Computing Multi-Homogeneous Bezout Numbers is Hard

Thinh Nguyen

Abstract

The multi-homogeneous B´ezout number is a bound for the number of solutions of a system of multi-homogeneous polynomial equations, in a suitable product of projective spaces.

Given an arbitrary, not necessarily multi-homogeneous system, one can ask for the optimal multi-homogenization that would minimize the B´ezout number.

In this paper, it is proved that the problem of computing, or even estimating the optimal multi-homogeneous B´ezout number is actually **NP**-hard.

In terms of approximation theory for combinatorial optimization, the problem of computing the best multi-homogeneous structure does not belong to **APX**, unless **P** = **NP**.

Moreover, polynomial time algorithms for estimating the minimal multi-homogeneous B´ezout number up to a fixed factor cannot exist even in a randomized setting, unless **BPP**⊇**NP**.

1 Introduction

The multi-homogeneous Bezout number is a bound for the number of solutions of a system of multi-homogeneous polynomial equations.

Estimating the number of isolated solutions of a polynomial system is useful for the design and analysis of homotopy algorithms [12]. Applications include problems in engineering like the design of certain mechanisms [15,18] or others, such as computational geometry.

An application of multi-homogeneous B´ezout bounds outside the realm of algebraic equation solving is discussed in [4], where the number of roots is used to bound geometrical quantities such as volume and curvature.

There is an important connection between root-counting and **NP**-completeness theory. Indeed, it is easy to reduce an **NP**-complete or **NP**-hard problem such as SAT, the Traveling Salesman problem, Integer Programming (and thus all other **NP** problems as well) to the question whether certain polynomial systems have a common zero.

The best-known example giving an estimate for the number of roots of a polynomial equation is the Fundamental Theorem of Algebra. It was generalized to multivariate polynomial systems at the end of the 18th century by Etienne B´ezout. The B´ezout number bounds the number of (isolated) complex solutions of a polynomial $f : \mathbb{C}^n \to \mathbb{C}^n$ from above by the product of the degrees of the involved polynomials. However, in many cases this estimate is far from optimal. A well known example is given by the eigenvalue problem: Given a $n \times n$ matrix M, find the eigenpairs $(\lambda,u) \in \mathbb{C} \times \mathbb{C}^n$ such that $Mu - \lambda u = 0$. If

we equate u_n to 1, the classical B´ezout number becomes 2^{n-1}, though of course only n solutions exist.

The multi-homogeneous B´ezout number provides a sharper bound on the number of isolated solutions of a system of equations, in a suitable product of projective spaces. The multi-homogeneous B´ezout bound depends on the choice of a *multi-homogeneous structure*, that is of a partition of the variables (λ,u) into several groups.

In the eigenvalue example, the eigenvector u is defined up to a multiplicative constant, so it makes sense to define it as an element of $\mathbb{P}^{n-1}$. With respect to the eigenvector λ, we need to introduce a homogenizing variable. We therefore rewrite the equation as: $\lambda_0 Mu - \lambda_1 u = 0$, and $\lambda = \lambda_1/\lambda_0$. Now the pair $(\lambda_0 : \lambda_1)$ is an element of $\mathbb{P}^1$. The multi-homogeneous B´ezout number for this system is precisely n.

Better bounds on the root number are known, such as Kushnirenko's [10] or Bernstein's [3]. However, interest in computing the multi-homogeneous B´ezout number stems from the fact that hardness results are known for those sharper bounds (see section 2.2 for details).

Another reason of interest is that in many cases, a natural multi-homogeneous structure is known or may be found with some additional human work.

In this paper, we consider the following problem. *Let $n \in \mathbb{N}$ and a finite $A \subset \mathbb{N}^n$ be given as input. Find the minimal multi-homogeneous B´ezout number, among all choices of a multi-homogeneous structure for a polynomial system with support A:*

$$\begin{aligned} f_1(z) &= \sum_{\alpha \in A} f_{1\alpha} z_{1\alpha_1} z_{2\alpha_2} \cdots z_{n\alpha_n} \\ &\dots \\ f_n(z) &= \sum_{\alpha \in A} f_{n\alpha} z_{1\alpha_1} z_{2\alpha_2} \cdots z_{n\alpha} \end{aligned} \qquad (1)$$

where the $f_{i\alpha}$ are non-zero complex coefficients.

Geometrically, this minimal B´ezout number is an upper bound for the number of isolated roots of the system (1) in $\mathbb{C}^n$.

The main result in this paper (restated formally in section 2.1 below) is:

Theorem 1. *There cannot possibly exist a polynomial time algorithm to approximate the minimal multi-homogeneous B´ezout number for (1) up to any fixed factor, unless* **P** = **NP**.

This means that computing or even approximating the minimal B´ezout number up to a fixed factor is **NP**-hard. In terms of the hierarchy of approximation classes (see [2] and section 2.4), the minimal multi-homogeneous B´ezout number does not belong to the class **APX** unless **P** = **NP**.

Motivated by what is known on volume approximation (see section 2.2), one could ask whether allowing for randomized algorithms would be of any improvement.

Theorem 2. *There cannot possibly exist a randomized polynomial time algorithm to approximate the minimal multi-homogeneous B´ezout number for (1) up to any fixed factor, with probability of failure ϱ < 1/4, unless* **BPP** ⊇ **NP**.

While the conjecture **BPP** 6⊇ **NP** is less widely known outside the computer science community than the conjecture **P** =6 **NP**, its failure would imply the existence of probabilistic polynomial time algorithms for solving problems such as the factorization of large integers or the discrete logarithm. Most widespread cryptographic schemes are based on the assumption that those two problems are hard.

