On Fixed Point Equations over Commutative Semirings

Javier Esparza, Stefan Kiefer, and Michael Luttenberger

Universität Stuttgart
Institute for Formal Methods in Computer Science
Stuttgart, Germany
{esparza,kiefersn,luttenml}@informatik.uni-stuttgart.de

Abstract. Fixed point equations $\mathbf{x} = \mathbf{f}(\mathbf{x})$ over ω-continuous semirings can be seen as the mathematical foundation of interprocedural program analysis. The sequence $\mathbf{0}, \mathbf{f}(\mathbf{0}), \mathbf{f}^2(\mathbf{0}), \ldots$ converges to the least fixed point $\mu\mathbf{f}$. The convergence can be accelerated if the underlying semiring is commutative. We show that accelerations in the literature, namely Newton's method for the arithmetic semiring [4] and an acceleration for commutative Kleene algebras due to Hopkins and Kozen [5], are instances of a general algorithm for arbitrary commutative ω-continuous semirings. In a second contribution, we improve the $\mathcal{O}(3^n)$ bound of [5] and show that their acceleration reaches $\mu\mathbf{f}$ after n iterations, where n is the number of equations. Finally, we apply the Hopkins-Kozen acceleration to itself and study the resulting hierarchy of increasingly fast accelerations.

1 Introduction

Interprocedural program analysis is the art of extracting information about the executions of a procedural program without executing it, and fixed point equations over ω-continuous semirings can be seen as its mathematical foundation. A program can be mapped (in a syntax-driven way) to a system of fixed point equations over an abstract semiring containing one equation for each program point. Depending on the information on the program one wants to compute, the carrier and the abstract semiring operations can be instantiated so that the desired information is the least solution of the system. To illustrate this, consider a (very abstractly defined) program consisting of one single procedure X. This procedure can either do an action a and terminate, or do an action b and call itself twice. Schematically:

$$X \xrightarrow{a} \varepsilon \qquad X \xrightarrow{b} XX$$

The abstract equation corresponding to this program is

$$x = r_a + r_b \cdot x \cdot x \tag{1}$$

where $+$ and $\cdot$ are the abstract semiring operations. In order to compute the language $L(X)$ of terminating executions of the program, we instantiate the

semiring as follows: The carrier is $2^{\{a,b\}^*}$ (the set of languages over the alphabet $\{a,b\}$), $r_a = \{a\}$, $r_b = \{b\}$, $+$ is set union, and $\cdot$ is language concatenation. It is easy to prove that $L(X)$ is the least solution of (1) under this interpretation. But we can also be interested in other questions. We may wish to compute the *Parikh image* of $L(X)$, i.e., the set of vectors $(n_a, n_b) \in \mathbb{N}^2$ such that some terminating execution of the program does exactly n_a a's and n_b b's, respectively. For this, we take $2^{\mathbb{N}^2}$ as carrier, $r_a = \{(1,0)\}$, $r_b = \{(0,1)\}$, define $+$ as set union and $\cdot$ by $X \cdot Y = \{(x_a + y_a, x_b + y_b) \mid (x_a, x_b) \in X, (y_a, y_b) \in Y\}$. We may also be interested in quantitative questions. For instance, assume that the program X executes a with probability p and b with probability $(1-p)$. The probability that X eventually terminates is the least solution of (1) interpreted over $\mathbb{R}^+ \cup \{0, \infty\}$ with $r_a = p$, $r_b = (1-p)$, and the standard interpretation of $+$ and $\cdot$ (see for instance [3, 4]). If instead of the probability of termination we are interested in the probability of the most likely execution, we just have to reinterpret $+$ as the max operator.

The semirings corresponding to all these interpretations share a property called *ω-continuity* [7]. This property allows to apply the Kleene fixed point theorem and to prove that the least solution of a system of equations $\mathbf{x} = \mathbf{f}(\mathbf{x})$ is the supremum of the sequence $\mathbf{0}, \mathbf{f}(\mathbf{0}), \mathbf{f}^2(\mathbf{0}), \ldots$, where $\mathbf{0}$ is the vector whose components are all equal to the neutral element of $+$. If the carrier of the semiring is finite, this yields a procedure to compute the solution. However, if the carrier is infinite, the procedure rarely terminates, and its convergence can be very slow. For instance, the approximations to $L(X)$ are all finite sets of words, while $L(X)$ is infinite. Another example is the probability case with $p = 1/2$; the least fixed point (the least solution of $x = 1/2x^2 + 1/2$) is 1, but $\mathbf{f}^k(0) \leq 1 - \frac{1}{k+1}$ for every $k \geq 0$, which means that the Kleene scheme needs 2^i iterations to approximate the solution within i bits of precision[1].

Due to the slow convergence of $(\mathbf{f}^k(\mathbf{0}))_{k\geq 0}$, it is natural to look for "accelerations". Loosely speaking, an acceleration is a procedure of low complexity that on input $\mathbf{f}$ yields a function $\mathbf{g}$ having the same least fixed point $\mu\mathbf{f}$ as $\mathbf{f}$, but such that $(\mathbf{g}^k(\mathbf{0}))_{k\geq 0}$ converges faster to $\mu\mathbf{f}$ than $(\mathbf{f}^k(\mathbf{0}))_{k\geq 0}$. In [5], Hopkins and Kozen present a very elegant acceleration—although they do not use this term—that works for *every* commutative and idempotent ω-continuous semiring[2], i.e., for every ω-continuous semiring in which $\cdot$ is commutative and $+$ is idempotent (this is the case for both the Parikh image and the probability of the most likley computation). They prove that, remarkably, the acceleration is guaranteed to terminate. More precisely, they show that the fixed point is always reached after at most $\mathcal{O}(3^n)$ iterations, where n is the number of equations.

In this paper we further investigate the Hopkins-Kozen acceleration. In the first part of the paper we show that, in a certain formal sense, this acceleration was already discovered by Newton more than 300 years ago. In the arithmetic semiring, where the carrier is $\mathbb{R}^+ \cup \{0, \infty\}$ and $+$ and $\cdot$ have their usual mean-

[1] This example is adapted from [4].

