Algebraic Properties of Word Equations

Štěpán Holub

March 9, 2016

Charles University, Prague

Outline

- Historical excursus
  - Fine and Wilf theorem (two original but less known proofs)
  - Compactness property of systems of word equations
- Encoding of word equations into polynomials

  [including a commercial break]

Fine and Wilf: The Periodicity Lemma, Proof 1

Theorem

Let $\{f_n\}_0^\infty$ and $\{g_n\}_0^\infty$ be two periodic sequences of periods h and k, respectively. If $f_n = g_n$ for $h + k - (h, k)$ consecutive integers n, then $f_n = g_n$ for all n. The result would be false if $h + k - (h, k)$ were replaced by anything smaller.

Fine and Wilf: The Periodicity Lemma, Proof 1

Theorem

Let $\{f_n\}_0^\infty$ and $\{g_n\}_0^\infty$ be two periodic sequences of periods h and k, respectively. If $f_n = g_n$ for $h + k - (h, k)$ consecutive integers n, then $f_n = g_n$ for all n. The result would be false if $h + k - (h, k)$ were replaced by anything smaller.

Proof.

Use discrete Fourier bases of functions with the period k and h:

$$\begin{aligned} \Psi : &\qquad \psi_j(n) = e^{2\pi i \frac{j}{k} n}, &\qquad j = 0, 1, \ldots, k-1, \\ \Phi : &\qquad \phi_j(n) = e^{2\pi i \frac{j}{h} n}, &\qquad j = 0, 1, \ldots, h-1. \end{aligned}$$

There are altogether $h + k - (h, k)$ linearly independent elements in $\Psi \cup \Phi$. Therefore the interpolation of the shared interval is unique iff it is of at least that length (with the support in $\Psi \cap \Phi$). $\square$

Fine and Wilf: The Periodicity Lemma, Proof 2

Theorem

Let $\{f_n\}_0^\infty$ and $\{g_n\}_0^\infty$ be two periodic sequences of periods h and k, respectively. If $f_n = g_n$ for $h + k - (h, k)$ consecutive integers n, then $f_n = g_n$ for all n. The result would be false if $h + k - (h, k)$ were replaced by anything smaller.

Fine and Wilf: The Periodicity Lemma, Proof 2

Theorem

Let $\{f_n\}_0^\infty$ and $\{g_n\}_0^\infty$ be two periodic sequences of periods h and k, respectively. If $f_n = g_n$ for $h + k - (h,k)$ consecutive integers n, then $f_n = g_n$ for all n. The result would be false if $h + k - (h,k)$ were replaced by anything smaller.

Proof.

$$F(x) = \sum_0^\infty f_n x^n = \frac{P(x)}{1 - x^h} \qquad G(x) = \sum_0^\infty g_n x^n = \frac{Q(x)}{1 - x^k}$$

$$F(x) - G(x) = \frac{P(x)(1 - x^k)/\left(1 - x^{(h,k)}\right) - Q(x)(1 - x^h)/\left(1 - x^{(h,k)}\right)}{(1 - x^h)(1 - x^k)/\left(1 - x^{(h,k)}\right)}$$

$\square$

Compactness property

- **Theorem (Compactness property)**
  Every infinite system of equations in finitely many unknowns is equivalent to a finite subsystem.

- **Theorem (Compactness property)**

  Every infinite system of equations in finitely many unknowns is equivalent to a finite subsystem.

  Easily equivalent (1980) to “Eherenfeucht’s conjecture”
  (beginning of 1970s - Nowa Księga Szkocka, problem 105)

- **Theorem**

  Every language over a finite alphabet has a finite test set (testing equality of morphisms on the language).

  - Proved independently by Albert & Lawrence (1985); and Guba (1986).
  - Core of both proofs: Hilbert’s basis theorem.

