
Can algebra be applied to prove nonexistence of certain algorithms? Can geometry be used to provide nonconstructive solutions to complexity problems? Landsberg’s book provides positive answers to these questions, focusing on two central, famous open problems: determine if $P$ is equal to $NP$, and what is the complexity of matrix multiplication.

1. Introduction

The development of computational sciences has influenced every single branch of mathematics. The use of computers has led to solutions of central problems—such as the 4-colour problem [3,4]. However, perhaps even more importantly, it shifted mathematicians’ attention, inspiring them with many challenges. The most famous one, which is in fact one of the Millennium Problems, is $P$ vs. $NP$. Informally one asks the following:

If a solution of a given algorithmic problem can be verified in polynomial time, must the problem be solvable in polynomial time?

In other words; could it be that verifying and finding solutions are always of comparable difficulty?

While all students of mathematics and computer science heard about $P$ vs. $NP$, there are many other great challenges in complexity theory. One of them is to determine the complexity of matrix multiplication. The problem is given two $n \times n$ matrices, how does one efficiently compute the product?

We all know one solution—the classical algorithm which performs $n^3 - n^2$ additions and $n^3$ multiplications. But is this the optimal way? Half a century ago Strassen set out to prove that the standard algorithm was optimal. He failed to do this and provided a most surprising answer: there exist faster algorithms!

Classically, to prove that a given problem has complexity $O(f(n))$, one provides an algorithm which solves the problem and proves that it performs at most $C \cdot f(n)$ steps, for some constant $C$. What else could one do? Could one prove that the algorithm we found is (close to) optimal? In Geometry and Complexity Theory, Landsberg shows how to answer such questions using algebraic geometry (i.e. the

The author was supported by Polish National Science Center project 2013/08/A/ST1/00804.
interplay between polynomials and their solution sets) and representation theory (i.e. group actions on vector spaces). A central notion is that of a tensor. Tensors generalise both matrices and homogeneous polynomials. There are many equivalent definitions of a complex tensor of a given format \( k_1 \times k_2 \cdots \times k_d \) for \( k_i \in \mathbb{Z}_{\geq 0} \):

- a \( d \)-linear map \( \mathbb{C}^{k_1} \times \cdots \times \mathbb{C}^{k_d} \to \mathbb{C} \);
- a \( d \)-dimensional table of size \( k_1 \times \cdots \times k_d \) filled with complex numbers;
- a \((d-1)\)-linear map \( \mathbb{C}^{k_1} \times \cdots \times \mathbb{C}^{k_d-1} \to \mathbb{C}^{k_d} \);
- an element of the vector space \( \mathbb{C}^{k_1} \otimes \cdots \otimes \mathbb{C}^{k_d} \).

We want to stress the analogy to matrices. One can regard matrices as two-dimensional tables filled with numbers, or linear maps or elements of the tensor product of two spaces.

The very general idea of relating tensors to complexity theory is as follows:

1. identify a task to be performed with a tensor;
2. consider the locus \( L \) of tensors that correspond to tasks of low complexity;
3. decide if our original task/tensor belongs to \( L \).

At first, one can be surprised that a lot of algorithmic problems may be encoded as tensors. As we will see below, this is in fact the easiest part. The geometric approach comes into play by examining the features of \( L \). It turns out that in many cases \( L \) has a very nice description. By far the hardest is the third point: tensor spaces are usually very large, and deciding if a point belongs to \( L \) may be extremely hard. The algebraic approach is as follows. One tries to find a polynomial that vanishes at all points of \( L \) and evaluate it at the point corresponding to the initial problem. If the value we obtain is nonzero, we have proved that our point does not belong to \( L \).

Before we proceed, let us present a few basic facts about tensors. A tensor \( T \) is of rank one if it is a tensor product of vectors: \( T = v_1 \otimes \cdots \otimes v_d \), where \( v_i \in \mathbb{C}^{k_i} \). Equivalently, this means that in the table representation of \( T \) the entry labelled by \( i_1, \ldots, i_d \) equals \( \prod_{j=1}^{d} (v_j)_{i_j} \), where \( (v_j)_{i_j} \) is the \( i_j \)-th coordinate of the vector \( v_j \). Deciding if a tensor has rank one is easy. We know how to test it using polynomials: precisely the \( 2 \times 2 \) subdeterminants of the representation of \( T \) as a table must vanish. It is also equivalent to the fact that all of the \( d \) presentations of a tensor as a multilinear map \( \mathbb{C}^{k_1} \times \cdots \times \mathbb{C}^{k_i} \times \cdots \times \mathbb{C}^{k_{d-1}} \to \mathbb{C}^{k_d} \) (where \( \mathbb{C}^{k_i} \) denotes the missing factor) have a one-dimensional image. Further, tensors of rank one, together with zero, form a closed set.

