Equations in Words

Daniel Dombek

based on Lothaire: Algebraic Combinatorics on words

18-19 May 2011

Table of contents

Table of contents

Monoids

- $(M, \odot, 1_M)$ is a monoid, if

  $\odot : M \times M \to M$ associative with neutral element 1_M

Monoids

- $(M, \odot, 1_M)$ is a monoid, if

$$\odot : M \times M \to M \text{ associative with neutral element } 1_M$$

- $\varphi : M \to N$ is a morphism, if

$$\varphi(uv) = \varphi(u)\varphi(v), \quad \varphi(1_M) = 1_N$$

Monoids

- $(M, \odot, 1_M)$ is a monoid, if

$$\odot : M \times M \to M \text{ associative with neutral element } 1_M$$

- $\varphi : M \to N$ is a morphism, if

$$\varphi(uv) = \varphi(u)\varphi(v), \quad \varphi(1_M) = 1_N$$

- A^*, A^+ finite words over an alphabet A

Monoids

- $(M, \odot, 1_M)$ is a monoid, if

$$\odot : M \times M \to M \text{ associative with neutral element } 1_M$$

- $\varphi : M \to N$ is a morphism, if

$$\varphi(uv) = \varphi(u)\varphi(v), \quad \varphi(1_M) = 1_N$$

- A^*, A^+ finite words over an alphabet A
- $w = a_1 a_2 \cdots a_k \in A^* \quad \to \quad |w| = k$

Monoids

- $(M, \odot, 1_M)$ is a monoid, if

$$\odot : M \times M \to M \text{ associative with neutral element } 1_M$$

- $\varphi : M \to N$ is a morphism, if

$$\varphi(uv) = \varphi(u)\varphi(v), \quad \varphi(1_M) = 1_N$$

- A^*, A^+ finite words over an alphabet A
- $w = a_1 a_2 \cdots a_k \in A^* \quad \to \quad |w| = k$
- factor, prefix, suffix

Submonoids

- N is a submonoid of M, if

$$N \subset M, \quad 1 \in N, \quad NN \subset N$$

Submonoids

- N is a submonoid of M, if

$$N \subset M, \quad 1 \in N, \quad NN \subset N$$

- for any set $X \subset A^*$: X^* submonoid of A^*

Submonoids

- N is a submonoid of M, if

$$N \subset M, \quad 1 \in N, \quad NN \subset N$$

- for any set $X \subset A^*$: X^* submonoid of A^*
- for any submonoid $P \subset A^*$: $\exists_1 X \subset A^*$, the minimal generating set of P,

$$X = (P \setminus \{1\}) \setminus (P \setminus \{1\})^2$$

Submonoids

- N is a submonoid of M, if

$$N \subset M, \quad 1 \in N, \quad NN \subset N$$

- for any set $X \subset A^*$: X^* submonoid of A^*
- for any submonoid $P \subset A^*$: $\exists_1 X \subset A^*$, the minimal generating set of P,

$$X = (P \setminus \{1\}) \setminus (P \setminus \{1\})^2$$

- monoid M is free, if

$$\exists \text{ an alphabet } B \text{ and an isomorphism of } B^* \text{ onto } M$$

Submonoids

- N is a submonoid of M, if

$$N \subset M, \quad 1 \in N, \quad NN \subset N$$

- for any set $X \subset A^*$: X^* submonoid of A^*
- for any submonoid $P \subset A^*$: $\exists_1 X \subset A^*$, the minimal generating set of P,

$$X = (P \setminus \{1\}) \setminus (P \setminus \{1\})^2$$

- monoid M is free, if

$$\exists \text{ an alphabet } B \text{ and an isomorphism of } B^* \text{ onto } M$$

- the minimal generating set of a free submonoid of A^* is a code

Free submonoids

Proposition

Let P be a submonoid of A^*, with minimal generating set X. Then the following statements are equivalent:

1. *P is free*
2. *any equality*

   $$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m, \quad x_i, y_j \in X$$

   implies $n = m$ and $x_i = y_i$ for all $i \in \hat{n}$
3. *for any $w \in A^*$ it holds that*

   $$pw, wq \in P \text{ for some } p, q \in P \Rightarrow w \in P$$

Free submonoids

Proposition

Let P be a submonoid of A^*, with minimal generating set X. Then the following statements are equivalent:

1. *P is free*
2. *any equality*

   $$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m, \quad x_i, y_j \in X$$

   implies $n = m$ and $x_i = y_i$ for all $i \in \hat{n}$
3. *for any $w \in A^*$ it holds that*

   $$pw, wq \in P \text{ for some } p, q \in P \Rightarrow w \in P$$

Corollary: An intersection of free submonoids of A^* is free.

