Solving word equations

Štěpán Holub

Department of Algebra
MFF UK, Prague

Prague Gathering of Logicians, February 13, 2016

Outline

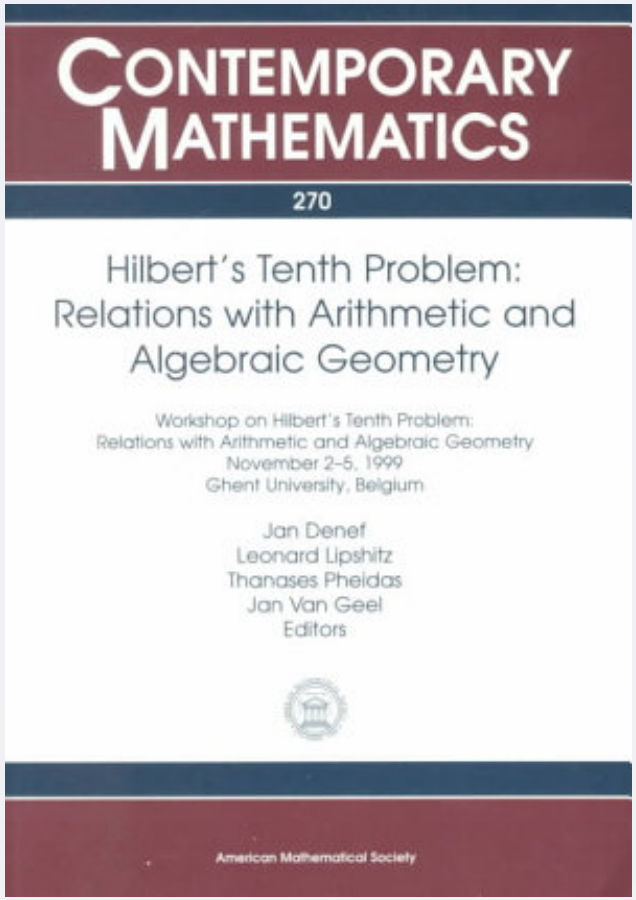
- Algorithms
- Compactness
- Independent systems and their size

Outline

- Algorithms
- Compactness
- Independent systems and their size

(running background question: combinatorics or algebra?)

Decidable?


CONTEMPORARY MATHEMATICS
270
Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry
Workshop on Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry November 2-5, 1999 Ghent University, Belgium
Jan Denef
Leonard Lipshitz
Thanases Pheidas
Jan Van Geel
Editors
American Mathematical Society

Decidable?

end of 1965. At that time he believed that the approach of Davis, Putnam and Robinson could not lead to a solution because it had not already done so. Instead Maslov suggested to me to try another approach advocated by A. A. Markov.

The idea was as follows. After pioneering result of Markov and Post about Thue problem, many other decision problems about words were also shown undecidable. There are many ways to represent words by numbers. One of such methods is naturally related to Diophantine equations. Namely, it is not difficult to show that every 2×2 matrix

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \tag{38}$$

with the m's being natural numbers and the determinant equal to 1, can be represented, in an unique way, as a product of matrices

$$M_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{39}$$

It is evident that any product of such matrices has natural number elements and the determinant equal to 1. This implies that we can uniquely represent a word $a_{i_1} \dots a_{i_m}$ in a two-letter alphabet $\{a_0, a_1\}$ by the four-tuple $\langle m_{11}, m_{12}, m_{21}, m_{22} \rangle$ such that

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = M_{i_1} \dots M_{i_m}. \tag{40}$$

Clearly, these numbers satisfy the Diophantine equation

$$m_{11}m_{22} - m_{21}m_{12} = 1 \tag{41}$$

and, vice versa, for every four numbers $m_{11}, m_{12}, m_{21}, m_{22}$ satisfying (41) there is unique word $a_{i_1} \dots a_{i_m}$ for which (40) holds.

Under this representation of words by matrices, the concatenation of words corresponds to matrix multiplication and thus can be easily expressed by a system of Diophantine equations. This opens a way of transforming an arbitrary system of *word equations* into an equivalent system of Diophantine equations. A quite natural way to attack Hilbert's tenth problem would be by proving the undecidability of systems of word equations.

I spent some time trying to do this. Much later it became known that this approach was fruitless because G. S. Makanin [**42**] found an algorithm for word equations. Luckily, I soon abandoned this approach.

