Title	Iteration Lemmata for Normed Semirings (Algebraic Systems, Formal Languages and Computations)
Author(s)	Kudlek, Manfred
Citation	数理解析研究所講究録 (2000), 1166: 131-137
Issue Date	2000-08
URL	http://hdl.handle.net/2433/64347
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
1166 巻 2000 年 131-137

Iteration Lemmata for Normed Semirings

Manfred Kudlek
Fachbereich Informatik, Universität Hamburg
email : kudlek@informatik.uni-hamburg.de

Abstract

In this article abstract iteration lemmata for algebraic, linear and rational languages defined by least fixed point solutions of corresponding systems of equations are presented. For this a norm on the underlying semiring has to be defined. A preliminary version was given in [2], an application on process algebras in [3].

Let $\mathcal{M} = (\mathbf{A}, \circ, \mathbf{1})$ be a monoid with binary operation $\circ : \mathbf{A} \times \mathbf{A} \rightarrow \mathbf{A}$ and unit element $\mathbf{1}$, i.e. $\mathbf{1} \circ \alpha = \alpha \circ \mathbf{1} = \alpha$.

$\mathcal{M}$ will be written instead of $\mathbf{A}$, and sometimes let the operation $\circ$ return (finite) subsets of $\mathcal{M}$, i.e. $\circ : \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{P}(\mathcal{M})$ where $\mathcal{P}(\mathcal{M})$ is the powerset of $\mathcal{M}$.

Extend $\circ$ to an associative binary operation $\circ : \mathcal{P}(\mathcal{M}) \times \mathcal{P}(\mathcal{M}) \rightarrow \mathcal{P}(\mathcal{M})$, being distributive with union $\cup$ ($A \circ (B \cup C) = (A \circ B) \cup (A \circ C)$ and $(A \cup B) \circ C = (A \circ B) \cup (B \circ C)$), with unit element $\{\mathbf{1}\}$ ($\{\mathbf{1}\} \circ A = A \circ \{\mathbf{1}\} = A$), and zero element $\emptyset$ ($\emptyset \circ A = A \circ \emptyset = \emptyset$).

Then $\mathcal{S} = (\mathcal{P}(\mathcal{M}), \cup, \circ, \emptyset, \{\mathbf{1}\})$ is an ω-complete semiring, i.e. if $A_i \subseteq A_{i+1}$ for $0 \leq i$ then $B \circ \bigcup_{i \geq 0} A_i = \bigcup_{i \geq 0} (B \circ A_i)$ and $(\bigcup_{i \geq 0} A_i) \circ B = \bigcup_{i \geq 0} (A_i \circ B)$.

Define also $A^0 = \{\mathbf{1}\}$, $A^1 = A, A^{k+1} = A \circ A^k$, $A^\circ = \bigcup_{k \geq 0} A^k$.

Let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be a set of variables such that $\mathcal{X} \cap \mathcal{M} = \emptyset$.

A *monomial* over $\mathcal{S}$ with variables in $\mathcal{X}$ is a finite string of the form : $A_1 \circ A_2 \circ \ldots \circ A_k$, where $A_i \in \mathcal{X}$ or $A_i \subseteq \mathcal{M}, |A_i| < \infty, i = 1, \ldots, k$. Without loss of generality, $A_i = \{\alpha_i\}$ with $\alpha_i \in \mathcal{M}$ suffices. The α_{ij} (or $\{\alpha_{ij}\}$) will be called *constants*. A *polynomial* $p(\underline{X})$ over $\mathcal{S}$ is a finite union of monomials where $\underline{X} = (X_1, \cdots, X_n)$.

In the following the symbol $\bigcirc$ will be used to denote finite products with operation $\circ$:

$$\bigcirc_{i=1}^{m} A_i = A_1 \circ \cdots \circ A_m$$

and the symbol $\bigcup$ to denote finite unions :

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n \ .$$

A *system of equations* over $\mathcal{S}$ is a finite set of equations :

$\mathcal{E} := \{X_i = p_i(\underline{X}) \mid i = 1,\ldots,n\}$, where $p_i(\underline{X})$ are polynomials. This will also be denoted by $\underline{X} = \underline{p}(\underline{X})$.