2 Background and Statement of Main Results

2.1 B´ezout numbers

In the definition of (1), we assumed for simplicity that each equation had the same *support* A. In general, a system $f(z)$ of n polynomial equations with support $(A_1,...,A_n)$ is a system of the form:

$$\begin{aligned} f_1(z) &= \mathrm{P}_{\alpha\in A_1} f_{1\alpha} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \\ &\dots \\ \alpha f_n(z) &= \mathrm{P}_{\alpha\, A_n} f_{n\alpha} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha} \\ &, \in \end{aligned} \qquad (2)$$

where the coefficients f_i are non-zero complex numbers.

A *multi-homogeneous structure* is given by a partition of $\{1,...,n\}$ into (say) k sets $I_1,...,I_k$. Then for each set I_j, we consider the group of variables $Z_j = \{z_i : i \in I_j\}$.

The degree of f_i in the group of variables Z_j is

$$d_{ij} \stackrel{\text{def}}{=} \max_{\boldsymbol{\alpha}\in A_i} \sum_{l\in I_j} \alpha_l$$

When for some j, for all i, the maximum d_{ij} is attained for all $\alpha \in A_i$, we say that (2) is homogeneous in the variables Z_j. The dimension of the projective space associated to Z_j is:

$$a \stackrel{\text{def}}{\begin{cases} \#I_j - \\ \end{cases}}$$

$_j$ = 1 if (2) is homogeneous in Z_j, and #I_j

otherwise.

We assume that $n = \sum_{j=1}^{k} a_j$. Otherwise, we would have an undetermined ($n < \sum_{j=1}^{k} a_j$) or overdetermined ($n > \sum_{j=1}^{k} a_j$) polynomial system, and multi-homogeneous Bézout numbers would have no meaning.

The multi-homogeneous Bézout number Bézout($A_1,\dots,A_n;I_1,\dots,I_k$) is the coefficient of $\prod_{j=1}^{k} \zeta_j^{a_j}$ in the formal expression $\prod_{i=1}^{n} \sum_{j=1}^{k} d_{ij}\zeta_j$ (see [12,16,17]). It bounds the maximal number of isolated roots of (2) in $\mathbb{P}^{a_1} \times \cdots \times \mathbb{P}^{a_k}$. Therefore it also bounds the number of *finite* roots of (2), i.e. the roots in $\mathbb{C}^n$.

In the particular case where $A = A_1 = \cdots = A_n$ there is a simpler expression for the multi-homogeneous Bézout number Bézout($A;I_1,\dots,I_k$) $\stackrel{\text{def}}{=}$ Bézout($A_1,\dots,A_n; I_1,\dots,I_k$), namely:

$$\text{Bézout}(A; I_1, \dots, I_k) = \binom{n}{a_1\ a_2\ \cdots\ a_k} \prod_{j=1}^{k} d_j^{a_j}, \tag{3}$$

where $d_j = d_{ij}$ (equal for each i) and the multinomial coefficient

$$\binom{n}{a_1\ a_2\ \cdots\ a_k} \stackrel{\text{def}}{=} \frac{n!}{a_1!\ a_2!\ \cdots\ a_k!}$$

is the coefficient of $\prod_{j=1}^{k} \zeta_j^{a_k}$ in $(\zeta_1 + \cdots + \zeta_k)^n$ (recall that $n = \sum_{j=1}^{k} a_j$).

Heuristics for computing a suitable multi-homogeneous structure ($I_1,\dots,I_k$) given $A_1,\dots,A_n$ are discussed in [11,13]. Surprisingly enough, there seems to be no theoretical results available on the complexity of computing the minimal Bézout number. It was conjectured in [11, p.78] that computing the minimal multi-homogeneous Bézout number is **NP**-hard.

Even, no polynomial time algorithm for computing the multi- homogeneous Bézout number *given a multi-homogeneous structure* seems to be known (see [13, p.240]).

This is why in this paper, we restrict ourselves to the case $A = A_1 = \cdots = A_n$. This is a particular subset of the general case, and any hardness result for this particular subset implies the same hardness result in the general case.

More formally, we adopt the Turing model of computation and we consider the function:

$$\text{Bézout} : n,k,A,I_1,\dots,I_k \mapsto \text{Bézout}(A;I_1,\dots,I_k)$$

where all integer numbers are in binary representation, and A is a list of n-tuples $(\alpha_1,\dots,\alpha_n)$, and each I_j is a list of its elements. In particular, the input size is bounded below by $n\#A_i$ and by $\max_{\alpha,i}[\log_2 \alpha_i]$. Therefore, Bézout($A;I_1,\cdots,I_k$) can be computed in polynomial time by a straight-forward application of formula (3). As a matter of fact, it can be computed in time polynomial in the size of A.

Problem 1 (Discrete optimization problem). Given n and A, compute

$$\min_{I} \text{Bézout}(A;I),$$

where $\mathsf{I} = (I_1,\ldots,I_k)$ ranges over all the partitions of $\{1,\ldots,n\}$.

Problem 2 (Approximation problem). Let $C > 1$ be fixed. Given n and A, compute some B such that

$$BC^{-1} < \mathrm{minB\acute{}ez}(A;\mathsf{I}) < BC$$

Again, $\mathsf{I} = (I_1,\ldots,I_k)$ ranges over all the partitions of $\{1,\ldots,n\}$.

In the problems above, we are not asking for the actual partition.

Theorem 1 (restated). *Problem 2 is* **NP***-hard.*

This is actually stronger than the conjecture by Li and Bai [11], that corresponds to the following immediate corollary:

Corollary 1. *Problem 1 is* **NP***-hard.*

2.2 Other bounds for the number of roots

Kushnirenko's Theorem [10] bounds the number of isolated solutions of (1) in $(\mathbb{C}_*)^n$ by $n!\,\mathrm{Vol}\,\mathrm{Conv}A$, where $\mathrm{Conv}A$ is the smallest convex polytope containing all the points of A.

This bound is sharper than the B´ezout bound, but the known hardness results are far more dramatic: In [9], Khachiyan proved that computing the volume of a polytope given by a set of vertices is #**P**-hard.

