



Semi-algebraic properties of Minkowski sums of a twisted cubic segment

Arthur Bik¹ · Adam Czaplinski² · Markus Wageringel³

Received: 6 June 2019 / Accepted: 30 January 2020 / Published online: 12 February 2020
© The Author(s) 2020

Abstract

We find a semi-algebraic description of the Minkowski sum $\mathcal{A}_{3,n}$ of n copies of the twisted cubic segment $\{(t, t^2, t^3) \mid -1 \leq t \leq 1\}$ for each integer $n \geq 3$. These descriptions provide efficient membership tests for the sets $\mathcal{A}_{3,n}$. These membership tests in turn can be used to resolve some instances of the underdetermined matrix moment problem, which was formulated by Michael Rubinstein and Peter Sarnak in order to study problems related to L -functions and their zeros.

Keywords Semi-algebraic sets · Implicitization · Twisted cubic

Mathematics Subject Classification 14P10

1 Introduction

The zeros of L -functions are known to be able to describe various geometrical and arithmetical objects and are the subjects of several conjectures (cf. [1–3]). For example, the Generalized Riemann Hypothesis conjectures that all non-trivial zeros of an L -function have real part $1/2$ and the Grand Simplicity Hypothesis asserts that the imaginary parts of zeros of Dirichlet L -functions are linearly independent over \mathbb{Q} (cf. [5]). L -functions can

The first author was supported by the Vici grant *Stabilisation in Algebra and Geometry* from the Netherlands Organisation for Scientific Research (NWO). The third author was supported by DFG grant GK 1916 *Kombinatorische Strukturen in der Geometrie* of the German Research Foundation.

✉ Markus Wageringel
markus.wageringel@uos.de

Arthur Bik
arthur.bik@math.unibe.ch

Adam Czaplinski
adam.czaplinski@uni-siegen.de

¹ Mathematisches Institut, Universität Bern, Alpeneggstrasse 22, 3012 Bern, Switzerland

² Department Mathematik, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany

³ Institut für Mathematik, Universität Osnabrück, Albrechtstrasse 28 A, 49076 Osnabrück, Germany

also be encountered in proofs of the Prime Number Theorem (cf. [6]) and in primality tests (cf. [4]).

Let ρ be an automorphic cusp form and let $L(s, \rho)$ be its standard L -function. A conjecture, which has been verified in many cases, states that under certain conditions the function $L(s, \rho)$ has an analytic continuation $\Lambda(s, \rho)$ that satisfies the functional equation

$$\Lambda(1 - s, \rho) = W(\rho)N_\rho^{s-1/2}\Lambda(s, \rho),$$

where N_ρ is the conductor of ρ and $W(\rho)$ is either 1 or -1 . The sign $W(\rho) \in \{\pm 1\}$ is called the root number of ρ . The problems of computing root numbers and counting the zeros of L -functions are related to the following problem with $\log N_\rho \approx n$.

Problem 1.1 (The underdetermined matrix moment problem) *Determine the possible sets of eigenvalues of a real orthogonal $(2n + 1) \times (2n + 1)$ matrix A given its first $k \leq n$ moments $\text{tr}(A)$, $\text{tr}(A^2)$, \dots , $\text{tr}(A^k)$.*

This problem is the object of study in the paper [7] by Michael Rubinstein and Peter Sarnak. For the full background and relevance of the problem, we refer to this paper.

Let A be a real orthogonal $(2n + 1) \times (2n + 1)$ matrix. Then its eigenvalues are

$$\det(A), e^{i\theta_1}, e^{-i\theta_1}, \dots, e^{i\theta_n}, e^{-i\theta_n}$$

for some $\theta_1, \dots, \theta_n \in [0, \pi]$. And conversely, any such sequence is the spectrum of a real orthogonal $(2n + 1) \times (2n + 1)$ matrix. We have

$$\text{tr}(A^j) = \det(A)^j + 2 \sum_{i=1}^n \cos(j\theta_i)$$

and $\cos(j\theta_i) = T_j(\cos(\theta_i))$ for all integers $j \geq 1$, where T_j is the j -th Chebyshev polynomial of the first kind. The polynomial $T_j(x)$ has degree j . So, given $\det(A)$ and $\text{tr}(A)$, $\text{tr}(A^2)$, \dots , $\text{tr}(A^k)$ for some integer $k \leq n$, we can compute $\sum_{i=1}^n \cos(\theta_i)^j$ for each $j \in \{1, \dots, k\}$ using Gaussian elimination on the coefficient vectors of T_1, \dots, T_k . As $\det(A) \in \{\pm 1\}$ only has finitely many possible values, we write $t_i = \cos(\theta_i) \in [-1, 1]$ and see that Problem 1.1 reduces to the following problem.

Problem 1.2 (The moment curve problem) *Determine the set*

$$\left\{ (t_1, \dots, t_n) \in [-1, 1]^n \mid \sum_{i=1}^n t_i^j = x_j \text{ for all } j \in \{1, \dots, k\} \right\}$$

given the real numbers $x_1, \dots, x_k \in \mathbb{R}$.