[2] Actually, in [5] the result is proved for commutative Kleene algebras, an algebraic structure more general than our semirings (cf. Section 4.1).

ings, one can compute the least solution of $\mathbf{x} = \mathbf{f}(\mathbf{x})$ as a zero of $\mathbf{f}(\mathbf{x}) - \mathbf{x}$. Due to this connection, Newton's numerical method for approximating the zeros of a differentiable function (see [8]) can also be seen as an acceleration for the arithmetic case, which has been been studied by Etessami and Yannakakis [4] in a different context. Here we show that the Hopkins-Kozen acceleration and Newton's are two particular instances of an acceleration for equations over arbitrary commutative ω-continuous semirings [7] and, in this sense, "the same thing".

In a second contribution, we improve the $\mathcal{O}(3^n)$ bound of [5] and show that the acceleration is actually much faster: the fixed point is already reached after n iterations. Finally, in a third contribution we investigate the possibility of "accelerating the acceleration". We study a hierarchy $\{\mathcal{H}_i\}_{i\geq 1}$ of increasingly faster accelerations, with $\mathcal{H}_1$ as the Hopkins-Kozen acceleration, and show that k iterations of the i-th acceleration can already be matched by ki iterations of the basic acceleration.

In Section 2 we introduce commutative ω-continuous semirings following [7]. In Section 3 we introduce the Hopkins-Kozen acceleration and Newton's method. In Section 4 we present our generalisation and derive both the Hopkins-Kozen acceleration and Newton's method as particular cases. In Section 5 we prove that the Hopkins-Kozen acceleration terminates after n steps. The hierarchy of accelerations is studied in Section 6. Missing proofs can be found in a technical report [2].

2 ω-Continuous Semirings

A *semiring* is a quintuple $\langle A, +, \cdot, 0, 1\rangle$ s.t.

(i) $\langle A, +, 0\rangle$ is a commutative monoid,
(ii) $\langle A, \cdot, 1\rangle$ is a monoid,
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in A$,
(iv) $0 \cdot a = a \cdot 0$ for all $a \in A$.

A semiring is

- *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in A$;
- *idempotent* if $a + a = a$ for all $a \in A$;
- *naturally ordered* if the relation $\leq$ given by $a \leq b \Leftrightarrow \exists c \in A : a + c = b$ is a partial order (this relation is always reflexive and transitive, but not necessarily antisymmetric);
- *complete* if it is possible to define "infinite sums" as an extension of finite sums, that are associative, commutative and distributive with respect to $\cdot$ as are finite sums. The formal axioms are given in [7]. In complete semirings, the unary *-operator is defined by $a^* = \sum_{j\geq 0} a^j$. Notice that $a^* = 1 + aa^*$;
- *ω-continuous* if it is naturally ordered, complete, and for all sequences $(a_i)_{i\in\mathbb{N}}$ with $a_i \in A$

$$\sup\left\{\sum_{i=0}^{n} a_i \mid n \in \mathbb{N}\right\} = \sum_{i\in\mathbb{N}} a_i.$$

Notation 1. *We abbreviate commutative ω-continuous semiring to* cc-semiring.

Remark 1. For our proofs the existence and ω-continuity of *countable* sums is sufficient. While in the idempotent case there is the term of commutative *closed semirings* for such structures (see [6]), it seems that there is no such term in the non-idempotent case.

Examples of semirings include $\langle \mathbb{N} \cup \{0, \infty\}, +, \cdot, 0, 1\rangle$, $\langle \mathbb{R}^+ \cup \{0, \infty\}, +, \cdot, 0, 1\rangle$, $\langle \mathbb{N} \cup \{0, \infty\}, \min, +, \infty, 0\rangle$ and $\langle 2^{\Sigma^*}, \cup, \cdot, \emptyset, \varepsilon\rangle$. They are all ω-continuous. The last two have an idempotent $+$-operation (min resp. $\cup$), and all but the last one are commutative.

2.1 Systems of Power Series

Let A be an ω-continuous semiring and let $\mathcal{X} = \{x_1, \ldots, x_n\}$ be a set of variables. We write $\mathbf{x}$ for the vector $(x_1, \ldots, x_n)^\top$. For every $i \in \{1, \ldots, n\}$, let $f_i(\mathbf{x})$ be a *(semiring) power series with coefficients in A*, i.e., a countable sum of products of elements of $A \cup \mathcal{X}$, and let $\mathbf{f}(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_n(\mathbf{x}))^\top$. We call $\mathbf{x} = \mathbf{f}(\mathbf{x})$ a *system of power series over A*. A vector $\bar{\mathbf{x}} \in A^n$ with $\mathbf{f}(\bar{\mathbf{x}}) = \bar{\mathbf{x}}$ is called a *solution* or a *fixed point* of $\mathbf{f}$.

Given two vectors $\bar{\mathbf{x}}, \bar{\mathbf{y}} \in A^n$, we write $\bar{\mathbf{x}} \leq \bar{\mathbf{y}}$ if $\bar{x}_i \leq \bar{y}_i$ (w.r.t. the natural order of A) in every component. The *least fixed point of* $\mathbf{f}$, denoted by $\mu\mathbf{f}$, is the fixed point $\bar{\mathbf{x}}$ with $\bar{\mathbf{x}} \leq \bar{\mathbf{y}}$ for every fixed point $\bar{\mathbf{y}}$. It exists and can be computed by the following theorem.