Compactness

$$\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \mathrm{SL}_2(\mathbb{N}_0) = \langle \mathbf{a}, \mathbf{b} \rangle \cong \{a, b\}^*$$

$$\mathbf{c} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{d} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \qquad \langle \mathbf{c}, \mathbf{d} \rangle \cong F_2$$

Compactness

$$\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \mathrm{SL}_2(\mathbb{N}_0) = \langle \mathbf{a}, \mathbf{b} \rangle \cong \{a, b\}^*$$

$$\mathbf{c} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{d} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \langle \mathbf{c}, \mathbf{d} \rangle \cong F_2$$

$$x_j \mapsto m_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$$

$$\begin{tikzcd} \Theta^* \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & M \arrow[dl, "\tilde{\varphi}"] \\ & \mathrm{SL}_2(\mathbb{N}_0) & \end{tikzcd}$$

Compactness

$$xyz = zyx$$

$$x \mapsto \begin{pmatrix} a_x & b_x \\ c_x & d_x \end{pmatrix} \quad y \mapsto \begin{pmatrix} a_y & b_y \\ c_y & d_y \end{pmatrix} \quad z \mapsto \begin{pmatrix} a_z & b_z \\ c_z & d_z \end{pmatrix}$$

$$a_z b_x c_y + a_x b_y c_z + b_x c_z d_y = a_z b_y c_x + a_x b_z c_y + b_z c_x d_y$$

$$a_x a_y b_z + a_x b_y d_z + b_x d_y d_z = a_y a_z b_x + a_z b_y d_x + b_z d_x d_y$$

$$a_y a_z c_x + a_x c_y d_x + c_z d_x d_y = a_x a_y c_z + a_x c_y d_z + c_x d_y d_z$$

$$a_y b_z c_x + b_z c_y d_x + b_y c_x d_z = a_y b_x c_z + b_y c_z d_x + b_x c_y d_z$$

$$a_x d_x - b_x c_x = 1$$

$$a_y d_y - b_y c_y = 1$$

$$a_z d_z - b_z c_z = 1$$

What is the size of the equivalent subsystem?

- The system is independent if it has no equivalent subsystem.

What is the size of the equivalent subsystem?

- The system is independent if it has no equivalent subsystem.
- Big open question

  Is the size of an independent system of equations over n unknowns bounded?

What is the size of the equivalent subsystem?

- The system is independent if it has no equivalent subsystem.
- Big open question

  Is the size of an independent system of equations over n unknowns bounded?
- Open already for three unknows (trivial for two).

What is the size of the equivalent subsystem?

- The system is independent if it has no equivalent subsystem.
- Big open question
  Is the size of an independent system of equations over n unknowns bounded?
- Open already for three unknows (trivial for two).
- Unbounded in free groups.
- Lower bound $\Omega(n^4)$ (explicit system by Karhumäki and Plandowski 1996, Karhumäki and Saarela 2011).

Bounds on the size of independent systems for three unknowns

Bounds on the size of independent systems for three unknowns

Let $E_1, \dots, E_m$, $m \geq 2$, be an independent system of equations in three unknowns having a nonperiodic solution.

- Aleksi Saarela, Systems of word equations, polynomials and linear algebra: A new approach, European J. Combin. 2015

  $m \leq (|E_1|_x + |E_1|_y)^2 + 1$ for some pair x, y of unknowns.

Bounds on the size of independent systems for three unknowns

Let $E_1, \ldots, E_m$, $m \geq 2$, be an independent system of equations in three unknowns having a nonperiodic solution.

- Aleksi Saarela, Systems of word equations, polynomials and linear algebra: A new approach, European J. Combin. 2015

  $m \leq (|E_1|_x + |E_1|_y)^2 + 1$ for some pair x, y of unknowns.

- ŠH, Jan Žemlička, Algebraic properties of word equations, Journal of Algebra 2015

  $m \leq 2(|E_1|_x + |E_1|_y) + 1$ for any pair x, y of unknowns.

Representation by polynomials

Let the alphabet A be a subset of $\mathbb{N}_0$, and let unknowns be $\Theta = \{x, y, z\}$.

$$P : A^* \to \mathbb{N}_0[\alpha]$$
$$a_0 a_1 a_2 \cdots a_n \mapsto a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

Representation by polynomials

Let the alphabet A be a subset of $\mathbb{N}_0$, and let unknowns be $\Theta = \{x, y, z\}$.

$$P : A^* \to \mathbb{N}_0[\alpha]$$
$$a_0 a_1 a_2 \cdots a_n \mapsto a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

For a morphism $\varphi : \Theta^* \to A^*$, let

$$\mathscr{P}(\varphi) = (P(\varphi(x)), P(\varphi(y)), P(\varphi(z))) \in \mathbb{Q}(\alpha)^3$$