This problem was also formulated by Michael Rubinstein and Peter Sarnak. Note that given the first k power sums of t_1, \dots, t_n , we can compute all symmetric polynomial expressions in t_1, \dots, t_n of degree at most k . So if $k = n$, then we are able to compute the coefficients of the polynomial $(x - t_1) \cdots (x - t_n)$, which not only allows us to recover t_1, \dots, t_n , but also shows that $t_1, \dots, t_n \in \mathbb{C}$ are unique up to reordering. So we are interested in the case where $k < n$. In this case, Michael Rubinstein and Peter Sarnak propose the following strategy: consider the set $\mathcal{C}_k := \{(t, t^2, \dots, t^k) \mid -1 \leq t \leq 1\} \subseteq \mathbb{R}^k$ and define

$$\mathcal{A}_{k,n} := \underbrace{C_k + C_k + \dots + C_k}_n$$

to be the Minkowski sum of n copies of C_k for each integer $n \geq 1$. Then we can determine the set of tuples $(t_1, \dots, t_n) \in [-1, 1]^n$ such that

$$\sum_{i=1}^n t_i^j = x_j$$

for all $j \in \{1, \dots, k\}$ recursively by first computing the set of $t_n \in [-1, 1]$ such that

$$(x_1, x_2, \dots, x_k) - (t_n, t_n^2, \dots, t_n^k) \in \mathcal{A}_{k,n-1}.$$

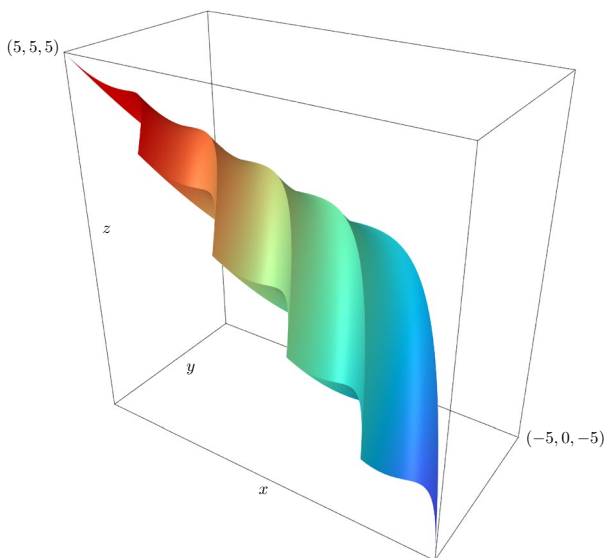
In order to do the latter, we need an efficient membership test for the set $\mathcal{A}_{k,n}$ for all $n > k$. For $k \in \{1, 2\}$, this is easy. In general, one way to get an efficient membership test would be to describe the sets $\mathcal{A}_{k,n}$ implicitly using only equalities and inequalities involving polynomial expressions in x_1, \dots, x_k and unions—in other words, using semi-algebraic descriptions of the sets $\mathcal{A}_{k,n}$. In this paper, we provide exactly such descriptions in the case that $k = 3$.

2 Main results

Let $n \geq 3$ be a positive integer. Our first result describes the boundary of $\mathcal{A}_{3,n}$. We need this result in order to prove the Main Theorem. However, it also provides us with a piecewise parametrization, which is useful for rendering a visualization of $\mathcal{A}_{3,n}$. See Fig. 1 for an example.

Before we give the semi-algebraic description of $\mathcal{A}_{3,n}$, we first discuss the intuition behind it. As Fig. 1 for $n = 5$ and the interactive 3D models for $n = 3, \dots, 20$

Fig. 1 A rendering of the semi-algebraic set $\mathcal{A}_{3,5}$. Interactive 3D models of $\mathcal{A}_{3,n}$ are available at <https://mathsites.unibe.ch/bik/A3n.html> for $n = 1, \dots, 20$



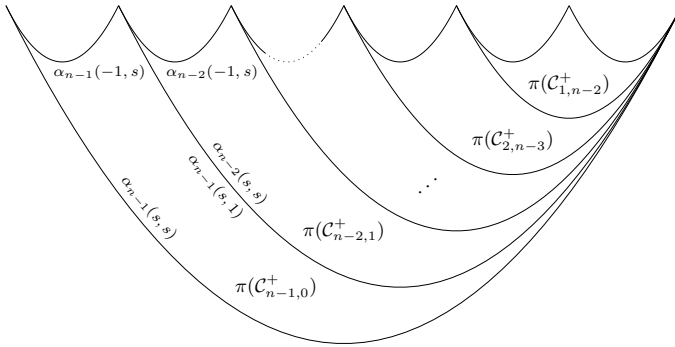


Fig. 2 The set $\mathcal{B}_n^b = \pi(C_{1,n-2}^+) \cup \dots \cup \pi(C_{n-1,0}^+)$