We define the rank of \( T \) by:

\[
\text{rk} \, T := \min \{ r : T = T_1 + \cdots + T_r, \text{ where } T_i \text{'s have rank one} \}.
\]

Note that for matrices this gives the well-known definition of a rank of a matrix. Rank is the basic complexity measure of a tensor. What is surprising is that for tensors, many methods from linear algebra turn into open problems, for example:

- determining the rank of a tensor is hard—precisely \( \text{NP} \)-hard \[19\];
- tensors of rank at most \( r \) do not have to form a closed set.

The latter means that if we consider all polynomials that vanish at tensors of rank at most \( r \), they also vanish on some other tensors of higher rank. For this reason one defines the border rank of a tensor:

\[
\text{brk} \, T := \min \{ r : \text{in any neighbourhood of } T \text{ there exists a tensor of rank } r \}.
\]
Clearly, \( \text{brk} T \leq \text{rk} T \), however, this inequality may be strict:
\[
\text{brk}(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1) = 2 < 3 = \text{rk}(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1).
\]

2. Fast matrix multiplication

Let \( \text{Mat}_n \simeq \mathbb{C}^{n^2} \) be the space of complex \( n \times n \) matrices. What is matrix multiplication? It is a map \( \text{Mat}_n \times \text{Mat}_n \rightarrow \text{Mat}_n \). Further, it is a bilinear map. According to one of our definitions of a tensor as a multilinear map, matrix multiplication is a tensor. Precisely, we denote it by \( M_n \) and regard it as an element of the space \( \text{Mat}_n^* \otimes \text{Mat}_n^* \otimes \text{Mat}_n \). Explicitly, fixing the basis of \( \text{Mat}_n^* \) and \( \text{Mat}_n \) to be \( e^{ij} \) and \( e_{ij} \), respectively, we have

\[
M_n = \sum_{i,j,k=1}^{n} e^{ij} \otimes e^{jk} \otimes e_{ki}.
\]

We have thus accomplished our first task: identifying the computational problem with a tensor. The analogy goes further—the presentation (1) is in fact an algorithm. We can read it as follows.

- To compute matrix multiplication, one needs to add \( n^3 \) partial results labelled by \( i, j, k \) from 1 to \( n \).
- In the \( i, j, k \)-th step one multiplies the \( (i, j) \)-th entry of the first matrix with the \( (j, k) \)-th entry of the second and puts the result in the \( (k, i) \)-th entry of the result.

This is the well-known algorithm to multiply matrices! What if we present \( M_n \) in a different way? In particular, is \( \text{rk} M_n = n^3 \)? The surprising answer by Strassen is no, even when \( n = 2 \) [37]. We have

\[
M_2 = (e^{21} + e^{22}) \otimes e^{11} \otimes (e_{21} - e_{22}) + (e^{11} + e^{22}) \otimes (e^{11} + e^{22})
\]
\[
\otimes (e_{11} + e_{22}) \otimes e^{11} \otimes (e^{12} - e^{22}) \otimes (e_{12} + e_{22}) + e^{22} \otimes (e^{21} - e^{11})
\]
\[
\otimes (e_{11} + e_{21}) + (e^{11} + e^{12}) \otimes e^{22} \otimes (e_{12} - e_{11}) + (e^{21} - e^{11})
\]
\[
\otimes (e^{11} + e^{12}) \otimes e_{22} + (e^{12} - e^{22}) \otimes (e^{21} + e^{22}) \otimes e_{11}.
\]

This again may be interpreted as an algorithm that represents multiplication of \( 2 \times 2 \) matrices as a sum of seven partial results. For example the first partial result is:

- the product of the sum of \( (2, 1) \) and \( (2, 2) \) entries of the first matrix times the \( (1, 1) \) entry of the second matrix put with plus in \( (2, 1) \) and minus in \( (2, 2) \) entries of the resulting matrix.

A reader may question the usefulness of such a presentation: although we only have seven partial results, each one involving one multiplication, there are many more additions.

The punchline is that we want to multiply large matrices. Let us consider two \( 1000 \times 1000 \) matrices. We may regard them as \( 2 \times 2 \) block matrices, each block being \( 500 \times 500 \) matrix. We may now apply Strassen’s algorithm! We will only have to perform seven multiplications of \( 500 \times 500 \) matrices (at the cost of slightly more additions of such matrices) instead of eight. This is indeed a gain—Strassen’s algorithm is implemented and used in practice to multiply very large matrices (especially if they do not have any special structure).
In general, the complexity of the optimal algorithm for matrix multiplication is governed by the constant $\omega$:

$$\omega = \inf \{ \tau : \text{the complexity of multiplication of two } n \times n \text{ matrices is } O(n^\tau) \}$$

$$= \inf \{ \tau : \text{rank of } M_n = O(n^\tau) \} = \inf \{ \tau : \text{border rank of } M_n = O(n^\tau) \}.$$

The equalities above are in fact nontrivial theorems [6,9,23,24], which tell us that the rank and border rank of $M_n$ are indeed the correct measures of the complexity of matrix multiplication. Clearly, $2 \leq \omega \leq 3$.