Representation by polynomials

$$S : E \times \{x, y, z\} \to \mathbb{Z}[X, Y, Z]$$

$$E : (xyyz, zyyx)$$

$$S_{E,x} = 1 - ZY^2$$

$$S_{E,y} = X + XY - Z - ZY$$

$$S_{E,z} = XY^2 - 1$$

$$\mathscr{S}_E = (S_{E,x}, S_{E,y}, S_{E,z}) \in \mathbb{Q}(X, Y, Z)^3$$

Representation by polynomials

$$S : E \times \{x, y, z\} \to \mathbb{Z}[X, Y, Z]$$

$$E : (xyyz, zyyx)$$

$$S_{E,x} = 1 - ZY^2$$

$$S_{E,y} = X + XY - Z - ZY$$

$$S_{E,z} = XY^2 - 1$$

$$\mathscr{S}_E = (S_{E,x}, S_{E,y}, S_{E,z}) \in \mathbb{Q}(X, Y, Z)^3$$

Length type $L = (L_x, L_y, L_z) \in \mathbb{N}_0^3$.

Representation by polynomials

$$S : E \times \{x, y, z\} \to \mathbb{Z}[X, Y, Z]$$

$$E : (xyyz, zyyx)$$

$$S_{E,x} = 1 - ZY^2$$

$$S_{E,y} = X + XY - Z - ZY$$

$$S_{E,z} = XY^2 - 1$$

$$\mathscr{S}_E = (S_{E,x}, S_{E,y}, S_{E,z}) \in \mathbb{Q}(X, Y, Z)^3$$

Length type $L = (L_x, L_y, L_z) \in \mathbb{N}_0^3$. Define $\mathscr{S}_E(L)$ by morphism

$$\Omega_L : \mathbb{Z}[X, Y, Z] \to \mathbb{Q}(\alpha)$$

$$X \mapsto \alpha^{L_x} \quad Y \mapsto \alpha^{L_y} \quad Z \mapsto \alpha^{L_z}$$

Representation by polynomials

φ with $L(\varphi) = \{|\varphi(x)|, |\varphi(y)|, |\varphi(z)|\}$ is a solution of E

if and only if

$$\mathscr{S}_E(L(\varphi)) \cdot \mathscr{P}(\varphi) = 0\,.$$

Representation by polynomials: Example (by Dirk Nowotka)

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

Representation by polynomials: Example (by Dirk Nowotka)

$$E_1 :(xyzz, zzxy)$$
$$E_2 :(xyxzz, zzxxy)$$

φ_i: a solution of the system without equation E_i

$$\begin{array}{llll} \varphi_\emptyset : & x \mapsto a & y \mapsto bab & z \mapsto ab \\ \varphi_1 : & x \mapsto a & y \mapsto babaabab & z \mapsto ab \\ \varphi_2 : & x \mapsto a & y \mapsto babab & z \mapsto ab \end{array}$$

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

If a common non-periodic solution φ, then $\mathscr{S}_{E_1}(L(\varphi))$ and $\mathscr{S}_{E_2}(L(\varphi))$ are linearly dependent over $\mathbb{Q}(\alpha)$.

$$E_1 :(xyzz, zzxy)$$
$$E_2 :(xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

If a common non-periodic solution φ, then $\mathscr{S}_{E_1}(L(\varphi))$ and $\mathscr{S}_{E_2}(L(\varphi))$ are linearly dependent over $\mathbb{Q}(\alpha)$.

$$\varphi_\emptyset : \quad x \mapsto a \quad y \mapsto bab \quad z \mapsto ab$$
$$\mathscr{P}(\varphi) = (a, b + a\alpha + b\alpha^2, a + b\alpha)$$
$$\mathscr{P}(\varphi) = (1, \alpha, 1) \qquad \mathscr{P}(\varphi) = (0, 1 + \alpha^2, \alpha)$$

