On word equations in one variable with constants

Dirk Nowotka   Aleksi Saarela

University of Kiel   University of Turku

Les Diablerets 2016

Setting

- $\Delta = \{x, y, z\}$ – variables
- $\Sigma = \{a, b\}$ – constants
- $(\Delta \cup \Sigma)^* \times (\Delta \cup \Sigma)^*$ – equations
- $h\colon (\Delta \cup \Sigma)^* \to \Sigma^*$ constant preserving – solution
- one-variable case: $[M]$ – set of solutions with $h(x) \in M$

Setting

- $\Delta = \{x, y, z\}$ – variables
- $\Sigma = \{a, b\}$ – constants
- $(\Delta \cup \Sigma)^* \times (\Delta \cup \Sigma)^*$ – equations
- $h\colon (\Delta \cup \Sigma)^* \to \Sigma^*$ constant preserving – solution
- one-variable case: $[M]$ – set of solutions with $h(x) \in M$

Examples

- $xaxbab = abaxbx$ $\qquad$ $h(x) = \varepsilon$ or $h(x) = ab$

Setting

- $\Delta = \{x, y, z\}$ – variables
- $\Sigma = \{a, b\}$ – constants
- $(\Delta \cup \Sigma)^* \times (\Delta \cup \Sigma)^*$ – equations
- $h\colon (\Delta \cup \Sigma)^* \to \Sigma^*$ constant preserving – solution
- one-variable case: $[M]$ – set of solutions with $h(x) \in M$

Examples

- $xaxbab = abaxbx$ $\quad$ $h(x) = \varepsilon$ or $h(x) = ab$
- $xxbaaba = aabaxbx$ $\quad$ $h(x) = a$ or $h(x) = aaba$

Setting

- $\Delta = \{x, y, z\}$ – variables
- $\Sigma = \{a, b\}$ – constants
- $(\Delta \cup \Sigma)^* \times (\Delta \cup \Sigma)^*$ – equations
- $h\colon (\Delta \cup \Sigma)^* \to \Sigma^*$ constant preserving – solution
- one-variable case: $[M]$ – set of solutions with $h(x) \in M$

Examples

- $xaxbab = abaxbx$ $\quad$ $h(x) = \varepsilon$ or $h(x) = ab$
- $xxbaaba = aabaxbx$ $\quad$ $h(x) = a$ or $h(x) = aaba$
- $xab = bax$ $\quad$ $[b(ab)^*]$

Setting

- $\mathrm{Sol}(E)$ – set of solutions of equation E

Setting

- $\mathrm{Sol}(E)$ – set of solutions of equation E
- $E_1, \ldots E_N$ system of equations – independent if $h_1, \ldots h_N$ exist s.t. $h_i \in \mathrm{Sol}(E_j)$ iff $i \neq j$
  $(h_1, \ldots h_N)$ – independence certificate

Setting

- $\mathrm{Sol}(E)$ – set of solutions of equation E
- $E_1, \ldots E_N$ system of equations – independent if $h_1, \ldots h_N$ exist s.t. $h_i \in \mathrm{Sol}(E_j)$ iff $i \neq j$
  $(h_1, \ldots h_N)$ – independence certificate
- $E_1, \ldots E_N$ independent system with non-periodic solution h – strongly independent system
  $(h_1, \ldots h_N, h)$ – strong independence certificate

Setting

- $\mathrm{Sol}(E)$ – set of solutions of equation E
- $E_1, \dots E_N$ system of equations – independent if $h_1, \dots h_N$ exist s.t. $h_i \in \mathrm{Sol}(E_j)$ iff $i \neq j$
  $(h_1, \dots h_N)$ – independence certificate
- $E_1, \dots E_N$ independent system with non-periodic solution h – strongly independent system
  $(h_1, \dots h_N, h)$ – strong independence certificate

Examples

- $xyz = zyx$ and $xyyz = zyyx$ strongly independent certificate $((a, b, abba), (a, b, aba), (a, b, a))$