There is a large literature on algorithms for approximating the volume of a convex body given by a separation oracle. The problem of approximating the volume of a polytope in vertex representation can be reduced to the latter by standard linear programming techniques.

It is known that no deterministic algorithm can approximate the volume in polynomial time ([14]). However, randomized polynomial time algorithms are known for the same problem [7,19].

The same situation seems to be the case regarding the estimation of the *mixed volume* [5], which gives the actual number of solutions in $(\mathbb{C}_*)^n$ for generic polynomials of the form (2) [3].

2.3 Probabilistic algorithms

A *probabilistic machine* is a machine that has access to *random* bits of information, each random bit costing one unit of time. Each random bit is an independent, uniformly distributed random variable in {0,1}. In that sense, a probabilistic machine is a machine that flips a fair coin, as many times as necessary, spending one unit of time at each flip. We can therefore speak of the probability that the machine returns a correct result.

The class **BPP** is the class of decision problems (X,X_{yes}) such that there is a probabilistic machine and a constant $\varrho < 1/2$ that will:

(i) Decide in polynomial time if $x \in X$.

(ii) Output YES or NO, in polynomial time.

(iii) For every x, the output is the correct answer to the question: does $x \in X_{\text{yes}}$? with probability $\geq 1 - \varrho$.

Notice that we can improve the probability that the result is correct by running the same machine several times. Therefore, in the definition above, we may as well take $\varrho = 1/4$.

More generally, a probabilistic machine solves a certain problem (e.g. Problem 2) in polynomial time with probability $\geq 1-\varrho$ if and only if it always terminates in polynomial time, and the answer is correct with probability $1 - \varrho$.

Theorem 2 (restated). *There is no $\varrho < 1/2$ and no probabilistic machine solving Problem 2 with probability $1 - \varrho$, unless* **BPP** $\supseteq$ **NP**.

2.4 Approximation classes

A theory of complexity classes appropriate for the study of combinatorial optimization problems is described in [2]. Problem 1 fits naturally in the class of combinatorial optimization problems. In this context, Problem 1 is characterized by:

(i) A set of *instances*, given by the set of pairs (n,A), $n \in \mathbb{N}$, $A \subset \mathbb{N}^n$ finite and non-empty.

(ii) For every instance (n,A), a set of feasible solutions, namely the set of partitions $\mathrm{I} = (I_1,\ldots,I_k)$ of $\{1,\ldots,n\}$.

(iii) An objective function (to minimize), $B\acute{}ez(A;\mathrm{I})$.

The class **NPO** of combinatorial optimization problems is analogous to the class **NP** of decision problems. Problem 1 belongs to that class:

(1) The size of each feasible solution is polynomially bounded on the size of each instance.

(2) Given an instance (n,A) and a string w, it can be decided in time polynomial in (n,A) whether w encodes a feasible solution $\mathrm{I} = (I_1,\ldots,I_k)$.

(3) The objective function can be computed in polynomial time.

The class **APX** of approximable problems in **NPO** is defined as the subset of **NPO** for which there is some $C > 1$ and a polynomial time algorithm such that, given an instance of the problem (say n,A)) produces a feasible solution I such that the objective function applied to that solution approximates the minimum up to a factor of C. Theorem 2 admits as a corollary:

Corollary 2. *Problem 1 does not belong to* **APX***, unless* **P** = **NP**.

Our result actually holds even if we do not require the algorithms to compute a feasible solution.

3 Proof of the Main Theorems

3.1 From graph theory to systems of equations.

Definition 1. A *k-coloring* of a graph $G = (V,E)$ is a partition of the set of vertices V into k disjoint subsets ("colors") I_j, so that adjacent vertices do not belong to the same "color" I_j.

Problem 3 (Graph 3-Coloring). Given a graph $G = (V,E)$, decide if there exists a 3-coloring of G.

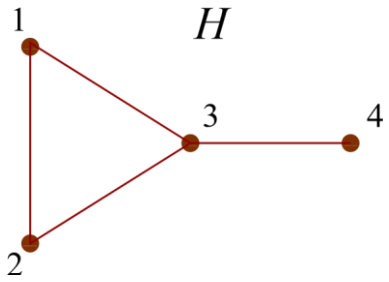

Figure 1: In this example, $A(H) = \{(0,0,0,0),(1,0,0,0),(0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,0,0), (1,0,1,0), (0,1,1,0), (0,0,1,1), (1,1,1,0)\}$. A possible polynomial with that support would be $1+v_1+v_2+v_3+v_4+v_1v_2+v_1v_3+v_2v_3+v_3v_4+v_1v_2v_3$.

It is known since [8] that the Graph 3-Coloring Problem is **NP**-hard (see also [6]). We will actually need to consider an equivalent formulation of the Graph 3-coloring problem.

Recall that the cartesian product of two graphs $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ is the graph $G_1 \times G_2 = (V_1 \times V_2, E)$ with $((v_1, v_2), (v_1', v_2')) \in E$ if and only if $v_1 = v_1'$ and $(v_2, v_2') \in E_2$ or $v_2 = v_2'$ and $(v_1, v_1') \in E_1$.

Also, let K_3 denote the complete graph with 3 vertices.

Lemma 1. *The graph G admits a 3-coloring if and only if the graph* $G \times K_3$ *admits a 3-coloring* $\mathsf{I} = (I_1,I_2,I_3)$ *with* $\#I_1 = \#I_2 = \#I_3 = |G|$.

Proof. G admits a 3-coloring if and only if $G \times K_3$ admits a 3-coloring. Moreover, any coloring I of $G \times K_3$ satisfies $\#I_1 = \#I_2 = \#I_3$. □

To each graph $H = (V,E)$ we will associate two spaces of polynomial systems. Each of those spaces is characterized by a support set $A = A(H)$ (resp. $A(H)^l$) to be constructed and corresponds to the space of polynomials of the form (1) with complex coefficients. Of particular interest will be graphs of the form $H = G \times K_3$.