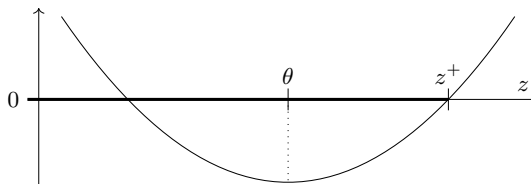


Fig. 3 Visualization of the condition $z \leq z^+$ in the proof of the Main Theorem. The parabola represents the function sending z to $f_{k1}(x - (n - k - 1), y - (n - k - 1), z - (n - k - 1))$

demonstrate, the set $\mathcal{A}_{3,n}$ looks like an oyster with an upper and lower shell forming the boundary. We call these upper and lower shells \mathcal{B}_n^+ and \mathcal{B}_n^- respectively. These two shells have identical projections to the (x, y) -plane, which we denote by \mathcal{B}_n^b , and both projection maps are one-to-one. This yields a first description of $\mathcal{A}_{3,n}$: for a point $(x, y, z) \in \mathbb{R}^3$ to lie in $\mathcal{A}_{3,n}$, it is necessary that (x, y) lies in \mathcal{B}_n^b . When this is the case, the point lies in $\mathcal{A}_{3,n}$ precisely when it lies below \mathcal{B}_n^+ and above \mathcal{B}_n^- .

Each of the two shells consists of $n - 1$ spiraling ridges. These are the sets $C_{k,n-k-1}^+$ and $C_{\ell,n-\ell-1}^-$ defined below respectively. The projections of the ridges are easily visualized on \mathcal{B}_n^b . See Fig. 2. We can now reformulate our first description of $\mathcal{A}_{3,n}$ in the following way: let $(x, y, z) \in \mathbb{R}^3$ be a point such that (x, y) lies in \mathcal{B}_n^b . Then (x, y) lies in the projections of $C_{k,n-k-1}^+$ and $C_{\ell,n-\ell-1}^-$ for some k, ℓ . The point (x, y, z) lies in $\mathcal{A}_{3,n}$ precisely when it lies below $C_{k,n-k-1}^+$ and above $C_{\ell,n-\ell-1}^-$.

Next, we think of (x, y) as being fixed. This turns the conditions of lying below $C_{k,n-k-1}^+$ and above $C_{\ell,n-\ell-1}^-$ into conditions on z . The former condition is equivalent to z being at most the biggest root of some parabola $f = Az^2 + Bz + C$ with $A > 0$ and can thus be expressed as $f(z)$ being at most 0 or z is at most the value $-B/2A$ where f attains its minimum. See Fig. 3. Similarly, the latter condition is equivalent to z being at least the smallest root of a parabola $f = Az^2 + Bz + C$ with $A > 0$ and can be expressed as $f(z)$ being at most 0 or z is at least the value $-B/2A$ where f attains its minimum. This is our description of $\mathcal{A}_{3,n}$.

In order to state our results precisely, we define the following sets:

- For all integers $k, \ell \geq 1$ and $a, b \geq 0$, we take

$$C_{k,a}^+ = \left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

$$C_{\ell,b}^- = \left\{ \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}.$$

- We take $\mathcal{B}_n^+ = \bigcup_{k=1}^{n-1} C_{k,n-k-1}^+$. $\mathcal{B}_n^- = \bigcup_{\ell=1}^{n-1} C_{\ell,n-\ell-1}^-$.
- We let \mathcal{B}_n^b be the set consisting of all points $(x, y) \in \mathbb{R}^2$ such that $ny \geq x^2$ and $y \leq n - 1 + (x + 2i - (n - 1))^2$ for each $i \in \{0, \dots, n - 1\}$.

We also let $\pi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ be the projection map sending $(x, y, z) \mapsto (x, y)$.

Theorem 2.1 *Let $(x, y) \in \mathcal{B}_n^b$ be a point and $z \in \mathbb{R}$ be a real number.*

- (a) *The boundary of $\mathcal{A}_{3,n}$ is the union of \mathcal{B}_n^+ and \mathcal{B}_n^- .*
- (b) *We have $\pi(\mathcal{B}_n^+) = \pi(\mathcal{B}_n^-) = \mathcal{B}_n^b$.*
- (c) *There exist unique numbers $z^+, z^- \in \mathbb{R}$ such that $(x, y, z^+) \in \mathcal{B}_n^+$ and $(x, y, z^-) \in \mathcal{B}_n^-$. We have $z^+ \geq z^-$. Moreover, equality holds precisely when the point (x, y) lies on the boundary of \mathcal{B}_n^b .*
- (d) *We have $(x, y, z) \in \mathcal{A}_{3,n}$ if and only if $z^+ \geq z \geq z^-$.*
- (e) *Every point on the boundary of $\mathcal{A}_{3,n}$ can be written as*

$$p = \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \\ t_1 \end{pmatrix} + \dots + \begin{pmatrix} t_n \\ t_n^2 \\ t_n^3 \\ t_n \end{pmatrix}$$

for some tuple $(t_1, \dots, t_n) \in [-1, 1]^n$. The set $\{t_1, \dots, t_n\} \setminus \{-1, 1\}$ has at most two elements and the tuple (t_1, \dots, t_n) is unique up to permutation of its entries.