Defect theorem

Let $X \subset A^*$ and F the minimal free submonoid containing X. The free hull of X is the code generating F.

Defect theorem

Let $X \subset A^*$ and F the minimal free submonoid containing X. The free hull of X is the code generating F.

Theorem (Defect theorem)

The free hull Y of a finite subset $X \subset A^*$, which is not a code, satisfies

$$\#Y \leq \#X - 1 .$$

Defect theorem

Let $X \subset A^*$ and F the minimal free submonoid containing X. The free hull of X is the code generating F.

Theorem (Defect theorem)

The free hull Y of a finite subset $X \subset A^*$, which is not a code, satisfies

$$\#Y \leq \#X - 1\,.$$

Proof: define $\alpha : X \to Y$:

$$x \in X \to \alpha(x) = y \in Y \text{ such that } x \in yY^*$$

α is surjective and not injective $\Rightarrow$ statement holds

Defect theorem

Let $X \subset A^*$ and F the minimal free submonoid containing X. The free hull of X is the code generating F.

Theorem (Defect theorem)

The free hull Y of a finite subset $X \subset A^*$, which is not a code, satisfies

$$\#Y \leq \#X - 1\,.$$

Proof: define $\alpha : X \to Y$:

$$x \in X \to \alpha(x) = y \in Y \text{ such that } x \in yY^*$$

α is surjective and not injective $\Rightarrow$ statement holds

Corollary: Each pair of words $x, y \in A^*$ is a code, unless x and y are powers of a single word $z \in A^*$.

Primitive words

A word $x \in A^*$ is primitive if it is not a power of another word.

Primitive words

A word $x \in A^*$ is primitive if it is not a power of another word.

Proposition

Let $x, y \in A^*$. If

$$x^n = y^m \quad m, n \geq 0\,,$$

there exists a word z such that $x, y \in z^*$.

In particular, for each word $w \in A^+$ there exists a unique primitive word x such that $w \in x^*$.

Primitive words

A word $x \in A^*$ is primitive if it is not a power of another word.

Proposition

Let $x, y \in A^*$. If

$$x^n = y^m \quad m, n \geq 0\,,$$

there exists a word z such that $x, y \in z^*$.

In particular, for each word $w \in A^+$ there exists a unique primitive word x such that $w \in x^*$.

This can be refined as:

Proposition

Let $x, y \in A^*$, $n = |x|$, $m = |y|$, $d = gcd(n, m)$. If two powers x^p and y^q have a common prefix of length at least $n + m - d$, then $x, y \in z^*$ for some z.

Conjugacy

Two words $x, y \in A^*$ are conjugate if there exist $u, v \in A^*$ such that

$$x = uv, \quad y = vu\,.$$

Conjugacy - an equivalence relation on A^*, classes generated by a cyclic permutation.

Conjugacy

Two words $x, y \in A^*$ are conjugate if there exist $u, v \in A^*$ such that

$$x = uv, \quad y = vu\,.$$

Conjugacy - an equivalence relation on A^*, classes generated by a cyclic permutation.