Theorem 1 (Kleene fixed point theorem, cf. [7]). *Let $\mathbf{x} = \mathbf{f}(\mathbf{x})$ be a system of power series over an ω-continuous semiring. Then $\mu\mathbf{f}$ exists and $\mu\mathbf{f} = \sup_{k \in \mathbb{N}} \mathbf{f}^k(\mathbf{0})$.*

3 Two Acceleration Schemes

Loosely speaking, an acceleration is a procedure that on input $\mathbf{f}$ yields a function $\mathbf{g}$ having the same least fixed point $\mu\mathbf{f}$ as $\mathbf{f}$, but converging "faster" to it, meaning that $\mathbf{f}^k(\mathbf{0}) \leq \mathbf{g}^k(\mathbf{0})$ for every $k \geq 0$. In order to exclude trivial accelerations like $\mathbf{g}(\mathbf{x}) = \mu\mathbf{f}$, a formal definition should require the procedure to have low complexity with respect to some reasonable complexity measure. Since such a definition would take too much space and would not be relevant for our results, we only use the term "acceleration" informally.

We describe two accelerations for different classes of cc-semirings. Both of them are based on the notion of derivatives. Given a polynomial or a power series $f(\mathbf{x})$, its derivative $\frac{\partial f}{\partial x_i}$ with respect to the variable x_i is defined as follows, where $a \in A$ and g, g_j, h are polynomials or power series (see also [5]):

$$\frac{\partial a}{\partial x_i} = 0 \qquad \frac{\partial}{\partial x_i}(g + h) = \frac{\partial g}{\partial x_i} + \frac{\partial h}{\partial x_i} \qquad \frac{\partial}{\partial x_i}(g \cdot h) = \frac{\partial g}{\partial x_i} \cdot h + g \cdot \frac{\partial h}{\partial x_i}$$

$$\frac{\partial x_j}{\partial x_i} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \qquad \frac{\partial}{\partial x_i} \sum_{j \in \mathbb{N}} g_j = \sum_{j \in \mathbb{N}} \frac{\partial g_j}{\partial x_i}$$

The *Jacobian* of a vector $\mathbf{f}(\mathbf{x})$ is then the $n\times n$-matrix $\mathbf{f}'(\mathbf{x})$ given by $\mathbf{f}'(\mathbf{x})_{ij} = \dfrac{\partial f_i}{\partial x_j}$.

3.1 The Hopkins-Kozen Acceleration

In [5] Hopkins and Kozen introduce an acceleration of the Kleene procedure for *idempotent* cc-semirings and prove that it reaches the fixed point after finitely many steps. Given a system of power series $\mathbf{x} = \mathbf{f}(\mathbf{x})$, the *Hopkins-Kozen sequence* is defined by

$$\boldsymbol{\kappa}^{(0)} = \mathbf{f}(\mathbf{0}) \quad \text{and} \quad \boldsymbol{\kappa}^{(k+1)} = \mathbf{f}'(\boldsymbol{\kappa}^{(k)})^* \cdot \boldsymbol{\kappa}^{(k)}.$$

Theorem 2 (Hopkins and Kozen [5]). *Let $\mathbf{x} = \mathbf{f}(\mathbf{x})$ be a system of power series over an idempotent cc-semiring. There is a function $N : \mathbb{N} \to \mathbb{N}$ with $N(n) \in \mathcal{O}(3^n)$ s.t. $\boldsymbol{\kappa}^{(N(n))} = \mu\mathbf{f}$, where n is the number of variables of the system.*

Actually, [5] prove the theorem for commutative Kleene algebras, whose axioms are weaker than those of idempotent cc-semirings. There is no notion of infinite sums in the Kleene algebra axioms, especially the Kleene star operator $*$ and its derivative are defined axiomatically.

Example 1. Let $\langle 2^{\{a\}^*}, +, \cdot, 0, 1\rangle$ denote the cc-semiring $\langle 2^{\{a\}^*}, \cup, \cdot, \emptyset, \{\varepsilon\}\rangle$. For simplicity, we write a^i instead of $\{a^i\}$. Consider the equation system

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2^2 + a \\ x_1^2 \end{pmatrix} = \mathbf{f}(\mathbf{x}) \text{ with } \mathbf{f}'(\mathbf{x})^* = (x_1 x_2)^* \begin{pmatrix} 1 & x_2 \\ x_1 & 1 \end{pmatrix}.$$

The Hopkins-Kozen acceleration reaches the least fixed point $\mu\mathbf{f}$ after two steps:

$$\boldsymbol{\kappa}^{(0)} = (a, 0)^\top, \quad \boldsymbol{\kappa}^{(1)} = (a, a^2)^\top, \quad \boldsymbol{\kappa}^{(2)} = (a^3)^*(a, a^2)^\top.$$

It is easy to check that $\boldsymbol{\kappa}^{(2)}$ is a fixed point of $\mathbf{f}$. By Theorem 2 we have $\boldsymbol{\kappa}^{(2)} = \mu\mathbf{f}$.

3.2 Newton's Acceleration

Newton's method for approximating the zeros of a differentiable real function $\mathbf{g}(\mathbf{x})$ is one of the best known methods of numerical analysis. It computes the sequence

$$\mathbf{x}^{(0)} = \mathbf{s} \quad \text{and} \quad \mathbf{x}^{(k+1)} = \mathbf{x}^{(k)} - \mathbf{g}'(\mathbf{x}^{(k)})^{-1} \cdot \mathbf{g}(\mathbf{x}^{(k)}).$$

starting at the *seed* $\mathbf{s}$. Under certain conditions on $\mathbf{g}(\mathbf{x})$ and on the seed $\mathbf{s}$ (typically the seed must be "close enough" to the solution) the sequence converges to a solution of the equation $\mathbf{g}(\mathbf{x}) = \mathbf{0}$.

In order to approximate a solution of an equation system $\mathbf{x} = \mathbf{f}(\mathbf{x})$ over the reals, we can apply Newton's method to the function $\mathbf{g}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) - \mathbf{x}$, which gives the sequence

$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(k+1)} = \mathbf{x}^{(k)} + (\mathbf{1} - \mathbf{f}'(\mathbf{x}^{(k)}))^{-1}(\mathbf{f}(\mathbf{x}^{(k)}) - \mathbf{x}^{(k)}).$$

4 An Acceleration for Arbitrary cc-Semirings

We show that the Hopkins-Kozen and Newton's accelerations are two instances of a general acceleration for arbitrary cc-semirings, which we call the cc-scheme. The proof relies on lemmata from [5] and [4], which we reformulate and generalise so that they hold for arbitrary cc-semirings.