The *solution* of $\mathcal{E}$ is an n-tuple $\underline{L} = (L_1,\ldots,L_n) \in \mathcal{P}(\mathcal{M})^n$ of subsets of $\mathcal{M}$, with $L_i = p_i(L_1,\ldots,L_n)$ and the n-tuple is minimal with this property, i.e. if $\underline{L'} = (L'_1,\ldots,L'_n)$ is another n-tuple satisfying $\mathcal{E}$, then $\underline{L} \leq \underline{L'}$ (where the order is defined componentwise with respect to inclusion, i.e. $\underline{A} = (A_1,\cdots,A_n) \leq (B_1,\cdots,B_n) = \underline{B} \Leftrightarrow \forall_{i=1}^n : A_i \subseteq B_i$).

It follows from the theory of semirings that any system of equations over $\mathcal{S}$ has a unique solution, and this is the least fixed point starting with

$\underline{X}^{(0)} = (X_1^{(0)},\cdots,X_n^{(0)}) = (\emptyset,\cdots,\emptyset) = \underline{\emptyset}$, and $\underline{X}^{(t+1)} = \underline{p}(\underline{X}^{(t)})$

Then the following fact holds : $\underline{X}^{(t)} \leq \underline{X}^{(t+1)}$ for $0 \leq t$.

This is seen by induction and the property of the polynomial with respect to inclusion, as $\underline{\emptyset} \leq \underline{X}^{(1)}$ and $\underline{X}^{(t+1)} = \underline{p}(\underline{X}^{(t)}) \leq \underline{p}(\underline{X}^{(t+1)}) = \underline{X}^{(t+2)}$.

For the theory of semirings see [1, 4].

A general system of equations is called *algebraic*. It is called *linear* if all monomials are of the form $A \circ X \circ B$ or A, and *rational* if they are either of the form $X \circ A$ or A, or of the form $A \circ X$ or A, with $A \subseteq M$ and $B \subseteq M$. Corresponding families of languages (solutions of such systems of equations) are denoted by $ALG(\circ)$, $LIN(\circ)$, and $RAT(\circ)$. In the case $\circ$ is commutative then all families are identical : $\underline{ALG(\circ) = LIN(\circ) = RAT(\circ)}$.

Note that the algebraic case corresponds to context-free languages if $\circ$ is usual catenation.

Grammars

Interpreting an equation $X_i = p_i(\underline{X})$ as a set of rewriting productions $X_i \rightarrow m_{ij}$ with $m_{ij} \in M(X_i)$ where $M(X_i)$ denotes the set of monomials of $p_i(\underline{X})$, *regular*, *linear*, and *context-free* grammars $G_i = (\mathcal{X},\mathcal{C},X_i,P)$ using the operation $\circ$, can be defined. Here $\mathcal{C}$ stands for the set of all constants in the system of equations, and P for all productions defined as above. As the productions are *context-free*, (*terminal*) derivation trees can also be defined. Note that the interior nodes of trees are labelled by variables, and the leafs by constants from $\mathcal{C}$.

Normal Forms

In the following lemma forests of terminal trees are constructed to represent approximations of the least fixed point, and it is shown that the sets of terminal derivation trees with respect to $\circ$ are equivalent with the latter.

Lemma 1 : *(Approximation of the least fixed point)*

Terminal trees for the approximation of the least fixed point and terminal derivation trees are *equivalent.*

Proof:

$\underline{X}^{(0)} = \underline{\emptyset}$, $\underline{X}^{(t+1)} = \underline{p}(\underline{X}^{(t)})$

Thus

$$X_i^{(t+1)} = \bigcup_j \bigcirc_k X_{ijk}^{(t)} \cup \bigcup_j \{\alpha_{ij}\}$$

in particular

$$X_i^{(0)} = \emptyset \ , \ X_i^{(1)} = \bigcup_j \{\alpha_{ij}\}$$

Construct forests $\mathcal{T}$ of terminal trees as follows :

$\mathcal{T}^{(1)}$ consists of all trees with roots $X_i^{(1)}$ and children (only leafs) $\{\alpha_{ij}\}$ $(1 \leq i \leq n)$.