Proposition

Two words $x, y \in A^+$ are conjugate iff there exists $z \in A^*$ such that

$$xz = zy\,.$$

More precisely, this equality holds iff there exist $u, v \in A^*$ such that

$$x = uv, \quad y = vu, \quad z \in u(vu)^*\,.$$

Table of contents

Equation in words - motivation

Consider two commuting words $x, y \in A^*$,

$$xy = yx\,,$$

it holds

$$x = u^n, y = u^p, \quad \text{for some } u \in A^*, n, p \geq 0\,.$$

Equation in words - motivation

Consider two commuting words $x, y \in A^*$,

$$xy = yx\,,$$

it holds

$$x = u^n, y = u^p, \qquad \text{for some } u \in A^*, n, p \geq 0\,.$$

The simplest example of equation in words:

- $x, y \cdots$ unknowns
- $xy = yx \cdots$ equation
- morphism α defined by $\alpha(x) = u^n, \alpha(y) = u^p$ satisfies $\alpha(xy) = \alpha(yx) \cdots$ solution of $xy = yx$

Definitions I

- alphabet of unknowns $\cdots$ Ξ fixed, finite, nonempty set

Definitions I

- alphabet of unknowns $\cdots$ Ξ fixed, finite, nonempty set
- system of equations $\mathcal{S}$ $\cdots$ set of pairs $(e, e') \in \Xi^* \times \Xi^*$

Definitions I

- alphabet of unknowns $\cdots$ Ξ fixed, finite, nonempty set
- system of equations $\mathcal{S}$ $\cdots$ set of pairs $(e, e') \in \Xi^* \times \Xi^*$
- solution of $\mathcal{S}$ $\cdots$ any morphism such that $\alpha(e) = \alpha(e')$ for all pairs $(e, e') \in \mathcal{S}$

Definitions I

- alphabet of unknowns $\cdots$ Ξ fixed, finite, nonempty set
- system of equations $\mathcal{S}$ $\cdots$ set of pairs $(e, e') \in \Xi^* \times \Xi^*$
- solution of $\mathcal{S}$ $\cdots$ any morphism such that $\alpha(e) = \alpha(e')$ for all pairs $(e, e') \in \mathcal{S}$

solving finite system of equations $\Leftrightarrow$ solving single equation

Definitions II

Morphism $\alpha : \Xi^* \to A^*$ can be:

- total $\cdots$ all letters of A occur in $\alpha(x)$ for some $x \in \Xi$

Definitions II

Morphism $\alpha : \Xi^* \to A^*$ can be:

- total $\cdots$ all letters of A occur in $\alpha(x)$ for some $x \in \Xi$
- nonerasing $\cdots$ $\alpha(x) \neq 1$ for all $x \in \Xi$

Definitions II

Morphism $\alpha : \Xi^* \to A^*$ can be:

- total $\cdots$ all letters of A occur in $\alpha(x)$ for some $x \in \Xi$
- nonerasing $\cdots$ $\alpha(x) \neq 1$ for all $x \in \Xi$
- cyclic $\cdots$ exists $v \in A^*$ such that $\alpha(x) \in v^*$ for all $x \in \Xi$

Definitions II

Morphism $\alpha : \Xi^* \to A^*$ can be:

- total $\cdots$ all letters of A occur in $\alpha(x)$ for some $x \in \Xi$
- nonerasing $\cdots$ $\alpha(x) \neq 1$ for all $x \in \Xi$
- cyclic $\cdots$ exists $v \in A^*$ such that $\alpha(x) \in v^*$ for all $x \in \Xi$

Let $\alpha_1 : \Xi^* \to A_1^*$, $\alpha_2 : \Xi^* \to A_2^*$ be total morphisms. If there is a nonerasing morphism $\theta : A_1^* \to A_2^*$, $\alpha_2 = \theta \circ \alpha_1$, then α_1 divides α_2 ($\alpha_1 \leqslant \alpha_2$)

Definitions II

Morphism $\alpha : \Xi^* \to A^*$ can be:

- total $\cdots$ all letters of A occur in $\alpha(x)$ for some $x \in \Xi$
- nonerasing $\cdots$ $\alpha(x) \neq 1$ for all $x \in \Xi$
- cyclic $\cdots$ exists $v \in A^*$ such that $\alpha(x) \in v^*$ for all $x \in \Xi$

Let $\alpha_1 : \Xi^* \to A_1^*$, $\alpha_2 : \Xi^* \to A_2^*$ be total morphisms. If there is a nonerasing morphism $\theta : A_1^* \to A_2^*$, $\alpha_2 = \theta \circ \alpha_1$, then α_1 divides α_2 ($\alpha_1 \leqslant \alpha_2$)

α_1 and α_2 are equivalent ($\alpha_1 \approx \alpha_2$), if $\alpha_1 \leqslant \alpha_2$ and $\alpha_2 \leqslant \alpha_1$.