The *cc-scheme* is given by:

$$\boldsymbol{\nu}^{(0)} = \mathbf{0} \quad \text{and} \quad \boldsymbol{\nu}^{(k+1)} = \boldsymbol{\nu}^{(k)} + \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot \boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}),$$

where $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ is any vector s.t. $\boldsymbol{\nu}^{(k)} + \boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}(\boldsymbol{\nu}^{(k)})$.
The scheme leaves the choice of $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ free, but there is always at least one $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ satisfying the condition (see Lemma 2 below).

The following theorem states that the cc-scheme accelerates the Kleene scheme $(\mathbf{f}^k(\mathbf{0}))_{k\in\mathbb{N}}$.

Theorem 3. *Let $\mathbf{x} = \mathbf{f}(\mathbf{x})$ be a system of power series over a cc-semiring. Then the iterates $\boldsymbol{\nu}^{(k)}$ of the cc-scheme exist and satisfy $\mathbf{f}^k(\mathbf{0}) \leq \boldsymbol{\nu}^{(k)} \leq \mu\mathbf{f}$ for all $k \geq 0$.*

The proof uses the following fundamental property of derivatives in cc-semirings:

Lemma 1 (Taylor's Theorem, cf. [5]). *Let $\mathbf{f}(\mathbf{x})$ and $\mathbf{d}$ be vectors of power series over a cc-semiring. Then*

$$\mathbf{f}(\mathbf{x}) + \mathbf{f}'(\mathbf{x}) \cdot \mathbf{d} \leq \mathbf{f}(\mathbf{x} + \mathbf{d}) \leq \mathbf{f}(\mathbf{x}) + \mathbf{f}'(\mathbf{x} + \mathbf{d}) \cdot \mathbf{d}.$$

The following lemma assures the existence of a suitable $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ for each k.

Lemma 2. *Let $\boldsymbol{\nu}^{(k)}$ be the k-th iterate of the cc-scheme. For all $k \geq 0$: $\mathbf{f}(\boldsymbol{\nu}^{(k)}) \geq \boldsymbol{\nu}^{(k)}$. So, there is a $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ such that $\boldsymbol{\nu}^{(k)} + \boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}(\boldsymbol{\nu}^{(k)})$.*

What remains to show for Theorem 3 is $\mathbf{f}^k(\mathbf{0}) \leq \boldsymbol{\nu}^{(k)} \leq \mu\mathbf{f}$ (cf. [2]).

In the rest of the section we show that the Hopkins-Kozen acceleration and Newton's acceleration are special cases of the cc-scheme.

4.1 Idempotent cc-Semirings

If addition is idempotent, we have $x \leq y$ iff $x + y = y$, as $x \leq y$ implies that there is a d with $x + d = y$ so that $x + y = x + (x + d) = x + d = y$. By Lemma 2 we have $\boldsymbol{\nu}^{(k)} \leq \mathbf{f}(\boldsymbol{\nu}^{(k)})$. In the cc-scheme (see above) we therefore may choose $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}(\boldsymbol{\nu}^{(k)})$. Moreover, since $\mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \geq \mathbf{1}$ by the definition of the Kleene star and since $\boldsymbol{\nu}^{(k)} \leq \mathbf{f}(\boldsymbol{\nu}^{(k)})$ by Lemma 2 we get

$$\boldsymbol{\nu}^{(k)} \leq \mathbf{f}(\boldsymbol{\nu}^{(k)}) \leq \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot \mathbf{f}(\boldsymbol{\nu}^{(k)})$$

and by idempotence

$$\boldsymbol{\nu}^{(k)} + \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot \mathbf{f}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot \mathbf{f}(\boldsymbol{\nu}^{(k)}) \,.$$

So the cc-scheme collapses in the idempotent case to

$$\boldsymbol{\nu}^{(0)} = \mathbf{0} \quad \text{and} \quad \boldsymbol{\nu}^{(k+1)} = \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot \mathbf{f}(\boldsymbol{\nu}^{(k)}).$$

In other words, $\boldsymbol{\nu}^{(k+1)}$ results from $\boldsymbol{\nu}^{(k)}$ by applying the operator $\mathcal{N}_{\mathbf{f}}(\mathbf{x}) := \mathbf{f}'(\mathbf{x})^* \cdot \mathbf{f}(\mathbf{x})$. Recall that the Hopkins-Kozen sequence is given by

$$\boldsymbol{\kappa}^{(0)} = \mathbf{f}(\mathbf{0}) \quad \text{and} \quad \boldsymbol{\kappa}^{(k+1)} = \mathbf{f}'(\boldsymbol{\kappa}^{(k)})^* \cdot \boldsymbol{\kappa}^{(k)}.$$

So it is obtained by repeatedly applying the Hopkins-Kozen operator $\mathcal{H}_{\mathbf{f}}(\mathbf{x}) := \mathbf{f}'(\mathbf{x})^* \cdot \mathbf{x}$, starting from $\mathbf{f}(\mathbf{0})$. While the two sequences are not identical, the following theorem shows that they are essentially the same.

Theorem 4.

1. *For all* $k > 0 : \boldsymbol{\kappa}^{(k-1)} \leq \boldsymbol{\nu}^{(k)} \leq \boldsymbol{\kappa}^{(k)}$.
2. *For all* $k \geq 0 : \boldsymbol{\kappa}^{(k)} = \mathcal{H}^k_{\mathbf{f}}(\mathbf{f}(\mathbf{0})) = \mathcal{N}^k_{\mathbf{f}}(\mathbf{f}(\mathbf{0}))$.