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)
- Joxan Jaffar, Minimal and complete word unification. *J. ACM*, 1990 (4-NEXPTIME, all solutions)

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)
- Joxan Jaffar, Minimal and complete word unification. *J. ACM*, 1990 (4-NEXPTIME, all solutions)
- Klaus U. Schulz, Makanin's Algorithm for Word Equations - Two Improvements and a Generalization. IWWERT 1990

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)
- Joxan Jaffar, Minimal and complete word unification. *J. ACM*, 1990 (4-NEXPTIME, all solutions)
- Klaus U. Schulz, Makanin's Algorithm for Word Equations - Two Improvements and a Generalization. IWWERT 1990
- Antoni Kościelski and Leszek Pacholski, Complexity of Makanins algorithm. *J. ACM*, 1996 (3-NEXPTIME)

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)
- Joxan Jaffar, Minimal and complete word unification. *J. ACM*, 1990 (4-NEXPTIME, all solutions)
- Klaus U. Schulz, Makanin's Algorithm for Word Equations - Two Improvements and a Generalization. IWWERT 1990
- Antoni Kościelski and Leszek Pacholski, Complexity of Makanins algorithm. *J. ACM*, 1996 (3-NEXPTIME)
- Claudio Gutiérrez, Satisfiability of word equations with constants is in exponential space. *FOCS*, 1998 (EXPSPACE)

Makanin's algorithm

- G. S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.*, 1977 (6-NEXPTIME ?)
- Joxan Jaffar, Minimal and complete word unification. *J. ACM*, 1990 (4-NEXPTIME, all solutions)
- Klaus U. Schulz, Makanin's Algorithm for Word Equations - Two Improvements and a Generalization. IWWERT 1990
- Antoni Kościelski and Leszek Pacholski, Complexity of Makanins algorithm. *J. ACM*, 1996 (3-NEXPTIME)
- Claudio Gutiérrez, Satisfiability of word equations with constants is in exponential space. *FOCS*, 1998 (EXPSPACE)
- Volker Diekert, Makanin's algorithm. In *Algebraic Combinatorics on Words*, 2002 (rational constraints)

Some ideas : Length type

$$xay = zbzb$$

Some ideas : Length type

$$xay = zbzb$$

$$(|x|, |y|, |z|) = (1, 4, 2)$$

Some ideas : Length type

$$xay = zbzb$$

$$(|x|, |y|, |z|) = (1, 4, 2)$$

x_1	a	y_1	y_2	y_3	y_4
z_1	z_2	b	z_1	z_2	b

Some ideas : Length type

$$xay = zbzb$$

$$(|x|, |y|, |z|) = (1, 4, 2)$$

x_1	a	y_1	y_2	y_3	y_4
z_1	z_2	b	z_1	z_2	b

Some ideas : Length type

$$xay = zbzb$$

$$(|x|, |y|, |z|) = (1, 4, 2)$$

x_1	a	y_1	y_2	y_3	y_4
z_1	z_2	b	z_1	z_2	b

$$x \mapsto a$$
$$y \mapsto baab$$
$$z \mapsto aa$$

Some ideas : Elementary transformations

$$xay = zbzb$$

Some ideas : Elementary transformations

$$xay = zbzb$$

$$|x| < |z|$$

Some ideas : Elementary transformations

$$xay = zbzb$$

$$|x| < |z|$$

$$z \mapsto xz$$

Some ideas : Elementary transformations

$$xay = zbzb$$

$$|x| < |z|$$

$$z \mapsto xz$$

$$xay = xzbxzb$$

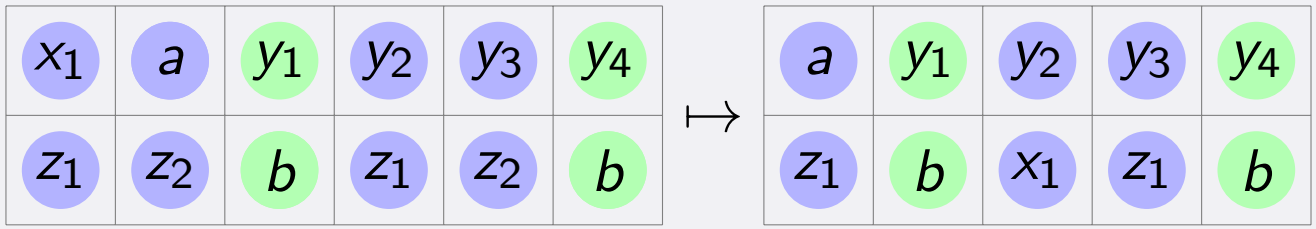
Some ideas : Elementary transformations

$$xay = zbzb$$

$$|x| < |z|$$

$$z \mapsto xz$$

$$xay = xzbxzb$$



Bound on the exponent of periodicity

$$\phi(u) = \phi(v) = pw^e s$$

Bound on the exponent of periodicity

$$\phi(u) = \phi(v) = pw^e s$$

- Makanin: double exponential

Bound on the exponent of periodicity

$$\phi(u) = \phi(v) = pw^e s$$

- Makanin: double exponential
- Kościelski and Pacholski: $\mathcal{O}(2^{1.07d})$