$\mathcal{T}^{(t+1)}$ is constructed from trees in $\mathcal{T}^{(1)}$ as the set of trees with roots $X_i^{(t+1)}$ and their children either $X_{ijk}^{(t)}$ being roots of trees from $\mathcal{T}^{(t)}$ or $\{\alpha_{ij}\}$.

Thus the set of frontiers of leafs of all trees in $\mathcal{T}^{(t)}$ with root $X_i^{(t)}$ is just the approximation $X_i^{(t)}$.

On the other hand, any terminal derivation tree for X_i is contained in $\mathcal{T}$. For this, interprete a deepest non-terminal vertex (i.e. with greatest distance from the root) as $X_j^{(1)}$ for some j, and the root as $X_i^{(t+1)}$ for some i. Then all non-terminal vertices get some step number s with $1 \leq s \leq t+1$.

□

Lemma 2 :

Any linear system of equations can be transformed, with additional variables, into another one where all monomials are of the form $X \circ \alpha$, $\alpha \circ X$, or α, and the new system has identical minimal solutions in the old variables.

Proof : Consider any monomial $\alpha \circ X \circ \beta$. Replace it by $\alpha \circ Y$, and add a new equation $Y = X \circ \beta$. Then it is obvious that the new system has identical solutions in the old variables.

□

In the following it will be shown that any algebraic system of equations can be transformed, with additional variables, into a system of equations where all monomials have the form $X \circ Y$ or $\{\alpha\}$, and the new system has identical minimal solutions for the old variables. To prove this some lemmata have to be shown first. To this end, the following is to be assumed about ω-complete semirings :

Postulate Δ

Let $\mathcal{S} = (\mathcal{P}(\mathcal{M}), \emptyset, \mathbf{1}, \cup, \circ)$ be an ω-complete semiring where $\mathcal{M}$ is a monoid. $\mathcal{S}$ has property (Δ), if $\mathbf{1} \in A \circ B \Leftrightarrow (\mathbf{1} \in A \wedge \mathbf{1} \in B)$.

This property states some kind of *nondivisibility* of the unit.

Lemma 3 :

If (Δ) holds then

$$\mathbf{1} \in \bigcirc_{i=1}^{k} A_i \ \Leftrightarrow \ \overset{k}{\underset{i=1}{\forall}} : \mathbf{1} \in A_i$$

Proof : $\Leftarrow$ is trivial.

$\Rightarrow$: $\forall_{i=1}^{k} : \mathbf{1} \in A_i$ implies $1 \in A_1 \wedge \forall_{i=2}^{k} : \mathbf{1} \in A_i$ by property (Δ), and then induction.

□

For each variable $X \in \mathcal{X}$ in an algebraic system of equations let $M(X)$ denote the set of monomials of X, i.e. $X = \bigcup_{m \in M(X)} m$.

Lemma 4 : (*Separation of variables and constants*)

For any algebraic system of equations there exists another one, possibly with additional variables, having the same (partial) solution in the original variables, for which the following property holds :

if $X_i = \bigcirc_{j=1}^{r(i)} m_{ij}$ then each monomial is either of the form $\bigcirc_{k=1}^{s(ij)} X_{ijk}$ or $\{\alpha_{ij}\}$ (a constant).

Proof : If m_{ij} is not of that form and not a constant then $m_{ij} = \bigcirc_{k=1}^{s(ij)} A_{ijk}$ with A_{ijk} either a variable or a constant β_{ijk}. Replace each constant β_{ijk} in it by a new variable Y_{ijk}, and add a new equation $Y_{ijk} = \{\beta_{ijk}\}$.

Trivially, the new system of equations has the same solution in the original variables.

□

Lemma 5 : (*Removal of* $\{1\}$)

For each algebraic system of equations there exists another one with the same set of variables, with no monomial being 1 and with solutions $L_i - \{1\}$, if L_i are the solutions of the old system.

Proof :

Let $\mathcal{Y}$ be a set of variables and $\mathcal{F}(\mathcal{Y})$ the set of all (formal) terms on $\mathcal{Y}$ with operation $\circ$. Define inductively

$\mathcal{Y}_1 = \{X \in \mathcal{X} \mid 1 \in M(X)\}$, $\mathcal{Y}_{i+1} = \mathcal{Y}_i \cup \{X \in \mathcal{X} \mid \exists m \in \mathcal{F}(\mathcal{Y}_i) : m \in M(X)\}$

Note that all monomials m consist only of variables.