4.2 The Semiring over the Nonnegative Reals

We now consider the cc-semiring $\langle \mathbb{R}^+ \cup \{0, \infty\}, +, \cdot, 0, 1\rangle$. In order to instantiate the cc-scheme, we have to choose $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)})$ so that $\boldsymbol{\nu}^{(k)} + \boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}(\boldsymbol{\nu}^{(k)})$ holds. By Lemma 2 we have $\boldsymbol{\nu}^{(k)} \leq \mathbf{f}(\boldsymbol{\nu}^{(k)})$, and so we can take $\boldsymbol{\delta}(\boldsymbol{\nu}^{(k)}) = \mathbf{f}(\boldsymbol{\nu}^{(k)}) - \boldsymbol{\nu}^{(k)}$. The cc-acceleration becomes

$$\boldsymbol{\nu}^{(0)} = \mathbf{0} \quad \text{and} \quad \boldsymbol{\nu}^{(k+1)} = \boldsymbol{\nu}^{(k)} + \mathbf{f}'(\boldsymbol{\nu}^{(k)})^* \cdot (\mathbf{f}(\boldsymbol{\nu}^{(k)}) - \boldsymbol{\nu}^{(k)}) .$$

It is easy to see that for any nonnegative real-valued square matrix $\mathbf{A}$, if $\sum_{k\in\mathbb{N}} \mathbf{A}^k = \mathbf{A}^*$ has only finite entries, then $(\mathbf{1} - \mathbf{A})^{-1}$ exists and equals $\mathbf{A}^*$. If this is the case for $\mathbf{A} = \mathbf{f}'(\boldsymbol{\nu}^{(k)})^*$, then Newton's method coincides with the cc-acceleration for the reals and thus converges to $\mu\mathbf{f}$. In [4] Etessami and Yannakakis give sufficient conditions for $\mathbf{f}'(\boldsymbol{\nu}^{(k)})^* = (\mathbf{1} - \mathbf{f}'(\boldsymbol{\nu}^{(k)}))^{-1}$ when $\mathbf{f}$ is derived from a recursive Markov chain.

5 Convergence Speed in Idempotent Semirings

In the first subsection we want to analyse how many steps the Newton iteration or, equivalently, the Hopkins-Kozen iteration needs to reach $\mu\mathbf{f}$ when we consider an idempotent cc-semiring $\langle A, +, \cdot, 0, 1\rangle$, i.e. we have the additional equation $1 + 1 = 1$. In the subsequent subsection we then generalise the obtained results to the setting of commutative Kleene algebras.

5.1 Idempotent cc-Semirings

In this subsection $\mathbf{f}$ again denotes a system of n power series in the variables $\mathcal{X} = \{x_1, \ldots, x_n\}$, i.e. we have $f_i(\mathbf{x}) = \sum_{\boldsymbol{\iota}\in\mathbb{N}^n} c^{(i)}_{\boldsymbol{\iota}} \mathbf{x}^{\boldsymbol{\iota}}$, where $\mathbf{x}^{\boldsymbol{\iota}}$ denotes the product $x_1^{\iota_1} \cdot \ldots \cdot x_n^{\iota_n}$ and $c^{(i)}_{\boldsymbol{\iota}} \in A$ for all $\boldsymbol{\iota} \in \mathbb{N}^n$ and $1 \leq i \leq n$. We define the concept of *derivation trees* of our system $\mathbf{f}$ as in formal language theory.

Notation 2. *In the following, if u is a node of a tree t, we identify u with the subtree of t rooted at u. In particular, t is also used to denote t's root. The* height $h(t)$ *of t is defined as usual, e.g. a tree consisting only of a single node has height* 0.

Definition 1. *A* partial derivation tree t of x_i *is a labelled tree satisfying:*

- *every node of t is labelled by either an element of A or an element of $\mathcal{X}$,*
- *its root is labelled by x_i, and*
- *for each node u of t labeled by some variable x_k the following holds: Let $p_u(\mathbf{x})$ be the product of the labels of u's children. Then p_u is a summand of f_k, i.e. there exists a $\boldsymbol{\iota} \in \mathbb{N}^n$ with $c_{\boldsymbol{\iota}}^{(k)} \neq 0$ and $c_{\boldsymbol{\iota}}^{(k)} \mathbf{x}^{\boldsymbol{\iota}} = p_u(\mathbf{x})$.*

We call a partial derivation tree t a derivation tree *if no leaf of t is labelled by a variable. The* yield $Y(t)$ *of a derivation tree t is the product of the labels of its leaves.*

As in the case of formal languages we have the following

Theorem 5.

1. *The sum of yields of all derivation trees of x_i with height $\leq h$ equals $(\mathbf{f}^h(\mathbf{0}))_i$.*
2. *The sum of yields of all derivation trees of x_i equals $(\mu\mathbf{f})_i$.*

In the following we show that because of commutativity and idempotence already a special class of derivation trees is sufficient to reach $\mu\mathbf{f}$.

Definition 2 (cf. Fig. 5.1). *The* dimension $\dim(t)$ *of a tree t is defined by:*

1. *A tree of height* 0 *or* 1 *has dimension* 0.
2. *Let t be a tree of height $h(t) > 1$ with children $c_1, c_2, \ldots, c_s$ where $\dim(c_1) \geq \dim(c_2) \geq \ldots \dim(c_s)$. Let $d_1 = \dim(c_1)$. If $s > 1$, let $d_2 = \dim(c_2)$, otherwise let $d_2 = 0$. Then we define*

$$\dim(t) := \begin{cases} d_1 + 1 & \text{if } d_1 = d_2 \\ d_1 & \text{if } d_1 > d_2. \end{cases}$$

Note that for a derivation tree t we have $h(t) > \dim(t)$.

Definition 3. *Let t be a derivation tree. We denote with $V(t)$ the number of distinct variables appearing as labels in t. We call t* compact *if $\dim(t) \leq V(t)$.*

In the following, we state two central lemmata that lead to the main result of this section. Lemma 3 tells us that it is sufficient to consider only compact derivation trees. Lemma 4 shows the connection between the dimension of a derivation tree and the Hopkins-Kozen sequence.