Setting

- $\mathrm{Sol}(E)$ – set of solutions of equation E
- $E_1, \ldots E_N$ system of equations – independent if $h_1, \ldots h_N$ exist s.t. $h_i \in \mathrm{Sol}(E_j)$ iff $i \neq j$
  $(h_1, \ldots h_N)$ – independence certificate
- $E_1, \ldots E_N$ independent system with non-periodic solution h – strongly independent system
  $(h_1, \ldots h_N, h)$ – strong independence certificate

Examples

- $xyz = zyx$ and $xyyz = zyyx$ strongly independent
  certificate $((a, b, abba), (a, b, aba), (a, b, a))$
- $x = \varepsilon$ and $y = \varepsilon$ and $z = \varepsilon$ independent (not strongly)
  certificate $((a, \varepsilon, \varepsilon), (\varepsilon, a, \varepsilon), (\varepsilon, \varepsilon, a))$

Context

Theorem (Laine & Plandowski 2011)

Let E be a one-variable equation.
If $\mathrm{Sol}(E)$ infinite, then $\mathrm{Sol}(E) = [(pq)^* p]$ with pq primitive.
If $\mathrm{Sol}(E)$ finite, then $|\mathrm{Sol}(E)| \leq 8 \log n + \mathcal{O}(1)$.

Context

Theorem (Laine & Plandowski 2011)

Let E be a one-variable equation.
If $\mathrm{Sol}(E)$ infinite, then $\mathrm{Sol}(E) = [(pq)^*p]$ with pq primitive.
If $\mathrm{Sol}(E)$ finite, then $|\mathrm{Sol}(E)| \leq 8 \log n + \mathcal{O}(1)$.

Theorem (Holub & Žemlička 2015)

A strongly independent system of 3-var equations (no constants) has at most $\mathcal{O}(n)$ equations, where n is the length of the shortest equation.

Conjectures

Conjecture (SOL-XAB)

There exists a number c, s.t. every one-var equation has either infinitely many or at most c solutions.

Conjectures

Conjecture (SOL-XAB)

There exists a number c, s.t. every one-var equation has either infinitely many or at most c solutions.

Conjecture (SIND-XAB)

There exists a number c, s.t. every strongly independent system of one-var equations is of size at most c.

Conjectures

Conjecture (SOL-XAB)

There exists a number c, s.t. every one-var equation has either infinitely many or at most c solutions.

Conjecture (SIND-XAB)

There exists a number c, s.t. every strongly independent system of one-var equations is of size at most c.

Conjecture (SIND-XYZ)

There exists a number c, s.t. every strongly independent system of three-var equations (no constants) is of size at most c.

Conjectures

Conjecture (SOL-XAB)

There exists a number c*, s.t. every one-var equation has either infinitely many or at most* c *solutions.*

Conjecture (SIND-XAB)

There exists a number c*, s.t. every strongly independent system of one-var equations is of size at most* c*.*

Conjecture (SIND-XYZ)

There exists a number c*, s.t. every strongly independent system of three-var equations (no constants) is of size at most* c*.*

Theorem

$$\text{SOL-XAB}(c) \Rightarrow \text{SIND-XAB}(c) \begin{cases} \Leftarrow \text{SIND-XYZ}(c) \\ \Rightarrow \text{SIND-XYZ}(6c+9) \end{cases}$$

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Theorem (Dabrowski & Plandowski 2011)

Let E one-var equation and pq primitive. Then

$$\mathrm{Sol}(E) \cap [(pq)^+ p]$$

is either equal to $[(pq)^+ p]$ or has at most one element.

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \ldots E_N$ strongly independent system of one-var equations.
If $N \geq 3$ then no equation has infinitely many solutions.