Trivially $\mathcal{Y}_i \subseteq \mathcal{Y}_{i+1}$, and therefore there exists k with $\mathcal{Y}_k = \mathcal{Y}_{k+j} = \mathcal{Y}$ for all $0 \leq j$ since $\mathcal{X}$ is finite.

The following fact holds :

$\{1\} \subseteq X \Leftrightarrow X \in \mathcal{Y}$.

$\Leftarrow$) If $X \in \mathcal{Y}$ then $1 \in X$ is seen by induction. Trivially, if $X \in \mathcal{Y}_1$ then $1 \in M(X)$ and therefore $1 \in X$. Assume $1 \in X$ for all $X \in \mathcal{Y}_j$ for $1 \leq j$. If $X \in \mathcal{Y}_{j+1}$ then by definition there exists a monomial $m \in \mathcal{F}(\mathcal{Y}_j)$ such that $m \in M(X)$. Therefore $1 \in X$.

$\Rightarrow$) Let $X = X_i$. $1 \in X_i$ implies $\{1\} \subseteq X_i^{(t)}$ for some $t \geq 1$. Let t be minimal, i.e. $1 \notin X_i^s$ for $s < t$. If $t = 1$ then $1 \in M(X_i)$ and therefore $X_i \in \mathcal{Y}_1 \subseteq \mathcal{Y}$.

Let $t > 1$. If $1 \in M(X_i)$ then again $X_i \in \mathcal{Y}_1 \subseteq \mathcal{Y}$. By assumption for t $1 \notin M(X_i)$. Then $\{1\} \subseteq Y_1^{(t-1)} \circ \cdots \circ Y_r^{(t-1)} = m_1 \in M(X_i)$. Property (Δ) implies $\{1\} \subseteq Y_j^{(t-1)}$ for $1 \leq j \leq r$. Put Y_j into the set $\mathcal{Z}$ if $1 \in M(Y_j)$, and repeat the procedure for all remaining $Y_j^{(t-1)}$ with $1 \notin M(Y_j)$. The procedure must terminate for some $Y_k^{(1)}$ for which $1 \in M(Y_k)$, yielding a set of variables $\mathcal{Z}$ with $1 \in M(Y)$ for $Y \in \mathcal{Z}$. Therefore $\mathcal{Z} \subseteq \mathcal{Y}$. By the construction there exists an $m \in M(X_i)$ with $m \in \mathcal{F}(\mathcal{Z}) \subseteq \mathcal{F}(\mathcal{Y})$. Obviously, $X_i \in \mathcal{Y}$.

Now, construct a new system of equations $\mathcal{E}'$ in which in all monomials m_{ij}, possibly some variables $Y_j \in \mathcal{Y}$ are deleted, such that the new monomials $m'_{ij} \neq \{1\}$.

Then the system $\mathcal{E}'$ has the solutions $L_i - \{1\}$.

□

Lemma 6 :

For each algebraic system of equations there exists another one with additional variables X'_i for each old X_i such that the monomials in $p'_i(\underline{X, X'})$ are either of the form $\{1\}$

or don't contain X'_j where $p'_i(\underline{X}, \underline{X'})$ means $p'_i(\underline{X}, \underline{X'})$. The solutions of the new system for the new variables X'_i are $L'_i = L_i$.

Proof :

By Lemma 5 let $\mathcal{E}'$ be a system of equations with $L'_i = L_i - \{\mathbf{1}\}$.

Construct a new system $\mathcal{E}''$ in which for each variable X_i a new one X'_i is defined. Let $p_i(\underline{X}, \underline{X'}) = p_i(\underline{X})$ for X_i and define $p'_i(\underline{X}, \underline{X'}) = \{\mathbf{1}\} + p_i(\underline{X})$ if $\mathbf{1} \in L_i$, and in case $\mathbf{1} \notin L_i$ $p'_i(\underline{X}, \underline{X'}) = p_i(\underline{X})$. Then the solutions for the new variables are $L'_i = L_i$.