Lemma 3. *For each derivation tree t of x_i there is a compact derivation tree t' of x_i with equal yield.*

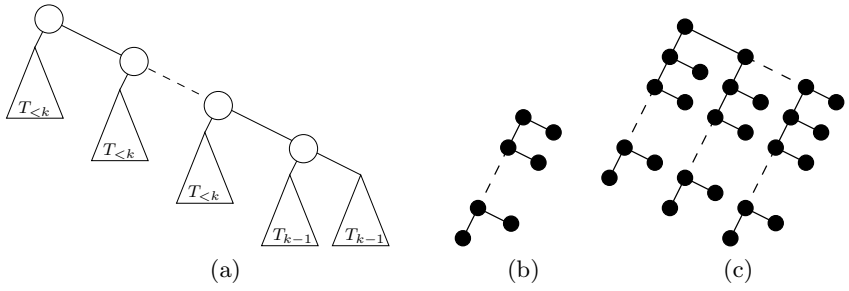

Fig. 1. (a) shows the general structure of a tree of dimension k, where $T_{<k}$ (T_{k-1}) represents any tree of dimension $< k$ ($= k-1$). (b) and (c) give some idea of the topology of one-, resp. two-dimensional trees in general.

Lemma 4. *Let t be a derivation tree of x_i s.t. $\dim(t) \leq k$. Then $Y(t) \leq (\boldsymbol{\kappa}^{(k)})_i$.*[3]

The proof of Lemma 3 bears some similarity to the proof of the pumping lemma for context free languages. Let us call a partial derivation tree a *pumping* tree (p-tree) if it has exactly one leaf which bears the same label as its root and all other leaves are labelled by elements of A. Because of commutativity, reallocating such a p-tree from one subtree of t to another one does not change t's yield. We use a reallocation procedure to inductively reduce the dimension of t's subtrees, which eventually results in decreasing the dimension of t itself.

Theorem 6. *Let $\mathbf{f} : A^n \to A^n$ be a system of power series over an idempotent cc-semiring $\langle A, +, \cdot, 0, 1\rangle$. Then $\mu\mathbf{f} = \boldsymbol{\kappa}^{(n)}$.*

Proof. First recall that by Theorem 3 ($\boldsymbol{\nu}^{(k)} \leq \mu\mathbf{f}$) and Theorem 4 ($\boldsymbol{\kappa}^{(k-1)} \leq \boldsymbol{\nu}^{(k)} \leq \boldsymbol{\kappa}^{(k)}$) we have $\boldsymbol{\kappa}^{(n)} \leq \mu\mathbf{f}$. Obviously, $V(t) \leq n$ for every derivation tree t of x_i. Lemma 3 allows to assume that t is compact, i.e. $\dim(t) \leq V(t) \leq n$. Lemma 4 thus implies $Y(t) \leq (\boldsymbol{\kappa}^{(n)})_i$. Therefore the sum of yields of derivation trees of x_i is less than or equal to $(\boldsymbol{\kappa}^{(n)})_i$. But Theorem 5 tells us that this sum is already $(\mu\mathbf{f})_i$. Hence $\mu\mathbf{f} \leq \boldsymbol{\kappa}^{(n)} \leq \mu\mathbf{f}$. □

Remark 2. The bound of this theorem is tight as can be shown by a generalisation of Example 1: If $\mathbf{f}(\mathbf{x}) = (x_2^2 + a, x_3^2, \ldots, x_n^2, x_1^2)^\top$, then $(\boldsymbol{\kappa}^{(k)})_1 = a$ for $k < n$, but $a^{2^n} \leq (\boldsymbol{\kappa}^{(n)})_1 = (\mu\mathbf{f})_1$.

5.2 Generalisation to Commutative Kleene Algebras

Notation 3. *Let M be any set. Then RExp_M denotes the set of* regular expressions *generated by the elements of M. We write $R_M : \mathsf{RExp}_M \to 2^{M^*}$ for their* canonical interpretation *as languages.*

[3] In fact one can similarly show that $(\boldsymbol{\kappa}^{(k)})_i$ equals exactly the sum of yields of all derivation trees of x_i of dimension less than or equal to k.

For this subsection, let $\mathbf{f}$ denote a system of n *regular expressions* $f_i \in \mathsf{RExp}_{K\cup\mathcal{X}}$. We are again interested in the least solution $\mu\mathbf{f}$ of $\mathbf{x} = \mathbf{f}(\mathbf{x})$, but this time over the *commutative Kleene algebra* $\langle K, +, \cdot, ^*, 0, 1\rangle$. A *commutative Kleene algebra* is an idempotent commutative semiring $\langle K, +, \cdot, 0, 1\rangle$ where the *-operator is only required to satisfy these two equations for all $a, b, c \in K$:

$$1 + aa^* \leq a^* \quad \text{and} \quad a + bc \leq c \to b^*a \leq c.$$

In [5] it is proved that $\mu\mathbf{f}$ can be computed by applying the Hopkins-Kozen operator $\mathcal{H}_\mathbf{f}$ to $\mathbf{f}(\mathbf{0})$ for a finite number of times. In addition, $\mathcal{H}^i_\mathbf{f}(\mathbf{f}(\mathbf{0})) \leq \mu\mathbf{f}$ for all $i \in \mathbb{N}$.

As in the setting of cc-semirings the Hopkins-Kozen operator is defined by $\mathcal{H}_\mathbf{f}(\mathbf{x}) = \mathbf{f}'(\mathbf{x})^*\mathbf{x}$. For $\mathcal{H}$ to be well defined over Kleene algebras, one has to define the partial derivatives $\frac{\partial}{\partial x_j}$ over $\mathsf{Reg}_{K\cup\mathcal{X}}$. This is done in [5] just as in the case of cc-semirings (see the beginning of Section 3), however the equation for the $\sum$-operator is replaced by the axiom $\frac{\partial \alpha^*}{\partial x_j} = \alpha^* \frac{\partial \alpha}{\partial x_j}$ for $\alpha \in \mathsf{RExp}_{K\cup\mathcal{X}}$.