Different concept of transformations: Compression

- Wojciech Plandowski, Wojciech Rytter, Application of Lempel-Ziv encodings to the solution of word equations. *ICALP* 1998

Different concept of transformations: Compression

- Wojciech Plandowski, Wojciech Rytter, Application of Lempel-Ziv encodings to the solution of word equations. *ICALP* 1998
- Wojciech Plandowski, Satisfiability of word equations with constants is in NEXPTIME. *STOC* 1999.

Different concept of transformations: Compression

- Wojciech Plandowski, Wojciech Rytter, Application of Lempel-Ziv encodings to the solution of word equations. *ICALP* 1998
- Wojciech Plandowski, Satisfiability of word equations with constants is in NEXPTIME. *STOC* 1999.
- Wojciech Plandowski, Satisfiability of word equations with constants is in PSPACE. *J. ACM* 2004.

Different concept of transformations: Compression

- Wojciech Plandowski, Wojciech Rytter, Application of Lempel-Ziv encodings to the solution of word equations. *ICALP* 1998
- Wojciech Plandowski, Satisfiability of word equations with constants is in NEXPTIME. *STOC* 1999.
- Wojciech Plandowski, Satisfiability of word equations with constants is in PSPACE. *J. ACM* 2004.
- Wojciech Plandowski, An efficient algorithm for solving word equations. *STOC*, 2006. (Graph representing all solutions)

Lempel - Ziv compression

aacaacabcabaaac

(0,0,a)
(1,1,c)
(3,4,b)
(3,3,a)
(12,3,$)

Lempel - Ziv compression

aacaacabcabaaac

(0,0,a)
(1,1,c)
(3,4,b)
(3,3,a)
(12,3,$)

$xay = zbzb$

Artur Jeż: Recompression

- Approximation of Grammar-Based Compression via Recompression. CPM 2013
- Artur Jeż, Recompression: a simple and powerful technique for word equations. *STACS* 2013.
- Recompression: Word Equations and Beyond. Developments in Language Theory 2013
- The Complexity of Compressed Membership Problems for Finite Automata. Theory Comput. Syst. 2014
- Approximation of grammar-based compression via recompression. Theor. Comput. Sci. 2015
- Faster Fully Compressed Pattern Matching by Recompression. ACM Transactions on Algorithms 2015
- One-Variable Word Equations in Linear Time. Algorithmica 2016

Artur Jeż: Recompression

- Guess letters at the beginning and the end of variables
- Compress chosen pairs of letters

Artur Jeż: Recompression

- Guess letters at the beginning and the end of variables
- Compress chosen pairs of letters

$$xay = zbzb$$

Artur Jeż: Recompression

- Guess letters at the beginning and the end of variables
- Compress chosen pairs of letters

$$xay = zbzb$$
$$bxbaayb = azbbazb$$

Artur Jeż: Recompression

- Guess letters at the beginning and the end of variables
- Compress chosen pairs of letters

$$xay = zbzb$$
$$bxbaayb = azbbazb$$
$$bxbaayb = azbbazb$$

Artur Jeż: Recompression

- Guess letters at the beginning and the end of variables
- Compress chosen pairs of letters

$$xay = zbzb$$
$$bxbaayb = azbbazb$$
$$bxbaayb = azbbazb$$
$$bxcayb = azbczb$$

General strategy of all algorithms

- Transformation rules (non-deterministic)
  - boundary equations (Makanin)
  - exponential expressions (Plandowski)
  - ordinary equations (Jeż)
- Terminating condition based on bounds on
  - length of the minimal solution
  - size of the transformed equation

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

length of the minimal solution: $N < 2^{q(n)\cdot n_v^{cn_V}}$

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

length of the minimal solution: $N < 2^{q(n)\cdot n_v^{cn_V}}$

NTIME: $\mathcal{O}(\log N \ \mathtt{poly}(n))$

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

length of the minimal solution: $N < 2^{q(n)\cdot n_v^{cn_V}}$

NTIME: $\mathcal{O}(\log N \ \mathtt{poly}(n))$

SPACE: $\mathcal{O}(n \log n)$

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

length of the minimal solution: $N < 2^{q(n)\cdot n_v^{cn_V}}$

NTIME: $\mathcal{O}(\log N \ \mathtt{poly}(n))$

SPACE: $\mathcal{O}(n \log n)$

NP hard (e.g. easy reduction of 3SAT)

Current knowledge

exponent of periodicity: $\mathcal{O}(2^{cn})$ (tight)

length of the minimal solution: $N < 2^{q(n)\cdot n_v^{cn_V}}$

NTIME: $\mathcal{O}(\log N \ \mathtt{poly}(n))$

SPACE: $\mathcal{O}(n \log n)$

NP hard (e.g. easy reduction of 3SAT)

NP complete ?