In Sect. 5, we find semi-algebraic descriptions of (in particular) $C_{k,a}^+$ and $C_{\ell,b}^-$. To write these descriptions down, we define

$$A_{k\ell} = k\ell(k + \ell)^2,$$

$$B_{k\ell}(x, y) = 2k\ell x(2x^2 - 3(k + \ell)y),$$

$$C_{k\ell}(x, y) = x^6 - 3(k + \ell)x^4y + 3(k^2 + k\ell + \ell^2)x^2y^2 - (k - \ell)^2(k + \ell)y^3,$$

$$D_{k\ell}(x, y) = (k + \ell)y - x^2,$$

$$f_{k\ell}(x, y, z) = A_{k\ell}z^2 + B_{k\ell}(x, y)z + C_{k\ell}(x, y)$$

for all positive integers $k, \ell \geq 1$. Note here that

$$B_{k\ell}^2 - 4A_{k\ell}C_{k\ell} = 4k\ell(\ell - k)^2D_{k\ell}^3$$

for all k, ℓ . We then use these descriptions together with the previous theorem to prove our main result.

Take the following sets:

$$X = \bigcup_{k=1}^{n-1} \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} + (n - k - 1) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{R}^3 \left| \begin{array}{l} y \leq k + (x + k)^2, \\ y \geq (k + 1)^{-1}x^2, \\ y \leq 1 + k^{-1}(x - 1)^2 \text{ and} \\ z \leq \frac{-B_{k1}(x,y)}{2A_{k1}} \text{ or } f_{k1}(x, y, z) \leq 0 \end{array} \right. \right\},$$

$$Y = \bigcup_{\ell=1}^{n-1} \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} + (n - \ell - 1) \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix} \in \mathbb{R}^3 \left| \begin{array}{l} y \leq \ell + (x - \ell)^2, \\ y \geq (\ell + 1)^{-1}x^2, \\ y \leq 1 + \ell^{-1}(x + 1)^2 \text{ and} \\ z \geq \frac{-B_{1\ell}(x,y)}{2A_{1\ell}} \text{ or } f_{1\ell}(x, y, z) \leq 0 \end{array} \right. \right\}.$$

Main Theorem *We have $\mathcal{A}_{3,n} = X \cap Y$.*

2.1 Structure of the paper

The first step of the proof is to show that the boundary of $\mathcal{A}_{3,n}$ is contained in the union of \mathcal{B}_n^+ and \mathcal{B}_n^- . We start doing this by proving a result about representations of points on the boundary of $\mathcal{A}_{3,n}$ in Sect. 3. In Sect. 4, we prove the statement for $n = 4$ and then conclude that it holds for all $n \geq 3$. After that, in Sect. 5, we find semi-algebraic descriptions for the components that make up the boundary. And then, in Sect. 6, we study the sets \mathcal{B}_n^+ and \mathcal{B}_n^- in more detail and prove Theorem 2.1 and the Main Theorem. We conclude the paper by discussing the problem for higher dimensions in Sect. 7.

3 Representations of points on the boundary of $\mathcal{A}_{3,n}$

The goal of this and the next section is to prove that the boundary of $\mathcal{A}_{3,n}$ is contained in the union of \mathcal{B}_n^+ and \mathcal{B}_n^- . We start with the following proposition.

Proposition 3.1 *Let $p \in \mathbb{R}^3$ be a point on the boundary of $\mathcal{A}_{3,n}$ and write*

$$p = \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \\ t_1 \end{pmatrix} + \dots + \begin{pmatrix} t_n \\ t_n^2 \\ t_n^3 \\ t_n \end{pmatrix}$$

for some tuple $(t_1, \dots, t_n) \in [-1, 1]^n$. Then the set $\{t_1, \dots, t_n\} \setminus \{-1, 1\}$ has at most two elements.