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

$$L(\varphi) = (1, 3, 2)$$
$$\mathscr{P}(\varphi) = (1, \alpha, 1) \qquad \mathscr{P}(\varphi) = (0, 1 + \alpha^2, \alpha)$$

$$\mathscr{S}_{E_1}(L(\varphi)) = (1 - \alpha^4, \alpha - \alpha^5, \alpha^4 + \alpha^6 - 1 - \alpha^2)$$
$$\mathscr{S}_{E_2}(L(\varphi)) = (1 - \alpha^5, \alpha - \alpha^6, \alpha^5 + \alpha^7 - 1 - \alpha^2)$$

$$\mathscr{S}_{E_2}(L(\varphi)) = \frac{1 - \alpha^5}{1 - \alpha^4} \cdot \mathscr{S}_{E_1}(L(\varphi))$$

$$E_1 :(xyzz, zzxy)$$
$$E_2 :(xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

GCD of all three 2×2 minors is

$$\tau(E_1, E_2) = X(1 + Z)(XY - Z^2).$$

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

GCD of all three 2×2 minors is

$$\tau(E_1, E_2) = X(1 + Z)(XY - Z^2).$$

$$\Omega_L : \quad X \mapsto \alpha^{L_x} \qquad Y \mapsto \alpha^{L_y} \qquad Z \mapsto \alpha^{L_z}$$

$$
\begin{aligned}
E_1 &: (xyzz, zzxy) \\
E_2 &: (xyxzz, zzxxy)
\end{aligned}
$$

$$
\begin{aligned}
\mathscr{S}_{E_1} &= (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z) \\
\mathscr{S}_{E_2} &= (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)
\end{aligned}
$$

GCD of all three 2×2 minors is

$$
\tau(E_1, E_2) = X(1 + Z)(XY - Z^2).
$$

$$
\Omega_L : \quad X \mapsto \alpha^{L_x} \qquad Y \mapsto \alpha^{L_y} \qquad Z \mapsto \alpha^{L_z}
$$

For what L, the polynomial τ vanishes under the mapping Ω_L?

$$E_1 : (xyzz, zzxy)$$
$$E_2 : (xyxzz, zzxxy)$$

$$\mathscr{S}_{E_1} = (1 - Z^2, X - XZ^2, XY + XYZ - 1 - Z)$$
$$\mathscr{S}_{E_2} = (1 + XY - Z^2 - XZ^2, X - X^2Z^2, X^2Y + X^2YZ - 1 - Z)$$

GCD of all three 2×2 minors is

$$\tau(E_1, E_2) = X(1 + Z)(XY - Z^2).$$

$$\Omega_L : \quad X \mapsto \alpha^{L_x} \qquad Y \mapsto \alpha^{L_y} \qquad Z \mapsto \alpha^{L_z}$$

For what L, the polynomial τ vanishes under the mapping Ω_L?

$$L_x + L_y = 2L_z$$
$$|\varphi(x)| + |\varphi(y)| = 2|\varphi(z)|$$

Prize problem

I will pay **200 €** to the first person who gives the answer (with a proof) to the following question:

Is there a positive integer $n \geq 2$ and words $u_1, u_2, \ldots, u_n$ such that both equalities

$$\begin{cases} (u_1 u_2 \cdots u_n)^2 = u_1^2 u_2^2 \cdots u_n^2, \\ (u_1 u_2 \cdots u_n)^3 = u_1^3 u_2^3 \cdots u_n^3, \end{cases}$$

hold and the words u_i, $i = 1, \ldots, n$, do not pairwise commute (that is, $u_i u_j \neq u_j u_i$ for at least one pair of indices $i, j \in \{1, 2, \ldots, n\}$)?

Linear spaces of length types

Length types are not individuals; they form cones of dimension equal to the rank of the solution.

$$\varphi_\emptyset : \quad x \mapsto a \quad y \mapsto bab \quad z \mapsto ab$$

Linear spaces of length types

Length types are not individuals; they form cones of dimension equal to the rank of the solution.

$$\varphi_\emptyset : \quad x \mapsto a \quad y \mapsto bab \quad z \mapsto ab$$

$$\vartheta_{k,\ell} : \quad a \mapsto a^k \quad b \mapsto b^\ell$$

Linear spaces of length types

Length types are not individuals; they form cones of dimension equal to the rank of the solution.

$$\varphi_\emptyset : \quad x \mapsto a \quad y \mapsto bab \quad z \mapsto ab$$

$$\vartheta_{k,\ell} : \quad a \mapsto a^k \quad b \mapsto b^\ell$$

Length types of solutions

$$\mathscr{L} = \{L(\vartheta_{k,\ell} \circ \varphi_\emptyset) \mid k, \ell \in \mathbb{N}\}$$

form a lattice in

$$\langle (1,1,1), (0,2,1) \rangle_{\mathbb{Q}} .$$

Vectors $\mathscr{S}_{E_1}(L)$ and $\mathscr{S}_{E_1}(L)$ are linearly dependent (i.e. the GCD of minors vanishes) for all $L \in \mathscr{L}$.

