On Fixed Point Equations over Commutative Semirings

Javier Esparza   Stefan Kiefer   *Michael Luttenberger*

{esparza,kiefersn,luttenml}@fmi.uni-stuttgart.de

Universität Stuttgart

28. Februar 2007

Outline

In this talk we ...

- study how to compute the *least fixed point* of *polynomials* over certain *semirings* ,

and show that ...

Outline

In this talk we ...

- study how to compute the *least fixed point* of *polynomials* over certain *semirings* ,

and show that ...

1. *Newton's method for approximating the zeros of a function over* $\mathbb{R}$ can be generalized to this setting, and

Outline

In this talk we ...

- study how to compute the *least fixed point* of *polynomials* over certain *semirings* ,

and show that ...

1. *Newton's method for approximating the zeros of a function over* $\mathbb{R}$ can be generalized to this setting, and
2. in the case of *idempotent addition* Newton's method *reaches* the least fixed point after $n + 1$ *steps* ,
    - where n is the number of polynomials,
    - improving the previous $O(3^n)$ upper bound by Hopkins and Kozen, LICS 99.

Definitions

Least fixed point of polynomials over semirings

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1 \rangle$

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1 \rangle$
  - Commutative addition $+$, commutative multiplication $\cdot$, distributivity, ...

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1\rangle$
  - Commutative addition $+$, commutative multiplication $\cdot$, distributivity, ...
  - E.g. $S = \mathbb{R}_{\geq 0}$ with usual operations

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1\rangle$
  - Commutative addition $+$, commutative multiplication $\cdot$, distributivity, ...
  - E.g. $S = 2^{\mathbb{N}^2}$ with

$$\begin{array}{lcl} A + B & := & A \cup B \\ A \cdot B & := & \{a + b \mid a \in A, b \in B\} \\ 0 & := & \emptyset \\ 1 & := & \{(0,0)\} \end{array}$$

Idempotent Addition: $A + A = A$.

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1\rangle$
- Naturally ordered:

$$a \leq b \Leftrightarrow \exists d : a + d = b.$$

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1\rangle$
- Naturally ordered:

$$a \leq b \Leftrightarrow \exists d : a + d = b.$$

  - Over $S = \mathbb{R}_{\geq 0}$: "$\leq = \leq$"

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1 \rangle$
- Naturally ordered:

$$a \leq b \Leftrightarrow \exists d : a + d = b.$$

- Over $S = 2^{\mathbb{N}^2}$: $\leq = \subseteq$.

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1 \rangle$
- Naturally ordered:

$$a \leq b \Leftrightarrow \exists d : a + d = b.$$

- *Countable summation* “as expected”

Definitions

Least fixed point of polynomials over semirings

1. Commutative ω-continuous semiring (short: *ccSR*)

- Commutative semiring $\langle S, +, \cdot, 0, 1\rangle$
- Naturally ordered:

$$a \leq b \Leftrightarrow \exists d : a + d = b.$$

- *Countable summation* "as expected"

$$\sum_{i \in \mathbb{N}} a_i = \sup^{\leq}\{a_1 + \ldots + a_k \mid k \in \mathbb{N}\}$$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$

- Commutative semiring $\langle S, +, \cdot, 0, 1 \rangle$
- Naturally ordered:

$$a \le b \Leftrightarrow \exists d : a + d = b.$$

- *Countable summation* "as expected"

$$\sum_{i \in \mathbb{N}} a_i = \sup^{\le}\{a_1 + \ldots + a_k \mid k \in \mathbb{N}\}$$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$
2. System of polynomials

- Fix n variables $X_1, \ldots, X_n$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$
2. System of polynomials

- Fix n variables $X_1, \ldots, X_n$
- Fix n polynomials $f_1, \ldots, f_n$ in $X_1, \ldots, X_n$,

  e.g.

$$\frac{1}{2}X^2 + \frac{1}{2} \quad \text{or} \quad \{(1,1)\}X^2 + \{(0,0)\}$$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$
2. System of polynomials