Proof Fix indices $1 \leq i < j < k \leq n$ and consider the map

$$\varphi : [-1, 1]^3 \rightarrow \mathbb{R}^3, \\ (r, s, t) \mapsto \begin{pmatrix} r \\ r^2 \\ r^3 \end{pmatrix} + \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + \sum_{\substack{\ell \in \{1, \dots, n\} \\ \ell \notin \{i, j, k\}}} \begin{pmatrix} t_\ell \\ t_\ell^2 \\ t_\ell^3 \end{pmatrix}.$$

Then we have $p = \varphi(t_i, t_j, t_k)$. The Jacobian of φ at the point (t_i, t_j, t_k) is

$$\begin{pmatrix} 1 & 1 & 1 \\ 2t_i & 2t_j & 2t_k \\ 3t_i^2 & 3t_j^2 & 3t_k^2 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 2 & \\ & & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ t_i & t_j & t_k \\ t_i^2 & t_j^2 & t_k^2 \end{pmatrix}$$

and hence has rank 3 if $t_i \neq t_j \neq t_k \neq t_i$. So, if in addition $t_i, t_j, t_k \notin \{-1, 1\}$, then every point in a small neighborhood around p is in the image of φ by the inverse function theorem. As this cannot happen for a point p on the boundary of $\mathcal{A}_{3,n}$, it follows that the set $\{t_1, \dots, t_n\} \setminus \{-1, 1\}$ has at most two elements. \square

From the proposition, it immediately follows that the boundary of $\mathcal{A}_{3,n}$ is contained in the union of the sets

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

over all integers $k, \ell \geq 1$ and $a, b \geq 0$ such that $k + \ell + a + b = n$. So to prove that the boundary of $\mathcal{A}_{3,n}$ is contained in the union of \mathcal{B}_n^+ and \mathcal{B}_n^- , it suffices to prove that every point that is contained in one of these sets and is not contained in $\mathcal{B}_n^+ \cup \mathcal{B}_n^-$ is also not contained in the boundary of $\mathcal{A}_{3,n}$.

Lemma 3.2 *Let $k \geq k' \geq 1, \ell \geq \ell' \geq 1, a \geq a' \geq 0$ and $b \geq b' \geq 0$ be integers. Take $n = k + \ell + a + b, n' = k' + \ell' + a' + b'$ and $-1 < s < t < 1$. Assume that*

$$p' = k' \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell' \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + a' \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b' \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

is not contained in the boundary of $\mathcal{A}_{3,n'}$. Then

$$p = k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

is not contained in the boundary of $\mathcal{A}_{3,n}$.

Proof If the point p' does not lie on the boundary of $\mathcal{A}_{3,n'}$, then the point p cannot lie on the boundary of

$$\mathcal{A}_{3,n'} + (k - k')(s, s^2, s^3) + (\ell - \ell')(t, t^2, t^3) + (a - a')(1, 1, 1) + (b - b')(-1, 1, -1)$$

and hence it can also not lie on the boundary of $\mathcal{A}_{3,n}$. □

To prove that the boundary of $\mathcal{A}_{3,n}$ is contained in the union of \mathcal{B}_n^+ and \mathcal{B}_n^- , we need to eliminate the cases where one of the following conditions holds:

- (1) $k, \ell \geq 2$,
- (2) $k = \ell = 1$ and $a, b > 0$,
- (3) $k = 1, \ell > 1$ and $a > 0$,
- (4) $k > 1, \ell = 1$ and $b > 0$.

Using the previous lemma, we see that it suffices to eliminate the cases where

$$(k, \ell, a, b) \in \{(1, 1, 1, 1), (1, 2, 1, 0), (2, 1, 0, 1), (2, 2, 0, 0)\}$$

and hence we first consider the boundary of $\mathcal{A}_{3,n}$ for $n = 4$.

4 The boundary of $\mathcal{A}_{3,4}$ versus the boundary of $\mathcal{A}_{3,n}$

In this section, we show that the boundary of $\mathcal{A}_{3,n}$ is contained in $\mathcal{B}_n^+ \cup \mathcal{B}_n^-$ for $n = 4$ and conclude from this that the same statement holds for all $n \geq 3$. We need to show that no point of

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 < s < t < 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

is contained in the boundary of $\mathcal{A}_{3,4}$ for $(k, \ell, a, b) = (1, 1, 1, 1), (1, 2, 1, 0), (2, 1, 0, 1), (2, 2, 0, 0)$. We start with the case $(k, \ell, a, b) = (2, 2, 0, 0)$.

Proposition 4.1 *Take $-1 < s < t < 1$. Then the point*

$$p = 2(s, s^2, s^3) + 2(t, t^2, t^3)$$

does not lie on the boundary of $\mathcal{A}_{3,4}$.

Proof Consider the system of equations

$$\begin{aligned} 2s + 2t &= t_1 + t_2 + t_3 + t_4, \\ 2s^2 + 2t^2 &= t_1^2 + t_2^2 + t_3^2 + t_4^2, \\ 2s^3 + 2t^3 &= t_1^3 + t_2^3 + t_3^3 + t_4^3 \end{aligned}$$

with the additional conditions that $-1 < t_1, t_2, t_3, t_4 < 1$ are pairwise distinct. If this system has a solution that satisfies the additional conditions, then the point p cannot lie on the boundary of $\mathcal{A}_{3,4}$ by Proposition 3.1. It turns out that such a solution (t_1, t_2, t_3, t_4) can

even be found when we assume that $t_1 + t_2 = t_3 + t_4$. Indeed, let $0 \neq \alpha \neq \beta \neq 0$ be such that $|\alpha|, |\beta| < 1 - \frac{1}{2}|s + t|$ and $\alpha^2 + \beta^2 = \frac{1}{2}(s - t)^2$. Then