A breakthrough result of Strassen, based on the algorithm for $2 \times 2$ matrices, proves that in fact $\omega \leq \log_2 7$. The estimation of $\omega$ remains a very hard open problem, with the current world record $2 \leq \omega < 2.38$ [15,30,40]. We would like to stress that all the best estimates for $\omega$ use the notion of border rank either explicitly or implicitly. The central conjecture in this field is the following.

**Conjecture 1.** The constant $\omega$ is equal to two.

The conjecture would imply that it is not much harder to multiply very large matrices than to add them (or even output the result)! The rank and border rank of $M_2$ have been determined—with quite a lot of effort [18,20,22,41]—and both equal seven. At the same time we know neither the rank nor the border rank of $M_3$. It is expected that $\text{rk} M_3 \neq \text{brk} M_3$, however at this point one cannot prove this conjecture. Special current explicit best estimates can be found in [7,21,26,28,36].

The most successful method to bound (border) rank of $M_n$ from above is known as the Strassen laser method. It relies on a small tensor $T$, preferably of low border rank, which can be used, in a nonconstructive way, to obtain a bound on border rank of $M_n$, for large $n$. The technique is based on degeneration. What is amazing is that the best tensor $T$ used in the last quarter-century basically has not changed—it is known as the Coppersmith–Winograd tensor. While the bounds on $\omega$ have been (slightly) improved, it is known that this method, starting with the Coppersmith–Winograd tensor, cannot provide a proof of Conjecture 1 [2].

Landsberg outlines a plan to overcome this problem using symmetry. Indeed, the Coppersmith–Winograd tensor exhibits a lot of symmetries [25]. Could one find other candidates for $T$ based on the property of having a large stabilizer group? A search for potential candidates has already begun [33]. Another suggested path is known as the Cohn–Umans program [11,12]. It seeks for tensors $T$ coming from (semi-)groups. This technique led to a lot of nice results and conjectures [1,13], though not to a breakthrough regarding Conjecture 1.

What about lower bounds on border rank of $M_n$? As it is often the case in complexity theory, lower bounds are very hard to come by. One of the big challenges is that although a general tensor has high rank and border rank—e.g., for $T \in \mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$ both the maximal rank and border rank are proportional to $m^2$—we cannot explicitly provide tensors with superlinear rank or border rank. Here explicit is defined rigorously, as generated in polynomial time in $m$, with integer entries by a Turing machine. There exist many explicit tensors, like $M_n$ for $m = n^2$; however so far we cannot prove that any of them has border rank greater than $2m$ or has rank greater than $3m$. This poses great challenges for the lower bounds on the complexity of optimal algorithms for matrix multiplication. To prove that $\omega > 2$, we need to show that the rank or border rank of $M_n$ is superlinear in $n^2$—the size of the matrix—while currently no one can break the above mentioned barriers for any tensor, not only matrix multiplication.
Note that, in particular, this means we do not even know a single polynomial that vanishes on tensors of rank 2m belonging to $\mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$. There exists a nice geometric explanation why finding such polynomials is so hard [8]; however, this is beyond the scope of this review. Let us mention, that the higher the rank of tensors, the higher the (minimal) degree of polynomials that may vanish on them—this explains a part of the problem. There is a beautiful, existential theory on bounds on degrees of polynomials that define symmetric, skew-symmetric, or general tensors of a given rank, when the dimension of the tensor changes [16,29,32]. However, applying it to explicit examples is currently impossible.

3. Algebraic $P$ vs. $NP$

One of the main approaches to $P$ vs. $NP$ is to characterise $NP$-complete problems. One can solve any $NP$-complete problem in polynomial time if and only if $P = NP$. It is widely believed that the only way to solve $P$ vs. $NP$ is to develop a method for lower complexity bounds. However, as Arora and Barak point out in their classical book [5], so far this is “complexity theory’s Waterloo”. One hopes that the methods of modern algebraic geometry can turn around the fate of this battle.