- Fix n variables $X_1, \ldots, X_n$
- Fix n polynomials $f_1, \ldots, f_n$ in $X_1, \ldots, X_n$, e.g.

$$\frac{1}{2}X^2 + \frac{1}{2} \quad \text{or} \quad \{(1,1)\}X^2 + \{(0,0)\}$$

- Set:

$$\mathbf{X} = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \text{ and } \mathbf{f}(\mathbf{X}) = \begin{pmatrix} f_1(\mathbf{X}) \\ \vdots \\ f_n(\mathbf{X}) \end{pmatrix}$$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$
2. System of polynomials $\mathbf{f}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}))^\top$

- Fix n variables $X_1, \ldots, X_n$
- Fix n polynomials $f_1, \ldots, f_n$ in $X_1, \ldots, X_n$, e.g.

$$\frac{1}{2}X^2 + \frac{1}{2} \quad \text{or} \quad \{(1,1)\}X^2 + \{(0,0)\}$$

- Set:

$$\mathbf{X} = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \text{ and } \mathbf{f}(\mathbf{X}) = \begin{pmatrix} f_1(\mathbf{X}) \\ \vdots \\ f_n(\mathbf{X}) \end{pmatrix}$$

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1\rangle$
2. System of polynomials $\mathbf{f}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}))^\top$
3. Least fixed point

- Fixed point: any solution of $\mathbf{X} = \mathbf{f}(\mathbf{X})$ over S^n.

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1\rangle$
2. System of polynomials $\mathbf{f}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}))^\top$
3. Least fixed point

- Fixed point: any solution of $\mathbf{X} = \mathbf{f}(\mathbf{X})$ over S^n.
- Existence guaranteed by *Kleene's fixed point theorem* :

Theorem (cf. Kuich, 1987)

For every system $\mathbf{f}$ *of polynomials over some ccSR the supremum of*

$$\mathbf{0}, \mathbf{f}(\mathbf{0}), \mathbf{f}^2(\mathbf{0}), \mathbf{f}^3(\mathbf{0}), \ldots$$

is the least fixed point $\mu\mathbf{f}$ *of* $\mathbf{f}$.

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1\rangle$
2. System of polynomials $\mathbf{f}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}))^\top$
3. Least fixed point $\mu\mathbf{f} = \sup\{\mathbf{f}^k(\mathbf{0}) \mid k \in \mathbb{N}\}$

- Fixed point: any solution of $\mathbf{X} = \mathbf{f}(\mathbf{X})$ over S^n.
- Existence guaranteed by *Kleene's fixed point theorem* :

Theorem (cf. Kuich, 1987)

For every system $\mathbf{f}$ *of polynomials over some ccSR the supremum of*

$$\mathbf{0}, \mathbf{f}(\mathbf{0}), \mathbf{f}^2(\mathbf{0}), \mathbf{f}^3(\mathbf{0}), \ldots$$

is the least fixed point $\mu\mathbf{f}$ *of* $\mathbf{f}$.

Definitions

Least fixed point of polynomials over semirings

1. ccSR $\langle S, +, \cdot, 0, 1 \rangle$
2. System of polynomials $\mathbf{f}(\mathbf{X}) = (f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}))^\top$
3. Least fixed point $\mu\mathbf{f} = \sup\{\mathbf{f}^k(\mathbf{0}) \mid k \in \mathbb{N}\}$

Two questions:

- Why is this framework interesting?
- How fast does the Kleene sequence converge to $\mu\mathbf{f}$?

Example: probabilistic recursive programs

- Consider the *procedure* X given by

$$X \stackrel{1/2}{\to} XX, \quad X \stackrel{1/2}{\to} \lambda.$$

- Probability that X *finally* terminates is the least solution of:

$$X = \frac{1}{2}X^2 + \frac{1}{2} =: f(X)$$

as shown by Etessami and Yannakakis at STACS 05.