$$(t_1, t_2, t_3, t_4) = \left(\frac{s+t}{2} + \alpha, \frac{s+t}{2} - \alpha, \frac{s+t}{2} + \beta, \frac{s+t}{2} - \beta \right)$$

is a solution to the system equalities so that $-1 < t_1, t_2, t_3, t_4 < 1$ are pairwise distinct. One can check that $|\alpha|, |\beta| < 1 - \frac{1}{2}|s + t|$ and $\alpha^2 + \beta^2 = \frac{1}{2}(s - t)^2$ for $\alpha, \beta = \pm \frac{1}{2}(s - t)$. Here we use that $|s - t| + |s + t| \leq 2 \cdot \max(|s|, |t|) < 2$. It follows that for any point (α, β) on the circle given by

$$\alpha^2 + \beta^2 = \frac{1}{2}(s - t)^2$$

that is sufficiently close to $(\frac{1}{2}(s - t), \frac{1}{2}(s - t))$ also satisfies these conditions. So to conclude the proof, we simply let (α, β) be such a point with $0 \neq \alpha \neq \beta \neq 0$. □

Next, we take care of the case $(k, \ell, a, b) = (1, 1, 1, 1)$.

Lemma 4.2 *Take $\delta > 0$. Then there exists an $\varepsilon > 0$ such that*

$$(s, s^2, s^3) + (t, t^2, t^3) + (1, 1, 1) - (0, 0, \varepsilon') \in \mathcal{A}_{3,3}$$

for all $-1 < s < t < 1$ and $0 \leq \varepsilon' \leq \varepsilon$ with $1 - t, t - s, s - (-1) \geq \delta$.

Proof For $0 \leq \lambda \ll 1$, consider $(t_1, t_2, t_3) = (s + \mu, t + \lambda - \mu, 1 - \lambda)$ where

$$\begin{aligned} \mu &= (\lambda + (t - s) - \sqrt{d})/2, \\ d &= (t - s)^2 + 2(t - s)\lambda + 4(1 - t)\lambda - 3\lambda^2. \end{aligned}$$

Assuming that $d \geq 0$ and $-1 \leq t_1, t_2, t_3 \leq 1$, one can check that

$$(s, s^2, s^3) + (t, t^2, t^3) + (1, 1, 1) - (0, 0, \varepsilon'(\lambda)) = \sum_{i=1}^3 (t_i, t_i^2, t_i^3) \in \mathcal{A}_{3,3}$$

for $\varepsilon'(\lambda) = 3\lambda(1 - t - \lambda)(1 - s - \lambda)$. Note that $\varepsilon'(0) = 0$. So to prove the lemma, it suffices to find a $c > 0$ such that $d \geq 0$ and $-1 \leq t_1, t_2, t_3 \leq 1$ for all $0 \leq \lambda \leq c$ and $\varepsilon'(c) > 0$, because we can then take $\varepsilon = \varepsilon'(c)$ and have $[0, \varepsilon] \subseteq \varepsilon'([0, c])$.

Take $c = \min(\delta, \delta^2)/1000 > 0$ and assume that $0 \leq \lambda \leq c$. Then we have

$$d \geq (t - s)^2 + 3\lambda(2\delta - \lambda) \geq (t - s)^2 \geq 0$$

and hence $\sqrt{d} \geq t - s$. We also have

$$\sqrt{d} - (t - s) = \frac{d - (t - s)^2}{\sqrt{d} + (t - s)} \leq \frac{2(t - s)\lambda + 4(1 - t)\lambda - 3\lambda^2}{2(t - s)} \leq \frac{12\lambda}{2\delta} \leq \delta/100$$

since $t - s, 1 - t \leq 2$. Hence $|\mu| \leq \delta/100$ and therefore $-1 \leq t_1, t_2, t_3 \leq 1$. We have

$$\varepsilon'(c) = 3c(1 - t - c)(1 - s - c) \geq 3c \cdot \delta/3 \cdot \delta/3 = c\delta^2/3 > 0.$$

Hence the statement of the lemma holds. □

Lemma 4.3 Take $\delta > 0$. Then there exists an $\varepsilon > 0$ such that

$$(s, s^2, s^3) + (t, t^2, t^3) + (-1, 1, -1) + (0, 0, \varepsilon') \in \mathcal{A}_{3,3}$$

for all $-1 < s < t < 1$ and $0 \leq \varepsilon' \leq \varepsilon$ with $1 - t, t - s, s - (-1) \geq \delta$.

