *The class of all ci-μ-semirings that satisfy every equation that holds in all continuous ci-semirings.*

3. *The class of all algebraically complete ci-semirings.*

Proof. By Theorem 7.1, the first two classes are actually the same, and by Corollary 7.2, this class contains the third. Thus, since $CR_{\Sigma\oplus}$ is an algebraically complete ci-semiring, we only need to prove that given any μ-semiring S that satisfies all of the equations of continuous ci-semirings, and given any function $h : \Sigma \to S$, there is a unique μ-semiring morphism $h^\sharp : CR_{\Sigma\oplus} \to S$ extending h. But since a version of Birkhoff's variety theorem holds for μ-semirings (and actually for all preiteration algebras), S is a "morphic image of a sub-μ-semiring of a direct product" [4] of continuous ci-semirings, viewed as ci-μ-semirings. In fact, since equipped with the pointwise order, any direct product of continuous ci-semirings is itself continuous, S is a morphic image of a sub-μ-semiring S'' of a continuous ci-semiring S'. Let f denote a surjective morphism $S'' \to S$, and let g be any function $\Sigma \to S'$ such that $f(g(\sigma)) = h(\sigma)$, for all $\sigma \in \Sigma$. Now g extends to a continuous semiring morphism $g^\sharp : L_{\Sigma\oplus} \to S'$, which is also a μ-semiring morphism. Thus, the restriction of $g^\sharp$ to $CR_{\Sigma\oplus}$ is a μ-semiring morphism $\overline{g} : CR_{\Sigma\oplus} \to S'$. Moreover, the image of $CR_{\Sigma\oplus}$ under $\overline{g}$ is a subset of S'', so that we may view $\overline{g}$ as a morphism $CR_{\Sigma\oplus} \to S''$. It follows that the composite of $\overline{g}$ with f is a morphism $h^\sharp : CR_{\Sigma\oplus} \to S$ which extends h. It is clear that $h^\sharp$ is unique. $\qquad\square$

References

[1] H. Bekić. Definable operations in general algebras, and the theory of automata and flowcharts. *Technical Report*, IBM Laboratory, Vienna, 1969.

[2] S. L. Bloom and Z. Ésik. Floyd-Hoare logic in iteration theories. *J. Assoc. Comput. Mach.*, 38(1991), 887–934.

[3] S. L. Bloom and Z. Ésik. Program correctness and matricial iteration theories. In: *Proc. Mathematical Foundations of Programming Semantics'91*, LNCS 598, Springer-Verlag, 1992, 457–475.

[4] S. L. Bloom and Z. Ésik. *Iteration Theories*. Springer-Verlag, 1993.

[5] S. Bozapalidis. Equational elements in additive algebras. *Theory Comput. Syst.*, 32(1999), 1–33.

[6] J. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, 1971.

[7] J. W. De Bakker and D. Scott, A theory of programs, *IBM Seminar*, Vienna, 1969.

[8] Z. Ésik. Group axioms for iteration. *Inform. and Comput.*, 148(1999), 131–180.

[9] Z. Ésik and H. Leiss. In preparation.

[10] S. Ginsburg. *The Mathematical Theory of Context-Free Languages*. McGraw-Hill, 1966.

[11] A. Ginzburg. *Algebraic Theory of Automata*. Academic Press, New York-London, 1968.

[12] J. S. Golan. *Semirings and their Applications*. Kluwer Academic Publishers, Dordrecht, 1999.

[13] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, Reading, Mass., 1979.

[14] M. W. Hopkins and D. Kozen. Parikh's theorem in commutative Kleene algebra. In: *Proc. IEEE Conf. Logic in Computer Science (LICS'99)*, IEEE Press, 1999, 394–401.

[15] D. T. Huynh. The complexity of semilinear sets. *Elektron. Informationsverarb. Kybernet*, 18(1982), 291–338.

[16] D. T. Huynh. The complexity of equivalence problems for commutative grammars. *Inform. and Control*, 66(1985), 103–121.