Compactness property

Compactness property

- System S is equivalent to T if and only if they have the same set of solutions.

Compactness property

- System S is equivalent to T if and only if they have the same set of solutions.

- Theorem (Compactness property)

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

Compactness property

- System S is equivalent to T if and only if they have the same set of solutions.

- **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).

Compactness property

- System S is equivalent to T if and only if they have the same set of solutions.

- 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

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

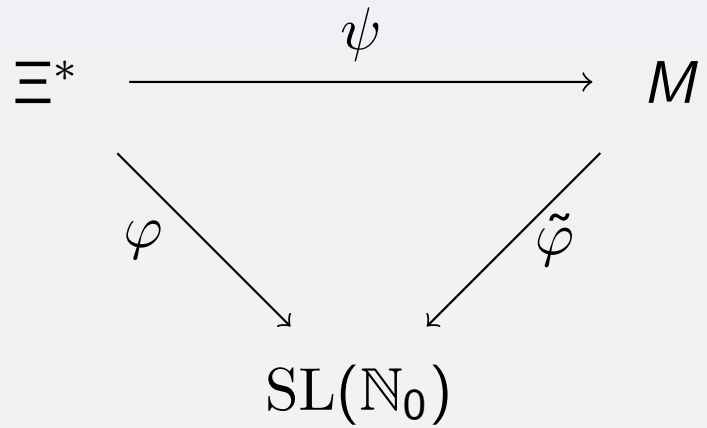
$$\mathbf{c} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{d} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \qquad \langle \mathbf{c}, \mathbf{d} \rangle \cong F_2$$

Compactness

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

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

$$x_j \mapsto m_j = \begin{pmatrix} a^{(j)} & b^{(j)} \\ c^{(j)} & d^{(j)} \end{pmatrix}$$



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?

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 (three-generated free group does not satisfy Ascending Chain Condition for normal subgroups).
- Lower bound $\Omega(n^4)$ (explicit system by Karhumäki and Plandowski, 1996).

Bounds on the size of independent systems for three 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.

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.

- Š. H., Jan Žemlička, Algebraic properties of word equations, Journal of Algebra 2015

1. $m \leq 2(|E_1|_x + |E_1|_y) + 1$ for any pair x, y of unknowns, and
2. $m \leq |E_1| + |E_2| + 1$.

Representation by polynomials

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

$$P : A^* \to \mathbb{N}[\alpha]$$

$$a_0 a_1 a_2 \cdots a_n \mapsto a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

Representation by polynomials

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

$$P : A^* \to \mathbb{N}[\alpha]$$

$$a_0 a_1 a_2 \cdots a_n \mapsto a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

For a morphism $h : \Xi^* \to A^*$, let

$$\mathcal{P}(h) = (P(h(x)), P(h(y)), P(h(z)))$$

Representation by polynomials

$$S : E \times \{x, y, z\} \to \mathbb{Z}[X, Y, Z]$$
$$E : (xyyz, zyyx)$$
$$S_{E,x} = 1 - ZY^2$$
$$S_{E,y} = X + XY - Z - ZY$$
$$S_{E,z} = XY^2 - 1$$
$$\mathcal{S}_E = (S_{E,x}, S_{E,y}, S_{E,z})$$

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

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

Representation by polynomials

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

if and only if

$$\mathcal{S}_E(L(h)) \cdot \mathcal{P}(h) = 0\,.$$

Representation by polynomials: Example

$$E_1 : (xyz, zyx)$$
$$E_2 : (xyyz, zyyx)$$

$$\mathcal{S}_{E_1} = (1 - ZY, X - Z, XY - 1)$$
$$\mathcal{S}_{E_2} = (1 - ZY^2, X + XY - Z - ZY, XY^2 - 1)$$

If a common non-periodic solution has a length type L, then $\mathcal{S}_{E_1}(L)$ and $\mathcal{S}_{E_2}(L)$ are linearly dependent.
This means that the determinant $Y(X - Z)$ must vanish under the substitution. Therefore $|x| = |z|$.

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 $i, j \in \{1, 2, \ldots, n\}$)?