Equations I

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyz, zxy)$$

Equations I

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyz, zxy)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k\,,$$

where $u, v \in A^*$ *and* $i, j, k \geq 0$.

Equations I

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyz, zxy)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k\,,$$

where $u, v \in A^*$ *and* $i, j, k \geq 0$*.*

Proof: define $\Theta = \{a, b\}$, $\varphi : \Theta^* \to \Xi^*, \varphi(a) = xy, \varphi(b) = z$.

Equations I

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyz, zxy)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k ,$$

where $u, v \in A^*$ *and* $i, j, k \geq 0$.

Proof: define $\Theta = \{a, b\}$, $\varphi : \Theta^* \to \Xi^*, \varphi(a) = xy, \varphi(b) = z$.

α solution of $(xyz, zxy) \Leftrightarrow \alpha \circ \varphi$ solution of (ab, ba)

Equations I

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyz, zxy)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k,$$

where $u, v \in A^*$ *and* $i, j, k \geq 0$.

Proof: define $\Theta = \{a, b\}$, $\varphi : \Theta^* \to \Xi^*, \varphi(a) = xy, \varphi(b) = z$.

α solution of $(xyz, zxy) \Leftrightarrow \alpha \circ \varphi$ solution of (ab, ba)

$\to$ defect theorem

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xy^2x, zt^2z)$$

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xy^2x, zt^2z)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k u, \quad \alpha(t) = v(uv)^l,$$

where $u, v \in A^*$ *and* $i, j, k, l \geq 0$ *such that* $i + j = k + l$.

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xy^2x, zt^2z)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k u, \quad \alpha(t) = v(uv)^l,$$

where $u, v \in A^*$ *and* $i, j, k, l \geq 0$ *such that* $i + j = k + l$*.*

Proof: set $\alpha(x) = a$, $\alpha(y) = b$, $\alpha(z) = c$, $\alpha(t) = d$

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xy^2x, zt^2z)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k u, \quad \alpha(t) = v(uv)^l,$$

where $u, v \in A^*$ *and* $i, j, k, l \geq 0$ *such that* $i + j = k + l$.

Proof: set $\alpha(x) = a$, $\alpha(y) = b$, $\alpha(z) = c$, $\alpha(t) = d$

equation splits into $ab = cd$, $ba = dc$

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xy^2x, zt^2z)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k u, \quad \alpha(t) = v(uv)^l,$$

where $u, v \in A^*$ *and* $i, j, k, l \geq 0$ *such that* $i + j = k + l$*.*

Proof: set $\alpha(x) = a$, $\alpha(y) = b$, $\alpha(z) = c$, $\alpha(t) = d$

equation splits into $ab = cd$, $ba = dc$
WLOG $|a| \geq |c|$, $a = ce, d = eb$

Equations II

Proposition

All solutions $\alpha : \Xi^* \to A^*$ of the equation

$$(xy^2x, zt^2z)$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = v(uv)^j, \quad \alpha(z) = (uv)^k u, \quad \alpha(t) = v(uv)^l,$$

where $u, v \in A^*$ and $i, j, k, l \geq 0$ such that $i + j = k + l$.

Proof: set $\alpha(x) = a$, $\alpha(y) = b$, $\alpha(z) = c$, $\alpha(t) = d$

equation splits into $ab = cd$, $ba = dc$
WLOG $|a| \geq |c|$, $a = ce, d = eb$

$\to bce = ebc$ (previous case)

Equations III

Proposition

All solutions $\alpha : \Xi^* \to A^*$ of the equation

$$((xy)^m x, z^n), \quad m > 1, n > 1$$

Equations III

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$((xy)^m x, z^n), \quad m > 1, n > 1$$

are cyclic.

Equations III

Proposition

All solutions $\alpha : \Xi^* \to A^*$ of the equation

$$((xy)^m x, z^n), \quad m > 1, n > 1$$

are cyclic.