Proof The proof is similar to the Proof of Lemma 4.2. For $0 \leq \lambda \ll 1$, one considers $(t_1, t_2, t_3) = (s - \lambda + \mu, t - \mu, -1 + \lambda)$ where

$$\begin{aligned} \mu &= (\lambda + (t - s) - \sqrt{d})/2, \\ d &= (t - s)^2 + 2(t - s)\lambda + 4(s - (-1))\lambda - 3\lambda^2. \end{aligned}$$

Assuming that $d \geq 0$ and $-1 \leq t_1, t_2, t_3 \leq 1$, one can check that

$$(s, s^2, s^3) + (t, t^2, t^3) + (-1, 1, -1) + (0, 0, \varepsilon'(\lambda)) = \sum_{i=1}^3 (t_i, t_i^2, t_i^3) \in \mathcal{A}_{3,3}$$

for $\varepsilon'(\lambda) = 3\lambda(t - (-1) - \lambda)(s - (-1) - \lambda)$. The other details are left to the reader. □

Proposition 4.4 Take $-1 < s < t < 1$. Then the point

$$p = (s, s^2, s^3) + (t, t^2, t^3) + (1, 1, 1) + (-1, 1, -1)$$

does not lie on the boundary of $\mathcal{A}_{3,4}$.

Proof Set $\delta = \min(1 - t, t - s, s - (-1))/2 > 0$ and let $\varepsilon > 0$ be the minimum of the two ε 's from Lemmas 4.2 and 4.3. Write $p = (x, y, z)$. The Jacobian of the map

$$(u, v) \mapsto (u, u^2) + (v, v^2) + (1, 1) + (-1, 1)$$

is invertible at (s, t) . It follows that all points in \mathbb{R}^2 in a small neighborhood of (x, y) are of the form

$$(u, u^2) + (v, v^2) + (1, 1) + (-1, 1)$$

with (u, v) in a small neighborhood of (s, t) by the Inverse Function Theorem. By shrinking this neighborhood, we may assume that $-1 < u < v < 1$ and $1 - v, v - u, u - (-1) \geq \delta$. Lemmas 4.2 and 4.3 now tell us that

$$(u, u^2, u^3) + (v, v^2, v^3) + (1, 1, 1) + (-1, 1, -1) + (0, 0, \varepsilon') \in \mathcal{A}_{3,4}$$

for all (u, v) in the neighborhood and $|\varepsilon'| < \varepsilon$. Hence p is in the interior of $\mathcal{A}_{3,4}$. □

Finally, we take care of the cases $(k, \ell, a, b) = (1, 2, 1, 0), (2, 1, 0, 1)$.

Lemma 4.5 Take $\delta > 0$. Then there exists an $\varepsilon > 0$ such that

$$(s, s^2, s^3) + 2(t, t^2, t^3) + (0, 0, \varepsilon') \in \mathcal{A}_{3,3}$$

for all $-1 \leq s < t < 1$ and $0 \leq \varepsilon' \leq \varepsilon$ with $1 - t, t - s \geq \delta$.

Proof The proof is similar to the Proof of Lemma 4.2. For $0 \leq \lambda \ll 1$, one considers

$$(t_1, t_2, t_3) = (s + 2\lambda, t - \lambda + \mu, t - \lambda - \mu)$$

where $\mu = \sqrt{2(t-s)\lambda - 3\lambda^2}$ and finds that

$$(s, s^2, s^3) + 2(t, t^2, t^3) + (0, 0, \varepsilon'(\lambda)) = \sum_{i=1}^3 (t_i, t_i^2, t_i^3) \in \mathcal{A}_{3,3}.$$

for $\varepsilon'(\lambda) = 6(t-s)^2\lambda - 24(t-s)\lambda^2 + 24\lambda^3$. The other details are left to the reader. \square

Lemma 4.6 Take $\delta > 0$. Then there exists an $\varepsilon > 0$ such that

$$2(s, s^2, s^3) + (t, t^2, t^3) - (0, 0, \varepsilon') \in \mathcal{A}_{3,3}$$

for all $-1 < s < t \leq 1$ and $0 \leq \varepsilon' \leq \varepsilon$ with $t - s, s - (-1) \geq \delta$.

Proof The proof is similar to the Proof of Lemma 4.2. For $0 \leq \lambda \ll 1$, one considers

$$(t_1, t_2, t_3) = (s + \lambda + \mu, s + \lambda - \mu, t - 2\lambda)$$

where $\mu = \sqrt{2(t-s)\lambda - 3\lambda^2}$ and finds that

$$2(s, s^2, s^3) + (t, t^2, t^3) - (0, 0, \varepsilon'(\lambda)) = \sum_{i=1}^3 (t_i, t_i^2, t_i^3) \in \mathcal{A}_{3,3}.$$

for $\varepsilon'(\lambda) = 6(t-s)^2\lambda - 24(t-s)\lambda^2 + 24\lambda^3$. The other details are left to the reader. \square

Proposition 4.7 Take $-1 < s < t < 1$. Then the point

$$p = (s, s^2, s^3) + 2(t, t^2, t^3) + (1, 1, 1)$$

does not lie on the boundary of $\mathcal{A}_{3,4}$.

