Complexity of linear algebra problems

Victor Kac

MIT

Sensational news shook the mathematical world on September 6, 2019:

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3.$$

This formula was established with the help of 500000 computers!

This equation is an example of **Hilbert's problem H10** (1900).

Provide a general algorithm, which, for any given Diophantine equation (a polynomial equation with integer coefficients and a finite number of unknowns), can ***decide*** *whether the equation has a solution with all unknowns taking integer values.*

Matijasevich Theorem (1970): THERE IS NO SUCH ALGORITM.

Example 1 Equation $x^2 + y^2 + z^2 = n$ is **decidable**, since, by the Legendre theorem it has a solution in integers if and only if $n \geq 0$ and $n \not\equiv 7 \bmod 8$

Example 2 Is equation $x^3 + y^3 + z^3 = n$ decidable?

Easy fact: If $n \equiv 4$ or $\equiv 5 \bmod 9$, it has no solutions.
Proof $k^3 \equiv 0$ or $\pm 1 \bmod 9$ for any integer k. □

Open Problem: It has a solution otherwise.

42 was the last integer ≤ 100 for which it wasn't known until September 6, 2019.

Proof of this problem would imply that this equation is decidable.

What if, instead of integers, one considers a finite field $\mathbb{F}_q$ in H10?

Example of a finite field $\mathbb{F}_2 = \{0, 1\}$,

$$0 \cdot 0 = 0 \cdot 1 = 0,\ 1 \cdot 1 = 1; \qquad 0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 1 = 0.$$

Then H10 is obviously **decidable**.

The next question: Is this problem “quickly” decidable, i.e. decidable in polynomial (in the data) time?

Answer unknown.

However, on can verify in polynomial time whether the given values of unknowns in $\mathbb{F}_q$ is a solution.

Definition

One says that a decision problem is in P if it can be solved in polynomial time, and it is in NP if its solution can be verified in polynomial time.

Easy fact: $P \Rightarrow NP$

Famous open problem: $NP \Rightarrow P$?
In other words, are there problems that are harder to compute than to verify, namely, they could not be solved in polynomial time, but the answer could be verified in polynomial time.

Example 1 H10 is outside of NP. (Because the values of the unknowns can be very large). But over a finite field it is in NP.

Example 2 (Difficult theorem) To determine whether an integer is a prime is a P problem.

Example 3 (Factoring of a integer problem, or the Bank security problem) Given positive integers n and k, determine whether n has a divisor $1 < d < k$. It is an NP decision problem, which is equivalent to the (computational) factoring problem.

Example 4 Determine whether a given system of homogeneous linear equations has a non-zero solution.

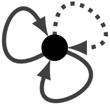
It is a P problem, due to the Gaussian elimination algorithm.

The last example is a linear algebra problem.

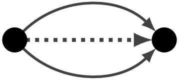
A general framework for linear algebra problems is representation theory of quivers (Gabriel 1972).

Quiver is an oriented graph.

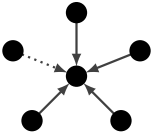
Example 1. L_m: one vertex and m loops



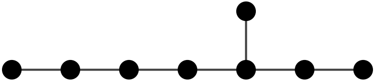
Example 2. 2_m: two vertices and m arrows from the first vertex to the second



Example 3. S_m: star with m legs

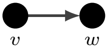


Example 4. E_8:



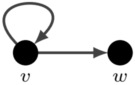
Definition

Representation π of a quiver Γ: to each vertex v one associate a finite-dimensional vector (linear) space U_v over a field $\mathbb{F}$, and to each oriented edge



one associates a linear map $U_v \xrightarrow{\pi_{v,w}} U_w$, for example:

Γ :



$$\pi : \begin{tikzcd} U_v \arrow[loop above, "\pi_{v,v}"] \arrow[r, "\pi_{v,w}"] & U_w \end{tikzcd}$$

Next, $\dim \pi \overset{\text{def}}{=} (\dim U_{v_1}, \ldots, \dim U_{v_r}) \in \mathbb{Z}_+^r$, where r is the number of vertices of Γ.

Isomorphism of representations of Γ and *direct sum* of representations $\pi_1 \oplus \pi_2$ are defined in the obvious way.

A representation π is called *indecomposable* (resp. *absolutely indecomposable*) if it does not decompose over $\mathbb{F}$ (resp. over any extension of $\mathbb{F}$) in a direct sum of two non-zero representations.

Geometric meaning of representations on examples:

L_m : m-tuple of $N \times N$ matrices, $N = \dim U_1$
2_m : m-tuple of linear maps from U_1 to U_2
S_m : arrangement of m subspaces in a vector space

Basic problem. Classification of representations of a quiver up to isomorphism.
Obviously it suffices to consider only *indecomposable* representations.

Important notion: **Cartan matrix** of a graph Γ

$$A = (a_{ij}) \qquad r \times r \text{ matrix},$$

$$\begin{aligned} a_{ii} &= 2 - 2\#(\text{loops at } v_i) \\ a_{ij} &= -\#(\text{edges connecting } v_i \text{ and } v_j) \end{aligned}.$$

Define a symmetric bilinear form on $\mathbb{Z}^r$ by $(\alpha_i|\alpha_j) = \frac{1}{2}a_{ij}$, where $\alpha_i = (0, \dots, \underset{i}{1}, \dots, 0)$. Then $(\alpha|\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathbb{Z}^r$.