  - Termination probabilities needed for further analysis.

Example: probabilistic recursive programs

- Consider the *procedure* X given by

$$X \stackrel{1/2}{\to} XX, \quad X \stackrel{1/2}{\to} \lambda.$$

- Probability that X *finally* terminates is the least solution of:

$$X = \frac{1}{2}X^2 + \frac{1}{2} =: f(X)$$

  as shown by Etessami and Yannakakis at STACS 05.

  - Termination probabilities needed for further analysis.

- *Kleene sequence* : $0, \quad 0.5, \quad 0.625, \quad 0.6953125, \ldots \to 1.$
- It can be shown: *only k bits of accuracy after 2^k steps* !

Example: Parikh image

- Consider

$$G : X \to aXXb, \quad X \to \lambda.$$

- Parikh image of $L(G)$

$$\{(\#_a w, \#_b w) \in \mathbb{N} \mid w \in L(G)\}$$

- This is the least fixed point of

$$f(X) = \{(1,1)\}X^2 + \{(0,0)\}$$

over $2^{\mathbb{N}^2}$.

Example: Parikh image

- Consider

$$G : X \to aXXb, \quad X \to \lambda.$$

- Parikh image of $L(G)$

$$\{(\#_a w, \#_b w) \in \mathbb{N} \mid w \in L(G)\}$$

- This is the least fixed point of

$$f(X) = \{(1,1)\}X^2 + \{(0,0)\}$$

  over $2^{\mathbb{N}^2}$.

- Kleene sequence: $f^k(\emptyset) = \{(i,i) \mid i \leq k\}$
- As $\mu f = \{(i,i) \mid i \in \mathbb{N}\}$ the Kleene sequence gives only a finite approximation!

Q: Is there a better way to approximate or even solve $\mathbf{X} = \mathbf{f}(\mathbf{X})$?

Q: Is there a better way to approximate or even solve $\mathbf{X} = \mathbf{f}(\mathbf{X})$?

A: Over the real numbers we can apply Newton's method to approximate the zeros of

$$\mathbf{g}(\mathbf{X}) = \mathbf{f}(\mathbf{X}) - \mathbf{X}.$$

- It many cases Newton's method *doubles* the number of correct bits in every step!

Q: Is there a better way to approximate or even solve $\mathbf{X} = \mathbf{f}(\mathbf{X})$?

A: Over the real numbers we can apply Newton's method to approximate the zeros of

$$\mathbf{g}(\mathbf{X}) = \mathbf{f}(\mathbf{X}) - \mathbf{X}.$$

- It many cases Newton's method *doubles* the number of correct bits in every step!

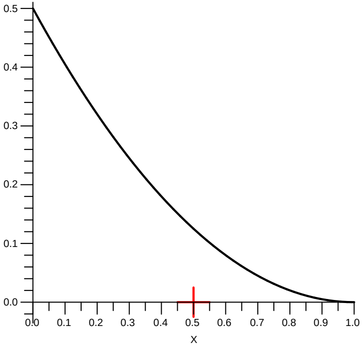
- In the next slides we
  - recall Newton's method, and
  - generalize it to ccSRs.

Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \rightarrow \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