□

Lemma 7 : (*Removal of monomials of the form* Y)

For each algebraic system of equations there exists another one with the same variables such that no monomial is of the form Y and with solution identical to the old one.

Proof :

Assume that the system is already in the form stated in lemmata 4, 5, and 6.

Construct inductively sets of variables for $X \in \mathcal{X}$:

$\mathcal{Y}_1(X) = \{X\}$

$\mathcal{Y}_{j+1}(X) = \mathcal{Y}_j(X) \cup \{Y \in \mathcal{X} \mid \exists Z \in \mathcal{Y}_j(X) : Y \in M(X)\}$

Since $\mathcal{X}$ is finite there exists a k with $\mathcal{Y}_k(X) = \mathcal{Y}_{k+j}(X) = \mathcal{Y}(X)$ for $j \geq 0$.

Obviously, the following fact holds : $Y \subseteq X \Leftrightarrow Y \in \mathcal{Y}(X)$.

Now construct the new system by taking all monomials which are constants and consider all monomials $m = Y_1 \circ \cdots \circ Y_k \in M(X)$ with $k \geq 2$. Construct the new monomials $m' = Z_i \circ \cdots \circ Z_k \in M(Y)$ with $X \in \mathcal{Y}(Y)$ and $Z_j \in \mathcal{Y}(Y_j)$.

Then $L'_i = L_i$.

□

Lemma 8 : (*Normal form*)

For each algebraic system there exists another one with additional variables such that either all monomials are $\mathbf{1} \in M(X)$ (then no other monomial contains X), or $Y \circ Z$, or $\{\alpha\}$ with $\alpha \neq \mathbf{1}$ and the solutions for the old variables are identical.

Proof :

Assume that the system of equations has the form stated in the previous lemmata.

Consider an arbitrary monomial $m = Y_1 \circ \cdots \circ Y_k \in M(X)$ with $k \geq 2$. Replace it by $Y_1 \circ Z_1 \in M(X)$ and the new equations $Z_1 = Y_2 \circ Z_2, \cdots, Z_{k-2} = Y_{k-1} \circ Y_k$.

Then the new system of equations obviously has the same solutions in the old variables.

□

In the following a notion of norm is introduced to state the abstract iteration lemmata.

Define a *norm* in $\mathcal{M} = (\mathbf{A}, \circ, \mathbf{1})$ to be a function $\| \| : \mathbf{A} \rightarrow \mathbf{N}_\infty$ (where $\mathbf{N}_\infty$ denotes the set of all natural numbers including 0 and the symbol of infinity ∞) with the following properties: $\|x\|, \|y\| \leq \|x \circ y\| \leq \|x\| + \|y\|$, $\|\mathbf{1}\| = 0$ and for $x \neq \mathbf{1} \neq y$ let the first inequality ($\leq$) be strict ($<$).

In the case that $\circ$ returns a finite subset the following properties should hold : $\|x\|, \|y\| \leq min\{\|z\| \mid z \in x \circ y\} \leq max\{\|z\| \mid z \in x \circ y\} \leq \|x\| + \|y\|$, and for $x \neq \mathbf{1} \neq y$ let the first inequality ($\leq$) be strict ($<$).

Define also a norm of subsets of $\mathcal{M}$ as a function $\mu : \mathcal{P}(\mathcal{M}) \rightarrow \mathbf{N}_\infty$, as follows : $\mu(A) = sup\{\|x\| \mid x \in A\}$. It is easy to check that μ enjoys the following properties: $\mu(\emptyset) = \mu(\{\mathbf{1}\}) = 0$, $\mu(A \circ B) \leq \mu(A) + \mu(B)$, if $A \neq \emptyset \neq B$ then $\mu(A), \mu(B) \leq \mu(A \circ B)$,

and $\mu(A \cup B) = max\{\mu(A), \mu(B)\}$. Moreover, it is obvious that $A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$ and $\mu(A^\circ) = \infty$.

Lemmata 1-8 allow for proving the following Theorems 1-3, known - in classical formal language theory - as iteration or pumping lemmata. It should, however, be noted that here they concern arbitrary monoids, not just a free (with respect to catenation) monoid of finite words over an alphabet. Nonetheless, proofs of these theorems with application of Lemmata 1-8 are analogous to those in the classical case.