Example 1. $L_m : \quad A = (2 - 2m),\ (\alpha|\alpha) = (1 - m)\alpha^2.$

Example 2: 2_m :

$$A = \begin{pmatrix} 2 & -m \\ -m & 2 \end{pmatrix},$$

$((\alpha_1|\alpha_2)|(\alpha_1|\alpha_2)) = \alpha_1^2 + \alpha_2^2 - m\alpha_1\alpha_2.$

Dimension map: $\pi \mapsto \dim \pi \in \mathbb{Z}^r$

Gabriel's Theorem (1972): A quiver Γ has only finitely many indecomposable representations if and only if its Cartan matrix A is positive definite (the most complicated example is $\Gamma = E_8$).
In this case the dimension map is one-to-one between indecomposable representations and the set of positive roots $\Delta_+(A) = \{\alpha \in \mathbb{Z}_+^r \,|\, (\alpha|\alpha) = 1\}$ of the finite-dimensional semisimple Lie algebra $\mathfrak{g}(A)$.

If the Cartan matrix is not positive definite, then the set of indecomposable representations of the quiver Γ, up to isomorphism, is a union of algebraic varieties of positive dimension. Thus we have to leave Linear Algebra and enter Algebraic Geometry, which studies systems of non-linear polynomial equations in several unknowns. The set of solutions is called an algebraic variety X.

After the Italian period of development of Algebraic Geometry, 1885–1935, the first new idea was proposed by A. Weil in 1949:

The set of solutions $X(\mathbb{F}_q)$ over a finite field $\mathbb{F}_q$ is a "generalized" polynomial $P_X(q)$ in q which carries a lot of information about the algebraic variety X. In particular, dimension of X = degree of $P_X(q)$.

Example: $X = N$-dimensional vector space, then $\mathbb{P}_X(q) = q^N$.

For an arbitrary graph Γ there is a generalization $\mathfrak{g}(A)$ of finite-dimensional semisimple Lie algebras, called a *Kac-Moody algebra*. It is infinite-dimensional if A is not positive definite, and its set of positive roots $\Delta_+(A)$ is infinite, but still allows an explicit description as a subset of $\mathbb{Z}_+^r$. In particular, $(\alpha|\alpha) \leq 1$ if $\alpha \in \Delta_+(A)$.

Example. For all the quivers 2_m, or for S_m with $m \leq 5$, this subset of $\mathbb{Z}_+^r$ is precisely $\Delta_+(A)$, but in general it is larger.

From the viewpoint of Weil's philosophy, it is natural to study absolutely indecomposable representations of a quiver Γ over a finite field $\mathbb{F}_q$.

Theorem

(a) *The number of (absolutely) indecomposable representations of a quiver Γ over $\mathbb{F}_q$ of dimension $\alpha \in \mathbb{Z}_+^r$ is independent of the orientation of Γ.*

(b) *This number is zero if $\alpha \notin \Delta_+(A)$.*

(c) *The number of absolutely indecomposable representations of dimension $\alpha \in \Delta_+(A)$ over $\mathbb{F}_q$ is given by a monic polynomial $P_{\Gamma,\alpha}(q)$ with integer coefficients of degree $1-(\alpha|\alpha)$.*

(d) *The coefficients of $P_{\Gamma,\alpha}(q)$ are non-negative.*

(e) *There exists an absolutely indecomposable representation over $\mathbb{F}_q$ of the quiver Γ of dimension α if and only if $\alpha \in \Delta_+(A)$.*

Proof.

See [Kac1980] for the proof (a)–(c); (d) was conjectured there and proved 33 years later by Hausel, Lettelier, Rodriguez-Villegas. □

Example: $\Gamma = 2_m, \alpha = \alpha_1 + \alpha_2$. Then $P_{\Gamma,\alpha}(q) = q^{m-1} + ... + q + 1$.

Returning to complexity, it is natural to ask the following question:

Quiver Problem: For a quiver Γ and $\alpha \in \Delta_+(A)$, can one find an absolutely indecomposable representation of Γ of dimension α over $\mathbb{F}_q$ in polynomial time?

Theorem

Given a finite field $\mathbb{F}_q$, and a representation π over $\mathbb{F}_q$ of a quiver Γ of dimension $\alpha \in \Delta_+(A)$, one can verify in polynomial time whether π is absolutely indecomposable or not. Consequently, the Quiver Problem is in NP.

Proof follows from two remarks.

Remark 1. π is absolutely indecomposable if and only if $\operatorname{End}\pi \subset \mathrm{Mat}_{N\times N}(\mathbb{F})$ consists of quasi-nilpotent matrices (i.e. matrices with equal eigenvalues).

Remark 2. A subalgebra $A \subset \mathrm{Mat}_{N\times N}(\mathbb{F})$ consists of quasi-nilpotent matrices if and only if two properties hold:

(i) A has a basis consisting of quasi-nilpotent matrices,

(ii) A_- is a nilpotent Lie algebra (with bracket $ab - ba$).

Problem. Is the Quiver Problem in P?