Linear spaces of length types

Length types of solutions

$$\mathscr{L} = \{L(\vartheta_{k,\ell} \circ \varphi_\emptyset) \mid k, \ell \in \mathbb{N}\}$$

form a lattice in

$$\langle (1,1,1), (0,2,1) \rangle_{\mathbb{Q}} \,.$$

Vectors $\mathscr{S}_{E_1}(L)$ and $\mathscr{S}_{E_1}(L)$ are linearly dependent (i.e. the GCD of minors vanishes) for all $L \in \mathscr{L}$.

Linear spaces of length types

Length types of solutions

$$\mathscr{L} = \{L(\vartheta_{k,\ell} \circ \varphi_\emptyset) \mid k, \ell \in \mathbb{N}\}$$

form a lattice in

$$\langle (1,1,1), (0,2,1) \rangle_{\mathbb{Q}} .$$

Vectors $\mathscr{S}_{E_1}(L)$ and $\mathscr{S}_{E_1}(L)$ are linearly dependent (i.e. the GCD of minors vanishes) for all $L \in \mathscr{L}$.

Lemma

Let $\lambda \in \mathbb{Z}^n \setminus \{0\}$ have coprime coefficients and let $N \subseteq \mathcal{N}(\lambda)$ be of rank $n-1$. Then $p \in \mathbb{Z}[\mathbf{X}]$ satisfies $\Omega_L(p) = 0$ for all $L \in N$ if and only if $\left(\mathbf{X}^{\lambda_\oplus} - \mathbf{X}^{\lambda_\ominus}\right) \mid p$.

Linear spaces of length types

Length types of solutions

$$\mathscr{L} = \{L(\vartheta_{k,\ell} \circ \varphi_\emptyset) \mid k, \ell \in \mathbb{N}\}$$

form a lattice in

$$\langle (1,1,1), (0,2,1) \rangle_{\mathbb{Q}} .$$

Vectors $\mathscr{S}_{E_1}(L)$ and $\mathscr{S}_{E_1}(L)$ are linearly dependent (i.e. the GCD of minors vanishes) for all $L \in \mathscr{L}$.

Lemma

Let $\lambda \in \mathbb{Z}^n \setminus \{0\}$ have coprime coefficients and let $N \subseteq \mathcal{N}(\lambda)$ be of rank $n-1$. Then $p \in \mathbb{Z}[\mathbf{X}]$ satisfies $\Omega_L(p) = 0$ for all $L \in N$ if and only if $\left(\mathbf{X}^{\lambda_\oplus} - \mathbf{X}^{\lambda_\ominus}\right) \mid p$.

$$\lambda = (1,1,-2) \quad \lambda_\oplus = (1,1,0) \quad \lambda_\ominus = (0,0,2) \quad (XY - Z^2)$$

The bound

Each independent equation E_i needs its own hyperplane of types for the solution φ_i.

The bound

Each independent equation E_i needs its own hyperplane of types for the solution φ_i.

How many distinct monomials $\left(\mathbf{X}^{\lambda_\oplus} - \mathbf{X}^{\lambda_\ominus}\right)$ can divide $\tau(E_1, E_2)$?

The bound

Each independent equation E_i needs its own hyperplane of types for the solution φ_i.

How many distinct monomials $\left(\mathbf{X}^{\lambda_\oplus} - \mathbf{X}^{\lambda_\ominus}\right)$ can divide $\tau(E_1, E_2)$?

special form of $\mathscr{S}_E$

$\Downarrow$

special form of τ

$\Downarrow$

bound on the number of minimal mononomials in τ

$\Downarrow$

bound on the number of mononomials $\left(\mathbf{X}^{\lambda_\oplus} - \mathbf{X}^{\lambda_\ominus}\right)$ dividing τ

Outlook

- Exploit better the special form of τ to improve the bound.
- Generalize the approach for all ranks, not just $n-1$.