We start by identifying the set V of vertices of H to the set $\{1,...,m\}$. Let K_s denote the complete graph of size s, i.e. the graph with s vertices all of them pairwise connected by edges.

To each copy of K_s, $s = 0,\ldots,3$ that can be embedded as a subgraph of H (say the subgraph generated by $\{v_1,\cdots,v_s\}$) we associate the monomial

$$z_{v_1} z_{v_2} \cdots z_{v_s}$$

(the empty graph K_0 corresponds to the constant monomial). Then we consider the linear space generated by all those monomials (Figure 1). Therefore, the support $A(H)$ is the set of all $e_{v_1} + \cdots + e_{v_s} \subset \mathbb{N}^m$ such that $0 \le s \le 3$ and $\{v_1,\ldots,v_s\}$ induces a copy of K_s as a subgraph of H. Here, e_i denotes the i-th vector of the canonical basis of $\mathbb{R}^n$.

Given a set A, we denote by A^l the l-fold i cartesian product of A.

The two spaces of polynomial systems associated to a graph H will be the polynomial systems with support $A(H)$ and $A(H)^l$.

Remark that none of the two classes of systems above is homogeneous in any possible group of variables (because we introduced a constant monomial). Therefore, in the calculation of the B´ezout number for a partition I, we can set $a_j = \#I_j$.

Lemma 2. *Let l be fixed. Then, there is a polynomial time algorithm to compute $A(H)$ and $A(H)^l$, given H.*

3.2 A gap between B´ezout numbers

In case the graph H admits a 3-coloring $\mathrm{I} = (I_1,I_2,I_3)$, any corresponding polynomial system is always trilinear (linear in each set of variables). If moreover H is of the form $H = G \times K_3$ with $|G| = n$, the cardinality of the I_j is always n, and formula (3) becomes:

$$\text{B´ez}(A(G \times K_3); \boldsymbol{I}) = \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

The crucial step in the proof of Theorem 1 is to show that

$$\text{B´ez}(A(G \times K_3); \boldsymbol{I}) \ge \frac{4}{3}\begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

unless $k = 3$ and I is a 3-coloring of $G \times K_3$.

In order to do that, we introduce the following cleaner abstraction for the B´ezout number: if $k \in \mathbb{N}$ and $\mathbf{a} = (a_1,\ldots,a_k) \in \mathbb{N}^k$ are such that $\sum_{j=1}^k a_j = 3n$, we set

$$B(\mathbf{a}) \stackrel{\text{def}}{=} \begin{pmatrix} 3n \\ a_1\ a_2\ \cdots\ a_k \end{pmatrix} \prod_{j=1}^{k} \left\lceil \frac{a_j}{n} \right\rceil^{a_j}$$

Lemma 3. *If $H = G \times K_3$ and $\mathrm{I} = (I_1,\ldots,I_k)$ is a partition of the set $\{1,\ldots,3n\}$ of vertices of H, then*

$$\text{B´ez}(A(H);\mathrm{I}) \ge B(\mathbf{a})$$

with $a_j = \#I_j$.

Proof. Consider the n disjoint copies of K_3 in $H = G \times K_3$ induced by the nodes of G. By the pigeonhole principle, there is at least one of those copies with at least $\lceil a_j/n \rceil$ elements of I_j. Hence, the degree d_j in the j-th group of variables is at least $\lceil a_j/n \rceil$.

The main step towards establishing the "gap" is the following Proposition:

Proposition 1. *Let* $n,k \in \mathbb{N}^n$ *and let* $a_1 \geq a_2 \geq \cdots \geq a_k \geq 1$ *be such that* $\sum_{j=1}^{k} a_j = 3n$. *Then, either* $k = 3$ *and* $a_1 = a_2 = a_3 = n$, *or:*

$$B(\mathbf{a}) \geq \frac{4}{3} B(n,n,n).$$

Moreover, this bound is sharp.

The proof of Proposition 1 is postponed to section 4.

Putting it all together,

Lemma 4. *Let G be a graph and* $n = |G|$. *If G admits a 3-coloring, then*

$$\min_{\boldsymbol{I}} \text{Béz}(A(G \times K_3); \boldsymbol{I}) = \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

Otherwise,

$$\min_{\boldsymbol{I}} \text{Béz}(A(G \times K_3); \boldsymbol{I}) \geq \frac{4}{3} \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

Proof. According to Lemma 1, G admits a 3-coloring if and only if $G \times K_3$ admits a 3-coloring.

If $\mathsf{I} = (I_1, I_2, I_3)$ is a 3-coloring of $G \times K_3$, then

$$\text{B´ez}(A(G \times K_3); \boldsymbol{I}) = \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

If $\mathsf{I} = (I_1, \ldots, I_k)$ is not a 3-coloring of $G \times K_3$, then we distinguish two cases.

We set $a_j = \#I_j$.

Case 1: a = (n,n,n) and hence $k = 3$. Then the degree in at least one group of variables is ≥ 2, and

$$\text{B´ez}(A(G \times K_3); \boldsymbol{I}) \geq 2^n \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}$$

Case 2: a = (6 n,n,n). Then

$$\text{B´ez}(A(G \times K_3); \boldsymbol{I}) \geq B(a_1, \ldots, a_k) \geq \frac{4}{3} \begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix},$$

where the first inequality follows from Lemma 3 and the second from Proposition 1. In both cases,

$$\min_{\boldsymbol{I}} \text{Béz}(A(G \times K_3), \boldsymbol{I}) \geq \frac{4}{3} \binom{3n}{n\ n\ n}.$$

□

Lemma 4 would be sufficient to prove a weaker version of Theorem 1, where the factor C in problem 2 is less than 4/3.