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \ldots E_N$ strongly independent system of one-var equations.
If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \ldots E_N$ strongly independent system of one-var equations.
If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \dots E_N$ strongly independent system of one-var equations. If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate
- h_3, h_4 solutions of E_1, E_2

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \dots E_N$ strongly independent system of one-var equations. If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate
- h_3, h_4 solutions of E_1, E_2
- $(pq)^i p = (p'q')^{i'} p'$ and $(pq)^j p = (p'q')^{j'} p'$ with $i < j$

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \ldots E_N$ strongly independent system of one-var equations. If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate
- h_3, h_4 solutions of E_1, E_2
- $(pq)^i p = (p'q')^{i'} p'$ and $(pq)^j p = (p'q')^{j'} p'$ with $i < j$
- $(pq)^{j-i} = (pq)^{j'-i'}$ implies $pq = p'q'$ implies $p = p'$ and $q = q'$

SOL-XAB$(c) \Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \dots E_N$ strongly independent system of one-var equations.
If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate
- h_3, h_4 solutions of E_1, E_2
- $(pq)^i p = (p'q')^{i'} p'$ and $(pq)^j p = (p'q')^{j'} p'$ with $i < j$
- $(pq)^{j-i} = (pq)^{j'-i'}$ implies $pq = p'q'$ implies $p = p'$ and $q = q'$
- Suppose $[(pq)^* p] \cap \mathrm{Sol}(E_2)$ finite

SOL-XAB(c) $\Rightarrow$ SIND-XAB(c)

Lemma

Let $E_1, \ldots E_N$ strongly independent system of one-var equations. If $N \geq 3$ then no equation has infinitely many solutions.

Suppose $\mathrm{Sol}(E_1) = [(pq)^* p]$.

- Suppose $\mathrm{Sol}(E_2) = [(p'q')^* p']$ and (h_1, h_2, h_3, h_4) s. i. certificate
- h_3, h_4 solutions of E_1, E_2
- $(pq)^i p = (p'q')^{i'} p'$ and $(pq)^j p = (p'q')^{j'} p'$ with $i < j$
- $(pq)^{j-i} = (pq)^{j'-i'}$ implies $pq = p'q'$ implies $p = p'$ and $q = q'$
- Suppose $[(pq)^* p] \cap \mathrm{Sol}(E_2)$ finite
- Contains two solutions h_3, h_4 contradicting previous theorem

SIND-XAB$(c) \Leftarrow$ SIND-XYZ(c)

Lemma

Let $\Sigma = \{a_1, \dots a_k\}$ *constants and*

$$\alpha\colon (\{x\} \cup \Sigma)^* \to \{x, y, z\}^*, \qquad x \mapsto x, \quad a_i \mapsto y^i z.$$

Let $E_1, \dots E_N$ *strongly independent system of one-var equations. Then* $\alpha(E_1), \dots \alpha(E_N)$ *strongly independent system of three-var equations (no constants).*

SIND-XAB(c) $\Leftarrow$ SIND-XYZ(c)

Lemma

Let $\Sigma = \{a_1, \ldots a_k\}$ *constants and*

$$\alpha\colon \ (\{x\} \cup \Sigma)^* \to \{x, y, z\}^*, \qquad x \mapsto x, \quad a_i \mapsto y^i z.$$

Let $E_1, \ldots E_N$ *strongly independent system of one-var equations. Then* $\alpha(E_1), \ldots \alpha(E_N)$ *strongly independent system of three-var equations (no constants).*

- Let $\beta\colon \Sigma^* \to \{a, b\}^*, \qquad a_i \mapsto a^i b$.

SIND-XAB(c) $\Leftarrow$ SIND-XYZ(c)

Lemma

Let $\Sigma = \{a_1, \dots a_k\}$ *constants and*

$$\alpha\colon (\{x\} \cup \Sigma)^* \to \{x, y, z\}^*, \qquad x \mapsto x, \quad a_i \mapsto y^i z.$$

Let $E_1, \dots E_N$ *strongly independent system of one-var equations. Then* $\alpha(E_1), \dots \alpha(E_N)$ *strongly independent system of three-var equations (no constants).*

- Let $\beta\colon \Sigma^* \to \{a, b\}^*, \qquad a_i \mapsto a^i b$.
- h is non-periodic solution of E, if, and only if,

  $$g_h\colon \{x, y, z\}^* \to \{a, b\}^*, \qquad x \mapsto \beta(h(x)), \quad y \mapsto a, \quad z \mapsto b$$

  is non-periodic solution of $\alpha(E)$.
  ($g_h \circ \alpha = \beta \circ h$ and β injective)