[17] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Inform. and Comput.*, 110(1994), 366–390.

[18] D. Kozen. On Hoare logic and Kleene algebra with tests. In: *Proc. IEEE Conf. Logic in Computer Science (LICS'99), IEEE, July 1999, 167–172.*

[19] D. Krob. Complete systems of B-rational identities. *Theoret. Comput. Sci.*, 89(1991), 207–343.

[20] W. Kuich. The Kleene and the Parikh theorem in complete semirings. In: *Proc. ICALP '87*, LNCS 267, Springer-Verlag, 212–225.

[21] W. Kuich. Gaussian elimination and a characterization of algebraic power series. In: *Proc. Mathematical Foundations of Computer Science, 1998*, LNCS 1450, Springer, Berlin, 1998, 512–521.

[22] W. Kuich and A. Salomaa. *Semirings, Automata, Languages.* Springer-Verlag, Berlin, 1986.

[23] E. G. Manes and M. A. Arbib. *Algebraic Approaches to Program Semantics.* Springer-Verlag, New York, 1986.

[24] D. Niwiński. On fixed-point clones (extended abstract). In: *Automata, Languages and Programming, Rennes, 1986*, LNCS 226, Springer, 1986. 464–473.

[25] R. J. Parikh. On context-free languages. *J. Assoc. Comput. Mach.*, 13(1966), 570–581.

[26] D. M. R. Park. Fixed point induction and proofs of program properties. In: *Machine Intelligence* 5, Edinburgh Univ. Press, 1970, 59–78.

[27] D. L. Pilling. Commutative regular equations and Parikh's theorem. *J. London Math. Soc.*, 6(1973), 663–666.

[28] V. N. Redko. On the algebra of commutative events. (Russian) *Ukrain. Mat. Ž.* 16(1964), 185–195.

[29] A. Salomaa. *Theory of Automata.* Pergamon Press, 1969.

[30] I. Takanami and N. Honda. A characterization of Parikh's theorem and semilinear sets by commutative semigroups with length. *Electronics and Communications in Japan*, 52(1969), 179–184.

Recent BRICS Report Series Publications

RS-01-28 Luca Aceto, Zoltán Ésik, and Anna Ingólfsdóttir. *A Fully Equational Proof of Parikh's Theorem*. June 2001. 28 pp.

RS-01-27 Mario Jose Cáccamo and Glynn Winskel. *A Higher-Order Calculus for Categories*. June 2001. 24 pp. Appears in Boulton and Jackson, editors, *Theorem Proving in Higher Order Logics: 14th International Conference*, TPHOLs '01 Proceedings, LNCS 2152, 2001, pages 136–153.

RS-01-26 Ulrik Frendrup and Jesper Nyholm Jensen. *A Complete Axiomatization of Simulation for Regular CCS Expressions*. June 2001. 18 pp.

RS-01-25 Bernd Grobauer. *Cost Recurrences for DML Programs*. June 2001. 51 pp. Extended version of a paper to appear in Leroy, editor, *Proceedings of the 6th ACM SIGPLAN International Conference on Functional Programming*, 2001.

RS-01-24 Zoltán Ésik and Zoltán L. Németh. *Automata on Series-Parallel Biposets*. June 2001. 15 pp. To appear in Kuich, editor, *5th International Conference*, Developments in Language Theory DLT '01 Proceedings, LNCS, 2001.

RS-01-23 Olivier Danvy and Lasse R. Nielsen. *Defunctionalization at Work*. June 2001. 45 pp. Extended version of an article to appear in Søndergaard, editor, *3rd International Conference on Principles and Practice of Declarative Programming*, PPDP '01 Proceedings, 2001.

RS-01-22 Zoltán Ésik. *The Equational Theory of Fixed Points with Applications to Generalized Language Theory*. June 2001. 21 pp. To appear in Kuich, editor, *5th International Conference*, Developments in Language Theory DLT '01 Proceedings, LNCS, 2001.