1. Evaluate $g(\nu^{(k)})$.
2. Determine the tangent t in $g(\nu^{(k)})$.
3. Set $\nu^{(k+1)}$ to the zero of t.

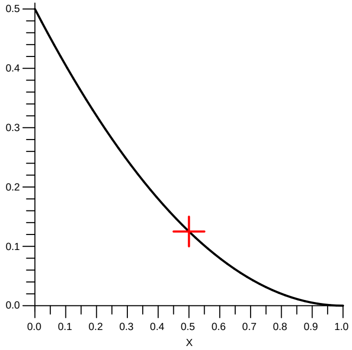


Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

1. Evaluate $g(\nu^{(k)})$.
2. Determine the tangent t in $g(\nu^{(k)})$.
3. Set $\nu^{(k+1)}$ to the zero of t.

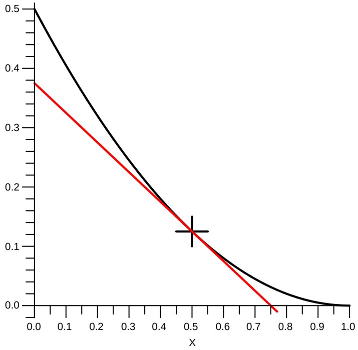


Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

1. Evaluate $g(\nu^{(k)})$.
2. Determine the tangent t in $g(\nu^{(k)})$.
3. Set $\nu^{(k+1)}$ to the zero of t.

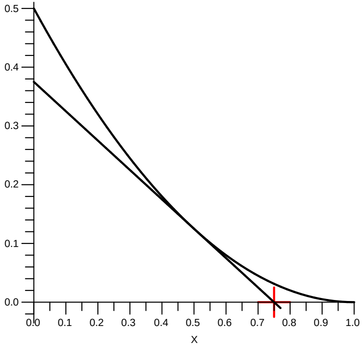


Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

1. Evaluate $g(\nu^{(k)})$.
2. Determine the tangent t in $g(\nu^{(k)})$.
3. Set $\nu^{(k+1)}$ to the zero of t.

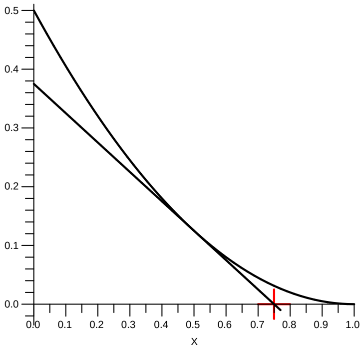


Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

$$\nu^{(k+1)} = \nu^{(k)} - g'(\nu^{(k)})^{-1} g(\nu^{(k)}).$$



Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)

Given a starting point $\nu^{(0)}$ repeat:

$$\nu^{(k+1)} = \nu^{(k)} - g'(\nu^{(k)})^{-1} g(\nu^{(k)}).$$

In our case

$$g(X) = f(X) - X$$

we have

$$g'(X) = f'(X) - 1$$

so that

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)}).$$

Recap on Newton's method

Definition (Newton's method for approximating the zeros of $g : \mathbb{R} \to \mathbb{R}$)
Given a starting point $\nu^{(0)}$ repeat:

$$\nu^{(k+1)} = \nu^{(k)} - g'(\nu^{(k)})^{-1} g(\nu^{(k)}).$$

In our example

$$g(X) = f(X) - X = \frac{1}{2}X^2 + \frac{1}{2} - X$$

starting from $\nu^{(0)} = 0$ we get:

$$0, \frac{1}{2}, \frac{3}{4}, \ldots, 1 - 2^{-k}$$

giving us *k bits after k steps* instead of k bits after 2^k!

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Problem : In an arbitrary ccSR

1. neither the derivative $f'(X)$,
2. nor the inverse of $1 - f'(\nu^{(k)})$,
3. nor the difference $f(\nu^{(k)}) - \nu^{(k)}$

are defined.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Problem : In an arbitrary ccSR

1. neither the derivative $f'(X)$,
2. nor the inverse of $1 - f'(\nu^{(k)})$,
3. nor the difference $f(\nu^{(k)}) - \nu^{(k)}$

are defined.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Problem : In an arbitrary ccSR

1. neither the derivative $f'(X)$,
2. nor the inverse of $1 - f'(\nu^{(k)})$,
3. nor the difference $f(\nu^{(k)}) - \nu^{(k)}$

are defined.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the derivative f'?

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the derivative f'?

A: Standard solution, take the *algebraic definition* , e.g.

$$\frac{\partial pq}{\partial X} = \frac{\partial p}{\partial X} q + p \frac{\partial q}{\partial X}, \quad \frac{\partial p + q}{\partial X} = \frac{\partial p}{\partial X} + \frac{\partial q}{\partial X}, \quad \frac{\partial X}{\partial X} = 1, \ldots$$

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the inverse of $1 - f'(\nu^{(k)})$?