Proof: $\alpha(xy)^m$ and $\alpha(z)^n$ have long common prefix $\Rightarrow$ powers of the same word

Equations III

Proposition

All solutions $\alpha : \Xi^* \to A^*$ of the equation

$$((xy)^m x, z^n), \quad m > 1, n > 1$$

are cyclic.

Proof: $\alpha(xy)^m$ and $\alpha(z)^n$ have long common prefix $\Rightarrow$ powers of the same word

$\alpha(xy) = u^i$, $\alpha(z) = u^j$ implies

$$\alpha(x) = u^{jn-im},\ \alpha(y) = u^{i-(jn-im)}\,.$$

Equations IV

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyx, z^n), \quad n > 1$$

Equations IV

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyx, z^n), \quad n > 1$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = vu\big((uv)^{i+1}u\big)^{n-2}uv, \quad \alpha(z) = (uv)^{i+1}u\,,$$

where $u, v \in A^*$ *and* $i \geq 0$.

Equations IV

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyx, z^n), \quad n > 1$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = vu\big((uv)^{i+1}u\big)^{n-2}uv, \quad \alpha(z) = (uv)^{i+1}u\,,$$

where $u, v \in A^*$ *and* $i \geq 0$.

Proof: if α noncyclic, then $|\alpha(x)| < |\alpha(z)|$

Equations IV

Proposition

All solutions $\alpha : \Xi^* \to A^*$ of the equation

$$(xyx, z^n), \quad n > 1$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = vu\big((uv)^{i+1}u\big)^{n-2}uv, \quad \alpha(z) = (uv)^{i+1}u\,,$$

where $u, v \in A^*$ and $i \geq 0$.

Proof: if α noncyclic, then $|\alpha(x)| < |\alpha(z)|$

$\alpha(x)\alpha(y)\alpha(x) = \alpha(z)^n \Rightarrow \alpha(z) = \alpha(x)w = t\alpha(x)$ for some $w, t \in A^*$

Equations IV

Proposition

All solutions $\alpha : \Xi^* \to A^*$ *of the equation*

$$(xyx, z^n), \quad n > 1$$

are of the form

$$\alpha(x) = (uv)^i u, \quad \alpha(y) = vu\big((uv)^{i+1}u\big)^{n-2}uv, \quad \alpha(z) = (uv)^{i+1}u\,,$$

where $u, v \in A^*$ *and* $i \geq 0$.

Proof: if α noncyclic, then $|\alpha(x)| < |\alpha(z)|$

$\alpha(x)\alpha(y)\alpha(x) = \alpha(z)^n \Rightarrow \alpha(z) = \alpha(x)w = t\alpha(x)$ for some $w, t \in A^*$

$\to$ w and t conjugated

Main theorem

Theorem

For all integers $n, m, p \geq 2$, the equation

$$(x^n y^m, z^p)$$

admits only cyclic solutions.

Main theorem

Theorem

For all integers $n, m, p \geq 2$, the equation

$$(x^n y^m, z^p)$$

admits only cyclic solutions.

Proof: by contradiction

suppose there is A finite, $u, v, w \in A^*$ not powers of a common word, $n, m, p \geq 2$ such that $u^m v^n = w^p$ and w has minimal length

Proof I

noncyclic solution $\rightarrow$ common prefix (suffix) of w^p and u^n (v^m) has bounded length:

Proof I

noncyclic solution $\rightarrow$ common prefix (suffix) of w^p and u^n (v^m) has bounded length:

$$(n-1)|v| < |w|$$
$$(m-1)|u| < |w|$$

Proof I

noncyclic solution $\rightarrow$ common prefix (suffix) of w^p and u^n (v^m) has bounded length:

$$(n-1)|v| < |w|$$
$$(m-1)|u| < |w|$$

trivial cases:

- $p \geq 4$
- $p = 3$ and $n, m \geq 3$

$\rightarrow$ contradiction

Proof II

1. $n = 2, m \geq 3, p = 3.$

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 .$$

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 .$$

$\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 \,.$$

   $\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

2. $n = m = 2, p = 3$.