3.3 Improving the gap

In order to obtain a proof valid for any C the idea is to increase the gap by considering several copies of a polynomial system, but each copy in a new set of variables. This idea works out because of the special multiplicative structure of the multi-homogeneous B´ezout number. We will need:

Proposition 2. *Let $m,l \in \mathbb{N}$. Let $A \subset \mathbb{N}^m$ be finite and assume that $0 \in A$. Then,*

$$\min_{\boldsymbol{J}} \text{Béz}(A^l; \boldsymbol{J}) = \binom{lm}{m\ m\ \cdots\ m} \left(\min_{\boldsymbol{I}} \text{Béz}(A; \boldsymbol{I})\right)^l$$

Proof. 1. Let $\mathcal{I} = (I_1, \cdots, I_k)$ be the partition of $\{1,...,m\}$ where the minimal B´ezout number for A is attained.

This induces a partition $\mathcal{J} = (J_{js})_{1 \leq j \leq k, 1 \leq s \leq l}$ of $\{1,...,m\} \times \{1,...,l\}$, given by $J_{js} = I_j \times \{s\}$. Identifying each pair (i,s) with $i + ms$, the J_{js} are also a partition of $\{1,...,lm\}$.

By construction of A^l, the degree d_{js} in the variables corresponding to J_{js} is equal to the degree d_j of the variables I_j in A.

The systems corresponding to A and A^l cannot be homogeneous for any partition, since $0 \in A$ and $0 \in A^l$. Then we have $a_j = \#I_j = a_{js}$ for any s. Therefore,

$$\begin{aligned}
\min_{\mathcal{K}} \text{B´ez}(A^l, \boldsymbol{K}) \ &\leq\ \text{B´ez}(A^l, \boldsymbol{J}) \\
&= \binom{lm}{\underbrace{a_1\ \cdots\ a_1}_{l \text{ times}}\ \cdots\ \underbrace{a_k\ \cdots\ a_k}_{l \text{ times}}} \prod_{s=1}^{l} \prod_{j=1}^{k} d_j^{a_j} \\
&= \binom{lm}{m\ m\ \cdots\ m} \left(\binom{m}{a_1\ a_2\ \cdots\ a_k} \prod_{j=1}^{k} d_j^{a_j} \right)^l \\
&= \binom{lm}{m\ m\ \cdots\ m} \left(\min_{\boldsymbol{I}} \text{Béz}(A; \boldsymbol{I})\right)^l
\end{aligned}$$

2. Now, suppose that the minimal B´ezout number for A^l is attained for a partition $\boldsymbol{J} = (J_1, \cdots, J_r$ $\{s\}$.). We claim that each J_t fits into exactly one of the l sets $\{1,...,m\} \times$

Suppose this is not the case. Assume without loss of generality that J_1 splits into $K \subset \{1,\ldots,m\} \times \{1\}$ and $L \subset \{1,\ldots,m\} \times \{2,\ldots,l\}$, both K and L non-empty.

If d_K denotes the degree in the K-variables and d_L the degree in the L variables, then $d_1 = d_K + d_L$. Also, $a_1 = a_K + a_L$ where a_K is the size of K and a_L is the size of L. The multi-homogeneous B´ezout number corresponding to the partition $J' = (K,L,J_2,\cdots,J_r)$ is:

$$\text{B´ez}(A^l; \boldsymbol{J}') = \binom{3lm}{a_K\ a_L\ a_2\ \cdots\ a_r} d_K^{a_K} d_L^{a_L} \prod_{j=2}^{r} d_j^{a_j}$$

Therefore,

$$\frac{\text{B´ez}(A^l; \boldsymbol{J}')}{\text{B´ez}(A^l, \boldsymbol{J})} = \frac{\binom{a_1}{a_K} d_K^{a_K} d_L^{a_L}}{(d_K + d_L)^{a_1}} < 1$$

and the B´ezout number was not minimal, thus establishing the claim.

3. Denote by $J = \cup_{s=1}^{l} J^{(s)}$ the partition minimizing the B´ezout number corresponding to A^l. In the notation above, we assume that $J^{(s)}$ is a partition of $\{1,\ldots,m\}\times\{s\}$.

In that case,

$$\begin{aligned}
\text{B´ez}(A^l; \boldsymbol{J}) &= \binom{lm}{m\ m\ \cdots\ m} \prod_{s=1}^{l} \left(\binom{m}{a_1^{(s)}\ \cdots\ a_k^{(s)}} \prod_{j=1}^{k} (d_j^{(s)})^{a_j^{(s)}} \right) \\
&= \binom{lm}{m\ m\ \cdots\ m} \prod_{s=1}^{l} \text{Béz}(A, \boldsymbol{J}^{(s)}) \\
&\geq \binom{lm}{m\ m\ \cdots\ m} \left(\min_{\boldsymbol{I}} \text{Béz}(A; \boldsymbol{I}) \right)^l
\end{aligned}$$

□

Combining Lemma 4 and Proposition 2, we established that:

Lemma 5. *Let G be a graph and n = |G|. Let l ∈ ℕ. If G admits a 3-coloring, then*

$$\min_{\boldsymbol{J}} \text{Béz}(A(G \times K_3)^l, \boldsymbol{J}) = \binom{3nl}{3n\ 3n\ \cdots\ 3n} \binom{3n}{n\ n\ n}^l$$

Otherwise,

$$\min_{\boldsymbol{J}} \text{Béz}(A(G \times K_3)^l, \boldsymbol{J}) \geq \left(\frac{4}{3}\right)^l \binom{3nl}{3n\ 3n\ \cdots\ 3n} \binom{3n}{n\ n\ n}^l$$

Proof of Theorem 1. Assume that `ApproxB´ez` is a deterministic, polynomial time algorithm for solving problem 2, i.e., for estimating the B´ezout number up to a factor of *C*.

Then the following algorithm decides Graph 3-coloring (Problem 3) in polynomial time:

Algorithm 1 (Decides Graph 3-coloring problem).