Budkina & Markov 1973; Spehner 1986

Classification of solutions of three-var equations (no constants):

$$\mathcal{A}: \; h(x) = a, \; h(y) = b, \; h(z) = c$$

Budkina & Markov 1973; Spehner 1986

Classification of solutions of three-var equations (no constants):

$\mathcal{A}:\ h(x) = a,\ h(y) = b,\ h(z) = c$

$\mathcal{B}:\ h(x), h(y), h(z) \in a^*$

Budkina & Markov 1973; Spehner 1986

Classification of solutions of three-var equations (no constants):

$\mathcal{A}:\ h(x) = a,\ h(y) = b,\ h(z) = c$

$\mathcal{B}:\ h(x), h(y), h(z) \in a^*$

$\mathcal{C}:$ Let $i, j \geq 0$. Then $\mathcal{C}_{xyz}(i, j)$ is set of

$$h(x) = a, \qquad h(y) = a^i b a^j, \qquad h(z) \in \{a, b\}^*$$

where one of $h(y)$ and $h(z)$ begins (ends) with b.

Budkina & Markov 1973; Spehner 1986

Classification of solutions of three-var equations (no constants):

$\mathcal{A}:$ $h(x) = a,\ h(y) = b,\ h(z) = c$

$\mathcal{B}:$ $h(x), h(y), h(z) \in a^*$

$\mathcal{C}:$ Let $i, j \geq 0$. Then $\mathcal{C}_{xyz}(i, j)$ is set of

$$h(x) = a, \qquad h(y) = a^i b a^j, \qquad h(z) \in \{a, b\}^*$$

where one of $h(y)$ and $h(z)$ begins (ends) with b.

$\mathcal{D}:$ Let $i, j, k, \ell, m \geq 0$ and $ik = j\ell = 0$ and $p, q \geq 1$ and $\gcd(p+1, q+1) = 1$. Then $\mathcal{D}_{xyz}(i, j, k, \ell, m, p, q)$ is

$$h(x) = a, \qquad h(y) = a^i b (a^m b)^p a^j, \qquad h(z) = a^k b (a^m b)^q a^\ell.$$

Budkina & Markov 1973; Spehner 1986

Classification of solutions of three-var equations (no constants):

$\mathcal{A}$: $h(x) = a,\ h(y) = b,\ h(z) = c$

$\mathcal{B}$: $h(x), h(y), h(z) \in a^*$

$\mathcal{C}$: Let $i, j \geq 0$. Then $\mathcal{C}_{xyz}(i, j)$ is set of

$$h(x) = a, \qquad h(y) = a^i b a^j, \qquad h(z) \in \{a, b\}^*$$

where one of $h(y)$ and $h(z)$ begins (ends) with b.

$\mathcal{D}$: Let $i, j, k, \ell, m \geq 0$ and $ik = j\ell = 0$ and $p, q \geq 1$ and $\gcd(p+1, q+1) = 1$. Then $\mathcal{D}_{xyz}(i, j, k, \ell, m, p, q)$ is

$$h(x) = a, \qquad h(y) = a^i b (a^m b)^p a^j, \qquad h(z) = a^k b (a^m b)^q a^\ell.$$

Every strongly independent system of size N over three-variables (no constants) has a certificate in $(\mathcal{C} \cup \mathcal{D})^{N+1}$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \ldots E_N$ strongly independent system in three variables with a certificate $(h_1, \ldots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \ldots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \dots E_N$ strongly independent system in three variables with a certificate $(h_1, \dots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \dots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

- Let i, j s.t. $h_{N+1} \in \mathcal{C}_{xyz}(i, j)$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \ldots E_N$ strongly independent system in three variables with a certificate $(h_1, \ldots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \ldots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

- Let i, j s.t. $h_{N+1} \in \mathcal{C}_{xyz}(i,j)$
- Then $(h_1, \ldots h_N) \in \mathcal{C}_{xyz}(i,j)^N$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \dots E_N$ strongly independent system in three variables with a certificate $(h_1, \dots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \dots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