We lift the result of the previous subsection to commutative Kleene algebras, improving the $\mathcal{O}(3^n)$ bound in [5]. More precisely we show that

$$\mathbf{f}(\mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0}))) = \mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0})). \tag{2}$$

In order to prove (2) we appeal to Redko's theorem [1] that essentially states that an equation of terms over any commutative Kleene algebra holds if it holds under the *canonical commutative interpretation*. See [2] for a technical justification of this fact. Let Σ be the finite set of elements of K appearing in $\mathbf{f}$. The canonical commutative interpretation $\mathsf{c}_\Sigma : \mathsf{RExp}_\Sigma \to 2^{\mathbb{N}^\Sigma}$ is then defined by $\mathsf{c}_\Sigma(\alpha) = \{\#w \mid w \in R_\Sigma(\alpha)\}$, where $\#w$ is the Parikh-vector of $w \in \Sigma^*$, i.e. $a \in \Sigma$ appears exactly $(\#w)_a$-times in w. We omit the subscript of c_Σ in the following. The idempotent cc-semiring of sets of Parikh-vectors $\mathcal{C}_\Sigma$ is defined by $\mathcal{C}_\Sigma = \langle 2^{\mathbb{N}^\Sigma}, \cup, +, \emptyset, \{\mathbf{0}\}\rangle$ with $A + B = \{a + b \mid a \in A, b \in B\}$ for all $A, B \subseteq \mathbb{N}^\Sigma$ and $\sum S = \bigcup S$ for all $S \subseteq 2^{\mathbb{N}^\Sigma}$. By Redko's theorem, we can prove (2) by showing $\mathsf{c}(\mathbf{f}(\mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0})))) = \mathsf{c}(\mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0})))$ over $\mathcal{C}_\Sigma$.

For any function $g : \mathsf{RExp}_\Sigma \to \mathsf{RExp}_\Sigma$, let g^c denote the commutative interpretation of g as a map over $\mathcal{C}_\Sigma$, i.e. $\mathsf{c}(g(\alpha)) = g^\mathsf{c}(\mathsf{c}(\alpha))$ for all $\alpha \in \mathsf{RExp}_\Sigma$. In particular $\mathsf{c}(\alpha^*) = \bigcup_{i\in\mathbb{N}} \mathsf{c}(\alpha^i)$. Notice that this definition is consistent with the axiomatic definition of derivatives of *-expressions, since

$$\mathsf{c}(\frac{\partial}{\partial x_i}(\alpha^*)) = \mathsf{c}(\alpha^* \frac{\partial}{\partial x_i}(\alpha)) = \bigcup_{j\in\mathbb{N}} \mathsf{c}(\alpha^j) \frac{\partial}{\partial x_i}(\mathsf{c}(\alpha)) = \frac{\partial}{\partial x_i} \bigcup_{j\in\mathbb{N}} \mathsf{c}(\alpha^j) = \frac{\partial}{\partial x_i}(\mathsf{c}(\alpha^*)).$$

We then have $(\mathcal{H}_\mathbf{f})^\mathsf{c} = \mathcal{H}_{\mathbf{f}^c}$. Furthermore, by Theorem 6, $\mathcal{H}^n_{\mathbf{f}^c}(\mathbf{f}^c(\emptyset))$ solves the equation system $\mathbf{x} = \mathbf{f}^\mathsf{c}(\mathbf{x})$ over $\mathcal{C}_\Sigma$. Combined, we have

$$\mathsf{c}(\mathbf{f}(\mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0})))) = \mathbf{f}^\mathsf{c}((\mathcal{H}^n_\mathbf{f})^\mathsf{c}(\mathbf{f}^\mathsf{c}(\emptyset))) = \mathbf{f}^\mathsf{c}(\mathcal{H}^n_{\mathbf{f}^c}(\mathbf{f}^c(\emptyset))) = \mathcal{H}^n_{\mathbf{f}^c}(\mathbf{f}^c(\emptyset)) = \mathsf{c}(\mathcal{H}^n_\mathbf{f}(\mathbf{f}(\mathbf{0}))).$$

This proves the following theorem.

Theorem 7. *Let* $\mathbf{f} \in \mathsf{RExp}^n_{K\cup\mathcal{X}}$ *define a system* $\mathbf{x} = \mathbf{f}(\mathbf{x})$ *over a commutative Kleene algebra* $\langle K, +, \cdot, ^*, 0, 1\rangle$. *Then* $\mu\mathbf{f} = \boldsymbol{\kappa}^{(n)}$.

6 A Hierarchy of Accelerations

In this section we apply the Hopkins-Kozen acceleration to itself. Let $\mathbf{x} = \mathbf{f}(\mathbf{x})$ be an equation system of degree-2-polynomials over a commutative Kleene algebra. Any polynomial equation system (even with *-expressions) can be reduced to this "Chomsky normal" form by introducing auxiliary variables.

Recall the Hopkins-Kozen operator $\mathcal{H}_{\mathbf{f}}(\mathbf{x}) = \mathbf{f}'(\mathbf{x})^*\mathbf{x}$. As shown in [5] and in the previous section, the sequence $\mathcal{H}^i_{\mathbf{f}}(\mathbf{f}(\mathbf{0}))$ is "faster" than $\mathbf{f}^i(\mathbf{f}(\mathbf{0}))$ to the extent that the fixed point iteration of $\mathcal{H}_{\mathbf{f}}$ reaches $\mu\mathbf{f}$ in a finite number of steps, whereas the fixed point iteration of $\mathbf{f}$ may not reach $\mu\mathbf{f}$. We study in this section how fast accelerations $\mathcal{H}_{\mathcal{H}_{\mathbf{f}}}, \mathcal{H}_{\mathcal{H}_{\mathcal{H}_{\mathbf{f}}}}, \ldots$ are compared to $\mathcal{H}_{\mathbf{f}}$. We write $\mathcal{H}_1$ for $\mathcal{H}_{\mathbf{f}}$ and $\mathcal{H}_{i+1}$ for $\mathcal{H}_{\mathcal{H}_i} = (\frac{\partial}{\partial \mathbf{x}}(\mathcal{H}_i(\mathbf{x})))^*\mathbf{x}$. In the following we mean $\mathcal{H}_{\mathbf{f}}$ when the subscript of $\mathcal{H}$ is omitted. Our hierarchy theorem states that using $\mathcal{H}_i$ once amounts to using $\mathcal{H}$ i-times:

Theorem 8. *For all $i \geq 1 : \mathcal{H}_i(\mathbf{x}) = \mathcal{H}^i(\mathbf{x})$.*

Combined with Theorem 6 we conclude that the least fixed point $\mu\mathbf{f}$ can be computed by (a) iteratively applying $\mathcal{H}$ to $\mathbf{f}(\mathbf{0})$ (n times) or (b) computing the operator $\mathcal{H}^n$ and applying it to $\mathbf{f}(\mathbf{0})$ once or (c) computing the operator $\mathcal{H}_n$ and applying it to $\mathbf{f}(\mathbf{0})$ once. A discussion which method is most appropriate depends on the the particular applications and is beyond the scope of this paper.

Example 2. We continue Example 1 where we have shown that $\mathcal{H}^2(\mathbf{f}(\mathbf{0})) = \mu\mathbf{f}$. Now we illustrate Theorem 8 by showing that $\mathcal{H}_2(\mathbf{f}(\mathbf{0})) = \mu\mathbf{f}$. We have

$$\mathcal{H}(\mathbf{x}) = \mathbf{f}'(\mathbf{x})^*\mathbf{x} = (x_1x_2)^* \begin{pmatrix} x_1 + x_2^2 \\ x_1^2 + x_2 \end{pmatrix} ,$$

$$\mathcal{H}'(\mathbf{x}) = (x_1x_2)^* \begin{pmatrix} 1 + x_2^3 & x_1^2 + x_2 \\ x_2^2 + x_1 & 1 + x_1^3 \end{pmatrix} ,$$

$$\mathcal{H}'(\mathbf{f}(\mathbf{0})) = \begin{pmatrix} 1 & a^2 \\ a & 1 + a^3 \end{pmatrix} \quad \text{and} \quad \mathcal{H}'(\mathbf{f}(\mathbf{0}))^* = (a^3)^* \begin{pmatrix} 1 & a^2 \\ a & 1 \end{pmatrix}.$$

So $\mathcal{H}_2(\mathbf{f}(\mathbf{0})) = \mathcal{H}'(\mathbf{f}(\mathbf{0}))^*\mathbf{f}(\mathbf{0}) = (a^3)^* \begin{pmatrix} a \\ a^2 \end{pmatrix} = \mu\mathbf{f}$.

7 Conclusions

We have studied the Hopkins-Kozen acceleration scheme for solving fixed point equations $\mathbf{x} = \mathbf{f}(\mathbf{x})$ over commutative Kleene algebras [5]. We have shown that, maybe surprisingly, the scheme is tightly related to Newton's method for approximating a zero of a differentiable real function. Loosely speaking, the scheme is the result of generalising Newton's method to commutative ω-continuous semirings in a very straightforward way, and then instantiating this generalisation to the case in which addition is idempotent. In the proof we very much profit from a result by Etessami and Yannakakis on using Newton's method to solve fixed

point equations derived from recursive Markov chains [4]. At the same time, our result extends Etessami and Yannakakis' result to arbitrary commutative ω-continuous semirings, a much more general algebraic setting.

We have also proved that the Hopkins-Kozen scheme terminates after n iterations for a system of n equations, improving on the $O(3^n)$ bound of [5]. As in [5], our bound holds for arbitrary commutative Kleene algebras.

Finally, we have studied the result of applying the scheme to itself, leading to a sequence of faster and faster accelerations. The Hopkins-Kozen scheme can be "arbitrarily faster" than the basis scheme derived from Kleene's theorem (the scheme computing $(\mathbf{f}^k(\mathbf{0}))_{k\geq 0}$) because it is guaranteed to terminate, while Kleene's scheme is not. We have shown that, on the contrary, the reduction in the number of iterations achieved by subsequent accelerations is very moderate: one iteration of the scheme obtained by applying k times the acceleration to itself is already matched by k iterations of the Hopkins-Kozen scheme.

Our work can be extended in several directions. Our proof of the new bound relies on formal languages concepts, and is therefore very non-algebraic. We intend to search for an algebraic proof. We also plan to investigate accelerations for the non-commutative case.

Acknowledgements

We thank Volker Diekert for helpful discussions and the anonymous referees for useful comments.

References

1. J.H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, 1971.
2. J. Esparza, S. Kiefer, and M. Luttenberger. On fixed point equations over commutative semirings. Technical report, 2006.
3. J. Esparza, A. Kučera, and R. Mayr. Model checking probabilistic pushdown automata. In *LICS 2004*. IEEE Computer Society, 2004.
4. K. Etessami and M. Yannakakis. Recursive Markov chains, stochastic grammars, and monotone systems of nonlinear equations. In *STACS*, pages 340–352, 2005.
5. M. W. Hopkins and D. Kozen. Parikh's theorem in commutative Kleene algebra. In *Logic in Computer Science*, pages 394–401, 1999.
6. D. Kozen. On Kleene algebras and closed semirings. In B. Rovan, editor, *Proc. Math. Found. Comput. Sci.*, volume 452 of *Lecture Notes in Computer Science*, pages 26–47, Banska-Bystrica, Slovakia, 1990. Springer-Verlag.
7. W. Kuich. *Handbook of Formal Languages*, volume 1, chapter 9: Semirings and Formal Power Series: Their Relevance to Formal Languages and Automata, pages 609 – 677. Springer, 1997.
8. J.M. Ortega. *Numerical Analysis: A Second Course*. Academic Press, New York, 1972.