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + (1 - f'(\nu^{(k)}))^{-1}(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the inverse of $1 - f'(\nu^{(k)})$?

- Recall the *geometric series*

$$(1-q)^{-1} = \sum_{k \in \mathbb{N}} q^k \text{ for } |q| < 1.$$

- In a ccSR

$$f'(\nu^{(k)})^* := \sum_{j \in \mathbb{N}} f'(\nu^{(k)})^j$$

  always exists.

A: Replace $(1 - f'(\nu^{(k)}))^{-1}$ by $f'(\nu^{(k)})^*$.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^*(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the inverse of $1 - f'(\nu^{(k)})$?

- Recall the *geometric series*

$$(1-q)^{-1} = \sum_{k \in \mathbb{N}} q^k \text{ for } |q| < 1.$$

- In a ccSR

$$f'(\nu^{(k)})^* := \sum_{j \in \mathbb{N}} f'(\nu^{(k)})^j$$

  always exists.

A: Replace $(1 - f'(\nu^{(k)}))^{-1}$ by $f'(\nu^{(k)})^*$.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^*(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the difference $f(\nu^{(k)}) - \nu^{(k)}$?

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^*(f(\nu^{(k)}) - \nu^{(k)})$$

Q: How to define the difference $f(\nu^{(k)}) - \nu^{(k)}$?

- We can show $\nu^{(k)} \leq f(\nu^{(k)})$ when starting from $\nu^{(0)} = 0$.
- By def. we find $\delta^{(k)}$ with $\nu^{(k)} + \delta^{(k)} = f(\nu^{(k)})$!

A: Replace $f(\nu^{(k)}) - \nu^{(k)}$ by *any* such $\delta^{(k)}$.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^{*}\delta^{(k)} \text{ with } \nu^{(0)} = 0$$

Q: How to define the difference $f(\nu^{(k)}) - \nu^{(k)}$?

- We can show $\nu^{(k)} \leq f(\nu^{(k)})$ when starting from $\nu^{(0)} = 0$.
- By def. we find $\delta^{(k)}$ with $\nu^{(k)} + \delta^{(k)} = f(\nu^{(k)})$!

A: Replace $f(\nu^{(k)}) - \nu^{(k)}$ by *any* such $\delta^{(k)}$.

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^{*}\delta^{(k)} \text{ with } \nu^{(0)} = 0$$

Q: And in the multivariate case?

Generalizing Newton's Method

For simplicity, consider Newton's method for the univariate case $g(X) = f(X) - X$:

$$\nu^{(k+1)} = \nu^{(k)} + f'(\nu^{(k)})^* \delta^{(k)} \text{ with } \nu^{(0)} = 0$$

Q: And in the multivariate case?

A: Replace X by $\mathbf{X}$, f by $\mathbf{f}$, and f' by

$$\mathbf{f}' = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial X_n} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix}$$

Newton's Method

Definition

For any system $\mathbf{f}(\mathbf{X})$ of n polynomials in n variables over any ccSR the *Newton sequence* is defined by

$$\begin{array}{rcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \delta^{(k)} \end{array}$$

where $\delta^{(k)}$ is *any* sequence satisfying $\nu^{(k)} + \delta^{(k)} = \mathbf{f}(\nu^{(k)})$.

Newton's Method

Definition

For any system $\mathbf{f}(\mathbf{X})$ of n polynomials in n variables over any ccSR the *Newton sequence* is defined by

$$\begin{array}{rcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \delta^{(k)} \end{array}$$

where $\delta^{(k)}$ is *any* sequence satisfying $\nu^{(k)} + \delta^{(k)} = \mathbf{f}(\nu^{(k)})$.