- Let i, j s.t. $h_{N+1} \in \mathcal{C}_{xyz}(i,j)$
- Then $(h_1, \dots h_N) \in \mathcal{C}_{xyz}(i,j)^N$

$$\alpha\colon \{x,y,z\}^* \to \{a,b,z\}^*,\ x \mapsto a,\ y \mapsto a^i b a^j,\ z \mapsto z$$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \ldots E_N$ strongly independent system in three variables with a certificate $(h_1, \ldots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \ldots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

- Let i, j s.t. $h_{N+1} \in \mathcal{C}_{xyz}(i,j)$
- Then $(h_1, \ldots h_N) \in \mathcal{C}_{xyz}(i,j)^N$

$$\alpha\colon \{x,y,z\}^* \to \{a,b,z\}^*,\ x \mapsto a,\ y \mapsto a^i b a^j,\ z \mapsto z$$

$$h'_n\colon \{a,b,z\}^* \to \{a,b\}^*,\ z \mapsto h_n(z) \quad \text{(const. preserving)}$$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{C}$)

Let $E_1, \dots E_N$ strongly independent system in three variables with a certificate $(h_1, \dots h_{N+1}) \in \mathcal{C}_{xyz}^{N+1}$.
There is a s. i. system $E'_1, \dots E'_N$ in one variable with $|E'_n| \leq |E_n|^2$.

- Let i, j s.t. $h_{N+1} \in \mathcal{C}_{xyz}(i,j)$
- Then $(h_1, \dots h_N) \in \mathcal{C}_{xyz}(i,j)^N$

$$\alpha\colon \{x,y,z\}^* \to \{a,b,z\}^*,\ x \mapsto a,\ y \mapsto a^i b a^j,\ z \mapsto z$$

$$h'_n\colon \{a,b,z\}^* \to \{a,b\}^*,\ z \mapsto h_n(z) \quad \text{(const. preserving)}$$

- Then $h_n = h'_n \circ \alpha$ and
- $\alpha(E_1), \dots \alpha(E_N)$ s. i. system in one-var, certificate $(h'_1, \dots h'_{N+1})$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Lemma ($\mathcal{D}$)

Let $E_1, \dots E_4$ strongly independent system in three variables with a certificate $(h_1, \dots h_5)$. Then at most one of the h_i can be in $\mathcal{D}_{xyz}$.

Strongly independent systems of 3-var equations w/o constants

From Lemmas $\mathcal{C}$ and $\mathcal{D}$ together with [Laine & Plandowski 2011] follows

Theorem

A strongly independent system of 3-var equations (no constants) has at most $16 \log n + \mathcal{O}(1)$ equations, where n is the length of the shortest equation.

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c + 9)$

Theorem

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c + 9)$.

(constants probably not optimal)

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Theorem

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$.

(constants probably not optimal)

- At most $c+1$ solutions in $\mathcal{C}_{xyz}$ by Lemma $\mathcal{C}$
- Considering all permutations of unknowns, then at most $6c+6$ in $\mathcal{C}$

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$

Theorem

SIND-XAB$(c) \Rightarrow$ SIND-XYZ$(6c+9)$.

(constants probably not optimal)

- At most $c+1$ solutions in $\mathcal{C}_{xyz}$ by Lemma $\mathcal{C}$
- Considering all permutations of unknowns, then at most $6c+6$ in $\mathcal{C}$
- At most one solution in $\mathcal{D}_{xyz}$ by Lemma $\mathcal{D}$
- Same for $\mathcal{D}_{yzx}$ and $\mathcal{D}_{zxy}$, giving three solutions in $\mathcal{D}$

Conclusion

- SOL-XAB$(c) \Rightarrow$ SIND-XAB$(c) \begin{cases} \Leftarrow \text{SIND-XYZ}(c) \\ \Rightarrow \text{SIND-XYZ}(6c+9) \end{cases}$
- Size of strongly independent systems in three-vars is in $\mathcal{O}(\log n)$