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 \,.$$

   $\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

2. $n = m = 2, p = 3$. Similar argument is used for

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^2 \,.$$

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2\,.$$

$\to$ previous case $(xyx, z^n) \to$ contradiction

2. $n = m = 2, p = 3$. Similar argument is used for

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^2\,.$$

3. $n, m \geq 2, p = 2$.

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 .$$

$\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

2. $n = m = 2, p = 3$. Similar argument is used for

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^2 .$$

3. $n, m \geq 2, p = 2$. We may assume $w = u^n v_1 = v_2 (v_1 v_2)^{m-1}$, where $v = v_1 v_2$.

Proof II

1. $n = 2, m \geq 3, p = 3$. It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 .$$

$\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

2. $n = m = 2, p = 3$. Similar argument is used for

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^2 .$$

3. $n, m \geq 2, p = 2$. We may assume $w = u^n v_1 = v_2 (v_1 v_2)^{m-1}$, where $v = v_1 v_2$.

$\rightarrow$ $u^n v_1^2 = (v_2 v_1)^m$ and $|w| > |v_2 v_1|$

Proof II

1. $n = 2, m \geq 3, p = 3.$ It holds $|w| < |u^2| < 2|w|$, and

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^m, \qquad \text{where } w = w_1 w_2 \,.$$

$\rightarrow$ previous case (xyx, z^n) $\rightarrow$ contradiction

2. $n = m = 2, p = 3.$ Similar argument is used for

$$w_1 w_2 w_1 = u^2, \quad w_2 w_1 w_2 = v^2 \,.$$

3. $n, m \geq 2, p = 2.$ We may assume $w = u^n v_1 = v_2 (v_1 v_2)^{m-1}$, where $v = v_1 v_2$.

$\rightarrow$ $u^n v_1^2 = (v_2 v_1)^m$ and $|w| > |v_2 v_1|$

$\rightarrow$ contradiction with the minimality of $|w|$

Table of contents

Parametrization

In previous examples - all solutions can be described by finite number of parameters (words, powers) $\cdots$ parametrizable equation

Parametrization

In previous examples - all solutions can be described by finite number of parameters (words, powers) $\cdots$ parametrizable equation

Hmelevskii (1976):

- all equations in 3 unknowns are parametrizable
- equations with 4 or more unknowns are not parametrizable (gave an example (xyz, ztx))

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha\,.$$

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha\,.$$

Any solution can be divided by some (unique) principal solution.

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha\,.$$

Any solution can be divided by some (unique) principal solution.

How to find principal solutions?

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha\,.$$

Any solution can be divided by some (unique) principal solution.

How to find principal solutions?

- we define fundamental solutions

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha \,.$$

Any solution can be divided by some (unique) principal solution.

How to find principal solutions?

- we define fundamental solutions
- those are "easy" to get

Principal solutions

Let $\alpha : \Xi^* \to A^*$ solve (e, e'). It is principal if for all solutions $\beta : \Xi^* \to B^*$ holds

$$\beta \leqslant \alpha \;\Rightarrow\; \beta \approx \alpha\,.$$

Any solution can be divided by some (unique) principal solution.

How to find principal solutions?

- we define fundamental solutions
- those are "easy" to get
- we show that fundamental solutions $\approx$ principal solutions

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if } y \in \Xi \setminus \{x'\} \\ xx' & \text{if } y = x' \end{cases}$$

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ xx' & \text{if } \; y = x' \end{cases}$$

$$\varepsilon_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ x & \text{if } \; y = x' \end{cases}$$

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ xx' & \text{if } \; y = x' \end{cases}$$

$$\varepsilon_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ x & \text{if } \; y = x' \end{cases}$$

- consider an equation $(e, e') \in \Xi^* \times \Xi^*$

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ xx' & \text{if } \; y = x' \end{cases}$$

$$\varepsilon_{xx'}(y) = \begin{cases} y & \text{if } \; y \in \Xi \setminus \{x'\} \\ x & \text{if } \; y = x' \end{cases}$$

- consider an equation $(e, e') \in \Xi^* \times \Xi^*$
- suppose $e = gxh$, $e' = gx'h'$, where $x, x' \in \Xi$, $x \neq x'$, $g, g', h, h' \in \Xi^*$