Theorem 1 : Let $L \in \underline{RAT(\circ)}$ with $L \subseteq \mathcal{M}$. Then there exists $n(L) > 0$ such that, for any $w \in L$ with $\mu(\{w\}) > n(L)$, there exist $x_1, x_2, x_3 \in \mathcal{M}$ such that:

(i) $w \in \{x_1\} \circ \{x_2\} \circ \{x_3\}$
(ii) $0 < \mu(\{x_1\} \circ \{x_2\}) \leq n(L)$
(iii) $\{x_1\} \circ \{x_2\}^\circ \circ \{x_3\} \subseteq L$

□

Theorem 2 : Let $L \in \underline{LIN(\circ)}$ with $L \subseteq \mathcal{M}$. Then there exists $n(L) > 0$ such that, for any $w \in L$ with $\mu(\{w\}) > n(L)$, there exist $x_1, x_2, x_3, x_4, x_5 \in \mathcal{M}$ such that :

(i) $w \in \{x_1\} \circ \{x_2\} \circ \{x_3\} \circ \{x_4\} \circ \{x_5\}$
(ii) $0 < \mu(\{x_1\} \circ \{x_2\} \circ \{x_4\} \circ \{x_5\}) \leq n(L)$
(iii) $0 < \mu(\{x_2\} \circ \{x_4\})$
(iv) $\forall k \geq 0 : \{x_1\} \circ \{x_2\}^k \circ \{x_3\} \circ \{x_4\}^k \circ \{x_5\} \subseteq L$

□

Theorem 3 : Let $L \in \underline{ALG(\circ)}$ with $L \subseteq \mathcal{M}$. Then there exists $n(L) > 0$ such that, for any $w \in L$ with $\mu(\{w\}) > n(L)$, there exist $x_1, x_2, x_3, x_4, x_5 \in \mathcal{M}$ such that :

(i) $w \in \{x_1\} \circ \{x_2\} \circ \{x_3\} \circ \{x_4\} \circ \{x_5\}$.
(ii) $0 < \mu(\{x_2\} \circ \{x_3\} \circ \{x_4\}) \leq n(L)$.
(iii) $0 < \mu(\{x_2\} \circ \{x_4\})$
(iv) $\forall k \geq 0 : \{x_1\} \circ \{x_2\}^k \circ \{x_3\} \circ \{x_4\}^k \circ \{x_5\} \subseteq L$.

□

In the well known proofs of the iteration lemmata let
$m = min\{\mu(\alpha) \mid \alpha \in \mathcal{C}\}$, $M = max\{\mu(\alpha) \mid \alpha \in \mathcal{C}\}$.
In the rational and linear case in normal forms it follows that for an expression A of a derivation tree of depth d the following fact holds : $m \cdot d \leq \mu(A) \leq M \cdot d$, such that for the iteration constant $N(L) = M \cdot |\mathcal{X}|$ can be chosen.
In the algebraic case in normal form for an expression A of a derivation tree follows $m \cdot d \leq \mu(A) \leq M \cdot 2^{|\mathcal{X}|-1}$, such that for the iteration constant $N(L) = M \cdot 2^{|\mathcal{X}|-1}$ can be taken.
The lemmata themselves then are shown in the same way as for the classical word languages with catenation where $m = M = 1$.
For this note that if $x \in L$ with $\mu(x) = \mu(\{x\}) > s$ then there must exist an expression A of a derivation with $x \in A$ and $\mu(A) > s$.

References

1 Golan, J. S. : *The Theory of Semirings with Application in Mathematics and Theoretical Computer Science.* Longman Scientific and Technical, 1992.

2 Kudlek, M. : *Generalized Iteration Lemmata*, PU.M.A., vol. 6 No.2, 211-216, 1995

3 Kudlek, M. : *Iteration Lemmata for certain Classes of Word, Trace and Graph Languages*, Fundamenta Informaticae, vol. 37, No. 4, 413-422, 1999

4 Kuich, W., Salomaa, A. : *Semirings, Automata, Languages.* EATCS Monographs on Theoretical Computer Science 5, Springer, Berlin, 1986.