Theorem

For any system $\mathbf{f}(\mathbf{X})$ of n polynomials in n variables over any ccSR we have

$$\mathbf{f}^k(\mathbf{0}) \leq \nu^{(k)} \leq \nu^{(k+1)} \leq \mu\mathbf{f},$$

i.e. the Newton sequence converges monotonically to $\mu\mathbf{f}$.

Examples

Newton's sequence:

$$\begin{array}{rcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \delta^{(k)} \end{array}$$

- When applied to
$$f(X) = \frac{1}{2}X^2 + \frac{1}{2}$$
we end up with the *traditional Newton's method* applied to
$$f(X) - X.$$
- Obvious, that's how we defined it.

Examples

Newton's sequence:

$$\begin{array}{lcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \delta^{(k)} \end{array}$$

- Parikh image:

$$f(X) = \{(1,1)\}X^2 + \{(0,0)\}$$

- Because of *idempotent* addition (union) and $\nu^{(k)} \leq f(\nu^{(k)})$:

$$\delta^{(k)} = f(\nu^{(k)})$$

Examples

Newton's sequence:

$$\begin{array}{rcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \delta^{(k)} \end{array}$$

- Parikh image:

$$f(X) = \{(1,1)\}X^2 + \{(0,0)\}$$

- Because of *idempotent* addition (union) and $\nu^{(k)} \leq f(\nu^{(k)})$:

$$\delta^{(k)} = f(\nu^{(k)})$$

- With $f'(X) = \{(1,1)\}X$:

$$\nu^{(0)} = \emptyset, \quad \nu^{(1)} = \{(0,0)\}, \quad \nu^{(2)} = \{(i,i) \mid i \in \mathbb{N}\} = \mu f.$$

- Newton converges after two steps!

Newton's Method for Idempotent Addition

Theorem

For any system $\mathbf{f}(\mathbf{X})$ *of* n *polynomials in* n *variables over any* idempotent *ccSR the* Newton sequence *defined by*

$$\begin{aligned} \nu^{(0)} &= \mathbf{0} \\ \nu^{(k+1)} &= \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^{*}\mathbf{f}(\nu^{(k)}) \end{aligned}$$

reaches $\mu\mathbf{f}$ after $n+1$ steps , *i.e.*

$$\mathbf{f}(\nu^{(n+1)}) = \nu^{(n+1)}.$$

Remarks on the Idempotent Case

$$\begin{aligned}\nu^{(0)} &= \mathbf{0} \\ \nu^{(k+1)} &= \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \mathbf{f}(\nu^{(k)})\end{aligned}$$

- Starting from $\nu^{(0)} = \mathbf{f}(\mathbf{0})$ you may write the sequence as

$$\nu^{(k+1)} = \mathbf{f}'(\nu^{(k)})^* \nu^{(k)}$$

- But this is *exactly* the sequence proposed by Hopkins and Kozen, LICS 99.

Remarks on the Idempotent Case

$$\begin{array}{rcl} \nu^{(0)} & = & \mathbf{0} \\ \nu^{(k+1)} & = & \nu^{(k)} + \mathbf{f}'(\nu^{(k)})^* \mathbf{f}(\nu^{(k)}) \end{array}$$

- Starting from $\nu^{(0)} = \mathbf{f}(\mathbf{0})$ you may write the sequence as

$$\nu^{(k+1)} = \mathbf{f}'(\nu^{(k)})^* \nu^{(k)}$$

- But this is *exactly* the sequence proposed by Hopkins and Kozen, LICS 99.
- Our result therefore
  - identifies Hopkins and Kozen's sequence as the Newton sequence, and
  - improves their $O(3^n)$ upper bound on the number of steps needed to reach $\mu\mathbf{f}$ to $n+1$.

In the paper:

- Newton's method also works for systems of *power series* .
- Our result on *idempotent* ccSRs can be lifted to the more general setting of *commutative Kleene Algebras* .
- Study the effect of applying Newton's method to itself.

The End

Thank you for your attention.