`Input:` a graph G `of size` n.

`Output:` YES if G admits a 3-coloring, NO otherwise.

`Constants:` $l = \left\lceil \frac{\log C}{2 \log 4/3} \right\rceil$.

1. `Compute`

$$\rho \leftarrow \frac{\textsc{ApproxBéz}\left(A(G \times K_3)^l\right)}{\begin{pmatrix} 3nl \\ 3n\ 3n\ \cdots\ 3n \end{pmatrix}\begin{pmatrix} 3n \\ n\ n\ n \end{pmatrix}^l}$$

2. **If** $\rho^2 < C$ **then** `Output YES,` **else** `Output NO.`

By our choice of the constant l, $\sqrt{C} \leq (4/3)^l$. Therefore, Lemma 5 asserts that the output of algorithm 1 is correct.

The bit-size of the numbers that occur when computing the denominator of line 2 are bounded above by $O(3nl\log(3nl))$. The size of the graph $G \times K_3$ is $O(n)$, and Lemma 2 says that A^l can be computed in polynomial time.

It follows that Algorithm 1 runs in polynomial time. Since Graph 3-coloring is **NP**-complete, we deduce that **P** = **NP**. □

Proof of Theorem 2. Assume now that `ApproxB´ez` is a probabilistic polynomial time algorithm for solving problem 2, which returns a correct result with probability $1 - \varrho$, $\varrho < 1/4$.

Then Algorithm 1 will return the correct answer for the Graph 3-coloring Problem, with probability at least $1 - \varrho$. This implies that Problem 3 is actually in **BPP**. □

4 Proof of Proposition 1

We will need the following trivial Lemma in the proof of Proposition 1:

Lemma 6. *Let* $x,n \in \mathbb{N}$. *Then,*

$$\left(\left\lceil \frac{x}{n} \right\rceil \frac{n}{x}\right)^x \geq 1 + \left((n-x) \mod n\right).$$

In particular, the left-hand side is ≥ 2 *whenever* $n \nmid x$, *and is always* ≥ 1.

Proof. Since $n\left\lceil \frac{x}{n} \right\rceil = x + (n-x) \mod n$, we have:

$$\left(\left\lceil \frac{x}{n} \right\rceil \frac{n}{x}\right)^x = \left(1 + \frac{(n-x) \mod n}{x}\right)^x \geq 1 + \left((n-x) \mod n\right)$$

□

Also, we will make use of the Stirling Formula [1, (6.1.38)]:

$$x! = \sqrt{2\pi}\ x^{x+\frac{1}{2}}\ e^{-x+\frac{\theta(x)}{12x}}, \tag{4}$$

where $0 < \theta(x) < 1$.

Proof of Proposition 1. The ratio between $B(\mathbf{a})$ and $B(n,n,n)$ is:

$$\frac{B(\mathbf{a})}{B(n,n,n)} = \prod_{j=1}^{k} \left\lceil \frac{a_j}{n} \right\rceil^{a_j} \ \frac{n!\ n!\ n!}{a_1!\ a_2!\ \cdots\ a_k!}$$

From Stirling formula (4) it follows immediately that:

$$\frac{B(\mathbf{a})}{B(n,n,n)} = \sqrt{2\pi}^{3-k} \ \prod_{j=1}^{k} \left\lceil \frac{a_j}{n} \right\rceil^{a_j} \ \frac{n^{3n+\frac{3}{2}}}{\prod_{j=1}^{k} a_j^{a_j+\frac{1}{2}}}\ e^{\frac{\theta(n)}{4n} - \sum \frac{\theta(a_j)}{12a_j}} \tag{5}$$

Now we distinguish the cases $k = 1$, $k = 2$, and $k \geq 3$. The first two cases are easy:

Case 1: If $k = 1$, then $a_1 = 3n$ and (5) becomes:

$$\frac{B(\mathbf{a})}{B(n,n,n)} = 2\pi\ \frac{n}{\sqrt{3}}\ e^{\frac{\theta(n)}{4n} - \frac{\theta(3n)}{36n}}$$

which is bounded below by $\frac{2\pi}{\sqrt{3}} e^{-1/36} \simeq 3.528218766.$

Case 2: If $k = 2$, Lemma 6 implies that

$$\frac{B(\mathbf{a})}{B(n,n,n)} \geq \sqrt{2\pi}\ \frac{n^{\frac{3}{2}}}{\sqrt{a_1\ a_2}}\ e^{-1/6}$$

Since $\sqrt{a_1\ a_2} \leq \frac{a_1+a_2}{2} = \frac{3n}{2}$, we obtain:

$$\frac{B(\mathbf{a})}{B(n,n,n)} \geq \frac{2}{3}\sqrt{2\pi} e^{-1/6} \simeq 1.414543350$$

Case 3: Let $k \geq 3$. If $a_3 = n$, then $k = 3$ and $a_1 = a_2 = a_3 = n$, so there is nothing to prove.

Therefore, we assume from now on that $a_3 < n$.

We separate the right-hand side of (5) into two products, the first for $j = 1,2,3$ and the second for $j \geq 4$. Equation (5) becomes now:

$$\frac{B(\mathbf{a})}{B(n,n,n)} = \left(\prod_{j=1}^{3} \left(\left\lceil \frac{a_j}{n} \right\rceil \frac{n}{a_j} \right)^{a_j}\ \frac{n^{\frac{3}{2}}}{\sqrt{a_1 a_2 a_3}}\ e^{\frac{\theta(n)}{4n} - \sum_{j=1}^{3} \frac{\theta(a_j)}{12a_j}} \right) \left(\sqrt{2\pi}^{3-k}\ \prod_{j=4}^{k} \frac{n^{a_j}}{a_j^{a_j+\frac{1}{2}}}\ e^{-\sum_{j=4}^{k} \frac{\theta(a_j)}{12a_j}} \right) \tag{6}$$

using the fact that $a_j < n$ for $j \geq 4$. In case $k = 3$, the second factor in equation (6) above is equal to one.