In 1979, Valiant proposed an algebraic version of $P$ vs. $NP$ [39]. The idea is to introduce two classes of (sequences of) polynomials. Polynomials in the class $VP$ are easy to evaluate and for polynomials in $VNP$ one can easily write down their coefficients. A prototypical example of an element in

- $VP$ is the $n \times n$ determinant $det_n = \sum_{\sigma \in S_n} (\text{sgn } \sigma) \prod_{i=1}^{n} x_{i\sigma(i)}$ of a matrix with $n^2$ distinct variables;
- $VNP$ is the $n \times n$ permanent $per_n = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i\sigma(i)}$ of the same matrix.

It turns out $per_n$ is in fact complete for the class $VNP$, i.e., $per_n \in VP$ if and only if $VP = VNP$.

A very natural question arises: Can we compute the permanent using the determinant? Precisely, can we find an $n \times n$ matrix $A$ with linear forms in $m^2$ variables $x_{i,j}$ and an additional variable $y$, such that $det A = y^{n-m} per_m$. This is possible when $n$ is of exponential size with respect to $m$ [17], but how do we prove this is not possible when $n$ depends polynomially on $m$? This is again a geometric problem! Indeed, $det_n$ is a point in the space $S^n(\mathbb{C}^{n^2})$ of (homogeneous) polynomials of degree $n$ in $n^2$ variables. The locus $L$ of all polynomials that are $n \times n$ determinants of linear forms is $\text{End}(\mathbb{C}^{n^2}) \cdot det_n$. Identifying $m^2 + 1$ variables $x_{i,j}$, $y$ with some of the $n^2$ variables, our question turns into, Does $y^{n-m} per_m$ belong to $L$?

We note that the type of the question is very much the same as for matrix multiplication. One big difference is that before we worked in a tensor space of dimension $(n^2)^3$. Now we have to deal with a much larger space of polynomials of dimension $(n+n^2-1) \choose n$. In a similar way, we could ask for a polynomial $P$ that vanishes on $L$, but does not vanish on $y^{n-m} per_m$. Here $P$ is a polynomial on the space of polynomials. This may sound confusing, until we realise we know similar objects from primary school! Indeed, consider the three-dimensional space of (inhomogeneous) degree two polynomials $ax^2 + bx + c$ in one variable. The discriminant $\Delta = b^2 - 4ac$ is a polynomial that vanishes on special polynomials, precisely those that have a double root. Of course finding nontrivial polynomials
that vanish on $L$ is much harder. It is one of the central problems in Geometric Complexity Theory, pioneered in the work of Mulmuley and Sohoni [31].

4. Final remarks

The area of interplay of algebraic geometry, complexity theory and tensors is currently very active. Let us mention three extremely interesting recent results. The first two are due to Yaroslav Shitov [34,35]. He provided counterexamples to the following two central conjectures in the field.

- **Strassen’s direct sum conjecture** [38]. Consider two tensors $T_1 \in V_1 \otimes V_2 \otimes V_3$, $T_2 \in V'_1 \otimes V'_2 \otimes V'_3$. By adding these two tensors we obtain $T_1 \oplus T_2 \in (V_1 \oplus V'_1) \otimes (V_2 \oplus V'_2) \otimes (V_3 \oplus V'_3)$. Is it true that $\text{rk}(T_1 \oplus T_2) = \text{rk} T_1 + \text{rk} T_2$?

- **Comon’s conjecture** [14]. Suppose $T$ is a symmetric tensor of rank $r$. Do there exist $r$ rank one symmetric tensors that add up to $T$?

Negative answers to both questions show how different the world of tensors is, when compared to matrices. The failure of Strassen’s conjecture has also the following striking consequence in complexity theory. If one wants to compute two multilinear maps, even if they have completely different domains, it may be more beneficial to compute them simultaneously then separately.

The last observation we present is based on [10]. It turns out that the constant $\omega$ may be defined simply using polynomials. Consider a cubic $sM_n := \sum_{i,j,k=1}^{d} x_{ij} x_{jk} x_{ki}$ in $n^2$ variables $x_{ij}$. One can ask for a representation of this cubic in terms of powers of linear forms $l_i$, namely $sM_n = \sum_{i=1}^{r} l_i^3$. The minimal $r$ is known as the Waring rank of $sM_n$. We have

$$\omega = \inf \{ \tau : \text{Waring rank of } sM_n = O(n^{\tau}) \}.$$ 

This observation opens even more possibilities for applications of methods of commutative algebra in complexity theory.

We greatly encourage mathematicians interested in these subjects (algebraic geometers in particular, but not only!) to find many, many more interesting results in the Geometry and Complexity Theory by J. M. Landsberg.

References


Mateusz Michałek

Max Planck Institute for Mathematics in the Sciences
Institute of Mathematics of the Polish Academy of Sciences
Warsaw, Poland; and
Department of Mathematics and Systems Analysis
Aalto University, Helsinki, Finland
Email address: michalek@mis.mpg.de