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if} \quad y \in \Xi \setminus \{x'\} \\ xx' & \text{if} \quad y = x' \end{cases}$$

$$\varepsilon_{xx'}(y) = \begin{cases} y & \text{if} \quad y \in \Xi \setminus \{x'\} \\ x & \text{if} \quad y = x' \end{cases}$$

- consider an equation $(e, e') \in \Xi^* \times \Xi^*$
- suppose $e = gxh$, $e' = gx'h'$, where $x, x' \in \Xi$, $x \neq x'$, $g, g', h, h' \in \Xi^*$
- $\varphi_{xx'}, \varphi_{x'x}$ are regular elementary transformations attached to (e, e')

Fundamental solutions I

We define following morphisms of Ξ^* into Ξ^*:

$$\varphi_{xx'}(y) = \begin{cases} y & \text{if } \ y \in \Xi \setminus \{x'\} \\ xx' & \text{if } \ y = x' \end{cases}$$

$$\varepsilon_{xx'}(y) = \begin{cases} y & \text{if } \ y \in \Xi \setminus \{x'\} \\ x & \text{if } \ y = x' \end{cases}$$

- consider an equation $(e, e') \in \Xi^* \times \Xi^*$
- suppose $e = gxh$, $e' = gx'h'$, where $x, x' \in \Xi$, $x \neq x'$, $g, g', h, h' \in \Xi^*$
- $\varphi_{xx'}, \varphi_{x'x}$ are regular elementary transformations attached to (e, e')
- $\varepsilon_{xx'}$ is singular elementary transformation attached to (e, e')

Fundamental solutions II

A transformation attached to (e, e') is any product $\varphi_n \cdots \varphi_1$ such that for all $i \in \hat{n}$, φ_i is an elementary transformation attached to

$$(\varphi_{i-1} \cdots \varphi_1(e), \varphi_{i-1} \cdots \varphi_1(e'))\,.$$

Fundamental solutions II

A transformation attached to (e, e') is any product $\varphi_n \cdots \varphi_1$ such that for all $i \in \hat{n}$, φ_i is an elementary transformation attached to

$$(\varphi_{i-1} \cdots \varphi_1(e), \varphi_{i-1} \cdots \varphi_1(e'))\,.$$

Suppose φ attached to (e, e') satisfies $\varphi(e) = \varphi(e')$. Then φ is called a fundamental solution of (e, e').

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

$(x|yz, x|zx)$

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

$$(x|yz, x|zx) \stackrel{\varphi_{zy}}{\rightarrow} (xz|yz, xz|x)$$

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

$$(x|yz, x|zx) \stackrel{\varphi_{zy}}{\to} (xz|yz, xz|x) \stackrel{\varphi_{yx}}{\to} (yxzy|z, yxzy|x)$$

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

$$(x|yz, x|zx) \stackrel{\varphi_{zy}}{\to} (xz|yz, xz|x) \stackrel{\varphi_{yx}}{\to} (yxzy|z, yxzy|x) \stackrel{\varepsilon_{zx}}{\to} (yzzyz, yzzyz)\,,$$

Fundamental solutions III

Example

Consider the equation (xyz, xzx)*:*

$$(x|yz, x|zx) \stackrel{\varphi_{zy}}{\to} (xz|yz, xz|x) \stackrel{\varphi_{yx}}{\to} (yxzy|z, yxzy|x) \stackrel{\varepsilon_{zx}}{\to} (yzzyz, yzzyz)\,,$$

hence $\varphi = \varepsilon_{zx}\varphi_{yx}\varphi_{zy}$ *is a fundamental solution of* (xyz, xzx)*. It is defined as*

$$\varphi(x) = yz, \quad \varphi(y) = zy, \quad \varphi(z) = z\,.$$

Equivalence

Proposition

Each nonerasing solution $\alpha : \Xi^* \to A^*$ of the equation (e, e') has a unique factorization

$$\alpha = \theta\varphi_n \cdots \varphi_1 \,,$$

where $\varphi_n \cdots \varphi_1$ is a factorization of a fundamental solution of (e, e') into elementary transformations and θ is nonerasing morphism.