Since $a_3 < n$, n 6 | a_3 and Lemma 6 implies that for $a_3 < n$

$$\prod_{j=1}^{3} \left(\left\lceil \frac{a_j}{n} \right\rceil \frac{n}{a_j} \right)^{a_j} \geq 2$$

Moreover, $\sqrt[3]{a_1 a_2 a_3} \leq (a_1 + a_2 + a_3)/3 \leq n$, so the first factor of the right-hand side of (6) can be bounded below by

$$\prod_{j=1}^{k} \left(\left\lceil \frac{a_j}{n} \right\rceil \frac{n}{a_j} \right)^{a_j} \quad \frac{n^{\frac{3}{2}}}{\sqrt{a_1 a_2 a_3}} \; e^{\frac{\theta(n)}{4n} - \sum_{j=1}^{3} \frac{\theta(a_j)}{12 a_j}} \geq 2e^{-1/4} \simeq 1.557601566$$

If $k = 3$ we are done. Otherwise, we notice that since the a_j are non-increasing, $a_j \leq \frac{3n}{4}$ for all $j \geq 4$. In order to bound the second factor of (6), we will need the following technical Lemma:

Lemma 7. *Let n,x* ∈ N *and let* $x \leq \frac{3n}{4}$. *Then, unless* (*n,x*) ∈ {(2,1),(3,2),(4,3), (6,4),(7,5),(8,6)}, *we have:*

$$\frac{n^x}{\sqrt{2\pi} x^{x+\frac{1}{2}}} e^{-\frac{1}{12x}} > 1$$

(Proof is postponed).

n	a_j	3*n*	**a**	j	*B*(**a**)	*B*(*n,n,n*)	$\frac{B(\mathbf{a})}{B(n,n,n)}$
2	1	6	1 1 1 **1 1 1**	4,5,6	720	90	8
			2 1 1 **1 1**	4,5	360		4
			2 2 1 **1**	4	180		2
			3 1 1 **1**	4	120		$\frac{4}{3}$
3	2	9	2 2 2 **2** 1	4	22680	1680	$\frac{27}{2}$
			3 2 2 **2**	4	7560		$\frac{9}{2}$
4	3	12	3 3 3 **3**	4	369600	34650	$\frac{32}{3}$
6	4	18	4 4 4 **4** 1 1	4	19297278000	17153136	1125
			4 4 4 **4** 2	4	9648639000		$\frac{1125}{2}$
			5 4 4 **4** 1	4	3859455600		225
			5 5 4 **4**	4	771891120		45

			6 4 4 **4**	4	643242600		$\frac{75}{2}$
7	5	21	5 5 5 **5** 1 6 5 5 **5**	4 4	246387645504 41064607584	399072960	$\frac{3087}{5}$ $\frac{1029}{10}$
8	6	24	6 6 6 **6**	4	2308743493056	9465511770	$\frac{10976}{45}$

Table 1: Ratios for all the exceptional pairs (n,**a**).

Therefore, unless some of the pairs (n,a_j), $j \geq 4$ belong to the exceptional subset {(2,1),(3,2),(4,3),(6,4),(7,5),(8,6)}, we have:

$$\frac{B(\mathbf{a})}{B(n,n,n)} \geq 2e^{-\frac{1}{4}} \simeq 1.557601566 .$$

Finally, we consider the values of n and **a** where some (n,a_j), $j \geq 4$, is in the exceptional subset. All the possible values of n and **a** are listed in table 1. The ratio is always $\geq 4/3$, and the value of $4/3$ is attained for $n = 2$ and **a** = (3,1,1,1). □

Proof of Lemma 7. Let

$$\begin{aligned} g_n(x) &= \log\left(\frac{n^x}{\sqrt{2\pi}x^{x+\frac{1}{2}}}e^{-\frac{1}{12x}}\right) \\ &= x\log n - x\log x - \frac{1}{2}\log x - \frac{1}{12x} - \frac{1}{2}\log 2\pi \end{aligned}$$

(see figure 2). We first consider values of $x \geq 7$. By hypothesis, $n/x \geq 4/3$ so $\log n - \log x \geq \log(4/3)$, and therefore $g_n(x) \geq h(x)$, where:

$$h(x) = x\log(4/3) - \frac{1}{2}\log x - \frac{1}{12x} - \frac{1}{2}\log 2\pi$$

(see Figure 2 also). Notice that $h(x)$ is independent of n. The derivative of h is

$$h'(x) = \log(4/3) - \frac{1}{2x} + \frac{1}{12x^2} = \frac{12\log(4/3)x^2 - 6x + 1}{12x^2}$$

The numerator vanishes at

$$x = \frac{1 \pm 1\sqrt{1 - 4/3\log(4/3)}}{4\log(4/3)}$$

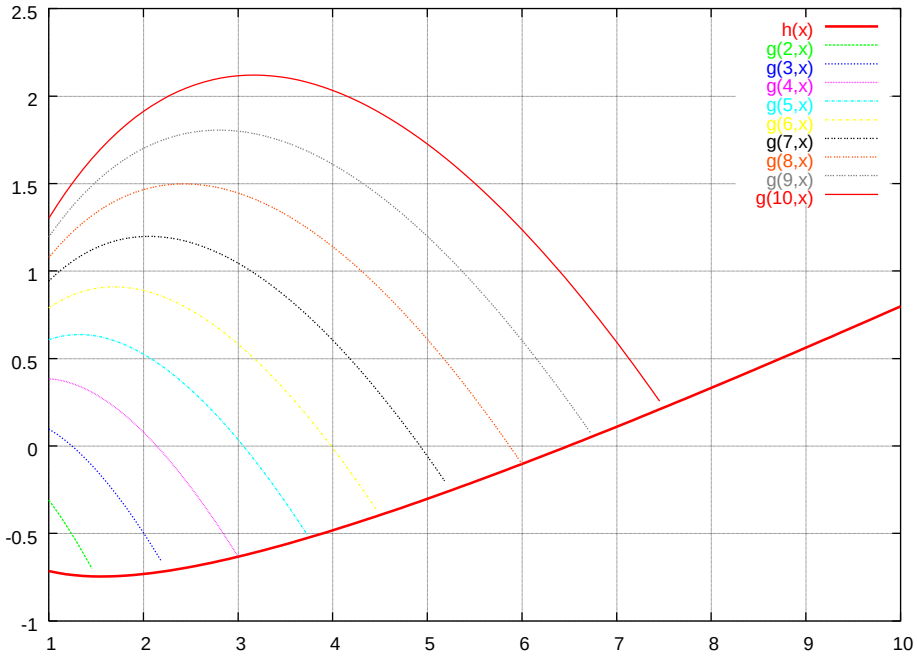

Figure 2: Plots of $g_n(x)$ and $h(x)$.

Numerically, $x \simeq 0.1867281114$ or $x \simeq 1.551301638$. Therefore, the function $h(x)$ is increasing for $x \geq 2$. Again, numerically $h(7) \simeq 0.1099761345$ and therefore, if $x \geq 7$ we always have: $e^{g_n(x)} \geq 1.1162 > 1$

Now we consider $x \leq 6$. Having $g_n > 0$, is equivalent to:

$$n > n_0(x) = xe^{\frac{1}{2x}\log x + \frac{1}{12x^2} + \frac{1}{2x}\log 2\pi}$$

At this point, we proved that $g_n(x)$ is positive, except possibly for pairs (n,x) with $1 \leq x \leq 6$ and $\frac{4}{3}x \leq n \leq n_0(x)$. The values of n_0 are tabulated in Table 2. From Table 2 it is clear that the only exceptions are those listed in the hypothesis.

x	$\frac{4}{3}x$	$n_0(x)$	Possible n's
1	1.333333333	2.724464424	2
2	2.666666666	3.844857634	3
3	4	4.939610298	4
4	5.333333333	6.016610872	5
5	6.666666666	7.081620345	6
6	8	8.137996302	8

Table 2: Possible values of n for x small

□

References

[1] Milton Abramowitz and Irene A. Stegun (eds.), *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, Dover Publications Inc., New York, 1992, Reprint of the 1972 edition.

[2] G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi, *Complexity and approximation*, Springer-Verlag, Berlin, 1999, Combinatorial optimization problems and their approximability properties; With 1 CD-ROM (Windows and UNIX).

[3] D. N. Bernstein, *The number of roots of a system of equations*, Funkcional. Anal. i Prilo˘zen. **9** (1975), 1–4. (Russian)

[4] Jean-Pierre Dedieu, Gregorio Malajovich, and Mike Shub, *On the curvature of the central path of linear programming theory* (2003), arXiv:math.OC/0312083.

[5] Martin Dyer, Peter Gritzmann, and Alexander Hufnagel, *On the complexity of computing mixed volumes*, SIAM J. Comput. **27** (1998), 356–400 (electronic).

[6] Michael R. Garey and David S. Johnson, *Computers and intractability*, W. H. Freeman and Co., San Francisco, Calif., 1979, A guide to the theory of NP-completeness; A Series of Books in the Mathematical Sciences.

[7] Ravi Kannan, L´aszl´o Lova´sz, and Miklo´s Simonovits, *Random walks and an* $O^*(n^5)$ *volume algorithm for convex bodies*, Random Structures Algorithms **11** (1997), 1–50.

[8] Richard M. Karp, *Reducibility among combinatorial problems*, Complexity of Computer Computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972), Plenum, New York, 1972, pp. 85–103.

[9] L. G. Khachiyan, *The problem of calculating the volume of a polyhedron is enumeratively hard*, Uspekhi Mat. Nauk **44** (1989), 179–180. (Russian)

[10] A.G. Kushnirenko, *Newton Polytopes and the B´ezout Theorem*, Funct. Anal. Appl. **10** (1976), 233–235.

[11] Tiejun Li and Fengshan Bai, *Minimizing multi-homogeneous B´ezout numbers by a local search method*, Math. Comp. **70** (2001), 767–787 (electronic).

[12] T. Y. Li, *Numerical solution of multivariate polynomial systems by homotopy continuation methods*, Acta Numerica, 1997, Acta Numer., vol. 6, Cambridge Univ. Press, Cambridge, 1997, pp. 399– 436.

[13] Ting Li, Zhenjiang Lin, and Fengshan Bai, *Heuristic methods for computing the minimal multihomogeneous B´ezout number*, Appl. Math. Comput. **146** (2003), 237–256.

[14] L´aszl´o Lova´sz, *An algorithmic theory of numbers, graphs and convexity*, CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 50, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1986,.

[15] Alexander Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, Prentice Hall Inc., Englewood Cliffs, NJ, 1987,.

[16] Alexander Morgan and Andrew Sommese, *A homotopy for solving general polynomial systems that respects m-homogeneous structures*, Appl. Math. Comput. **24** (1987), 101–113.

[17] I. R. Shafarevich, *Basic algebraic geometry*, Springer Study Edition, Springer-Verlag, Berlin, 1977, Translated from the Russian by K. A. Hirsch; Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

[18] Charles Wampler, Alexander Morgan, and Andrew Sommese, *Numerical continuation methods for solving polynomial systems arising in kinematics*, Journal Mechanical Design **112** (1990), 59–68.

[19] A. G. Werschulz and H. Wo´zniakowski, *What is the complexity of volume calculation?*, J. Complexity **18** (2002), 660–678, Algorithms and complexity for continuous problems/Algorithms, computational complexity, and models of computation for nonlinear and multivariate problems (Dagstuhl/South Hadley, MA, 2000).