Equivalence

Proposition

Each nonerasing solution $\alpha : \Xi^* \to A^*$ of the equation (e, e') has a unique factorization

$$\alpha = \theta\varphi_n \cdots \varphi_1 \,,$$

where $\varphi_n \cdots \varphi_1$ is a factorization of a fundamental solution of (e, e') into elementary transformations and θ is nonerasing morphism.

Note: $\varphi_n \cdots \varphi_1$ is also a principal solution $\to$ each solution of a given equation can be divided by some unique principal solution

Graph associated with an equation

- denote by V the subset of $\Xi^* \times \Xi^*$ containing $(1, 1)$ and all pairs (f, f') where f, f' nonempty not having common prefix

Graph associated with an equation

- denote by V the subset of $\Xi^* \times \Xi^*$ containing $(1, 1)$ and all pairs (f, f') where f, f' nonempty not having common prefix
- let E be a set of edges: $(f, f') \xrightarrow{\varphi} (g, g') \in G \Leftrightarrow \varphi$ is an elementary transformation attached to (f, f') satisfying $\varphi(f) = hg$, $\varphi(f') = hg'$ with h as long as possible

Graph associated with an equation

- denote by V the subset of $\Xi^* \times \Xi^*$ containing $(1,1)$ and all pairs (f, f') where f, f' nonempty not having common prefix
- let E be a set of edges: $(f, f') \xrightarrow{\varphi} (g, g') \in G \Leftrightarrow \varphi$ is an elementary transformation attached to (f, f') satisfying $\varphi(f) = hg$, $\varphi(f') = hg'$ with h as long as possible
- the graph associated with (e, e') is defined as induced subgraph G' of $G = (V, E)$ containing only vertices (e, e'), $(1, 1)$ and those "in between"

Graph associated with an equation

- denote by V the subset of $\Xi^* \times \Xi^*$ containing $(1, 1)$ and all pairs (f, f') where f, f' nonempty not having common prefix
- let E be a set of edges: $(f, f') \xrightarrow{\varphi} (g, g') \in G \Leftrightarrow \varphi$ is an elementary transformation attached to (f, f') satisfying $\varphi(f) = hg$, $\varphi(f') = hg'$ with h as long as possible
- the graph associated with (e, e') is defined as induced subgraph G' of $G = (V, E)$ containing only vertices (e, e'), $(1, 1)$ and those "in between"
- examples ...

Remarks

Denote:

- $|f|_x = \#\{$ occurences of $x \in \Xi$ in $f \in \Xi^*\}$

Remarks

Denote:

- $|f|_x = \#\{$ occurences of $x \in \Xi$ in $f \in \Xi^*\}$
- $\|f\| = \max\{|f|_x, x \in \Xi\}$

Remarks

Denote:

- $|f|_x = \#\{$ occurences of $x \in \Xi$ in $f \in \Xi^*\}$
- $\|f\| = \max\{|f|_x, x \in \Xi\}$

Proposition

Assume that

- $|e|_x|e'|_x \leq 1$ *for all* $x \in \Xi$,
- $\max\{\|e\|, \|e'\|\} \leq 2$.

Then the graph associated with (e, e') *is finite.*

Remarks

Denote:

- $|f|_x = \#\{$ occurences of $x \in \Xi$ in $f \in \Xi^*\}$
- $\|f\| = \max\{|f|_x, x \in \Xi\}$

Proposition

Assume that

- $|e|_x|e'|_x \leq 1$ *for all* $x \in \Xi$,
- $\max\{\|e\|, \|e'\|\} \leq 2$.

Then the graph associated with (e, e') *is finite.*

Remarks:

- similar procedure for solving equations with constants

Remarks

Denote:

- $|f|_x = \#\{$ occurences of $x \in \Xi$ in $f \in \Xi^*\}$
- $\|f\| = \max\{|f|_x, x \in \Xi\}$

Proposition

Assume that

- $|e|_x|e'|_x \leq 1$ *for all* $x \in \Xi$,
- $\max\{\|e\|, \|e'\|\} \leq 2$.

Then the graph associated with (e, e') *is finite.*

Remarks:

- similar procedure for solving equations with constants
- Makanin algorithm - decides if a solution exists even if the graph is infinite, nondeterministic but always decides