Proof The proof is similar to the proof of Proposition 4.4. For (u, v) in a small neighborhood of (s, t) , we find points in $\mathcal{A}_{3,4}$ above

$$(u, u^2, u^3) + 2(v, v^2, v^3) + (1, 1, 1)$$

using Lemma 4.5 and we find points below using Lemma 4.6. Note here that in the latter case the role of the pair (s, t) from Lemma 4.6 is played by $(v, 1)$. \square

Proposition 4.8 Take $-1 < s < t < 1$. Then the point

$$p = 2(s, s^2, s^3) + (t, t^2, t^3) + (-1, 1, -1)$$

does not lie on the boundary of $\mathcal{A}_{3,4}$.

Proof The proof is similar to the proof of Proposition 4.7. For (u, v) in a small neighborhood of (s, t) , we find points in $\mathcal{A}_{3,4}$ above

$$2(u, u^2, u^3) + (v, v^2, v^3) + (-1, 1, -1)$$

using Lemma 4.5 and we find points below using Lemma 4.6. Note here that in the former case the role of the pair (s, t) from Lemma 4.5 is played by $(-1, u)$. \square

By combining Propositions 3.1, 4.1, 4.4, 4.7 and 4.8, we see that the boundary of $\mathcal{A}_{3,n}$ is contained in $\mathcal{B}_n^+ \cup \mathcal{B}_n^-$ for $n = 4$. We now use this knowledge to prove the same for $n > 4$.

Theorem 4.9 *The boundary of $\mathcal{A}_{3,n}$ is contained in the union of \mathcal{B}_n^+ and \mathcal{B}_n^- .*

Proof For $n = 3$, this follows directly from Proposition 3.1. For $n = 4$, we additionally use Propositions 4.1, 4.4, 4.7 and 4.8. For $n > 4$, we need to show that points of the form

$$k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

with $-1 < s < t < 1$, $k, \ell \geq 1$ and $a, b \geq 0$ are not on the boundary of $\mathcal{A}_{3,n}$ when one of the following conditions holds:

- (1) $k, \ell \geq 2$,
- (2) $k = \ell = 1$ and $a, b > 0$,
- (3) $k = 1, \ell > 1$ and $a > 0$,
- (4) $k > 1, \ell = 1$ and $b > 0$.

This is done by combining Lemma 3.2 with Propositions 4.1, 4.4, 4.7 and 4.8. \square

5 The semi-algebraic components of the boundary of $\mathcal{A}_{3,n}$

Consider the sets

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

for $k, \ell \geq 1$. Recall that

$$\begin{aligned} A_{k\ell} &= k\ell(k + \ell)^2, \\ B_{k\ell}(x, y) &= 2k\ell x(2x^2 - 3(k + \ell)y), \\ C_{k\ell}(x, y) &= x^6 - 3(k + \ell)x^4y + 3(k^2 + k\ell + \ell^2)x^2y^2 - (k - \ell)^2(k + \ell)y^3, \\ D_{k\ell}(x, y) &= (k + \ell)y - x^2, \\ f_{k\ell}(x, y, z) &= A_{k\ell}z^2 + B_{k\ell}(x, y)z + C_{k\ell}(x, y) \end{aligned}$$

and $B_{k\ell}^2 - 4A_{k\ell}C_{k\ell} = 4k\ell(\ell - k)^2D_{k\ell}^3$ from Sect. 2. Our goal for this section is to prove the following proposition and theorem.

Proposition 5.1 *If $k = \ell$, then*

$$f_{k\ell}(x, y, z) = A_{k\ell} \left(z + \frac{B_{k\ell}(x, y)}{2A_{k\ell}} \right)^2$$

decomposes the polynomial $f_{k\ell}$ into irreducible factors over \mathbb{Q} . If $k \neq \ell$, then $f_{k\ell}$ is irreducible over \mathbb{C} .

Theorem 5.2 *The set*

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\}$$

consists of all points

$$(x, y, z) \in [-(k + \ell), (k + \ell)] \times [0, (k + \ell)] \times [-(k + \ell), (k + \ell)]$$

such that $f_{k\ell}(x, y, z) = 0$, the inequalities

$$0 \leq k\ell D_{k\ell}(x, y) \leq k^2(k + \ell + x)^2, \ell^2(k + \ell - x)^2$$

hold and in addition the following requirements are met:

- *If $k < \ell$, then the inequality $z \leq \frac{-B_{k\ell}(x,y)}{2A_{k\ell}}$ must hold.*
- *If $k = \ell$, then equation $z = \frac{-B_{k\ell}(x,y)}{2A_{k\ell}}$ must hold.*
- *If $k > \ell$, then the inequality $z \geq \frac{-B_{k\ell}(x,y)}{2A_{k\ell}}$ must hold.*

For the remainder of the section, we fix integers $k, \ell \geq 1$ and we write

$$A = A_{k\ell}, B = B_{k\ell}, C = C_{k\ell}, D = D_{k\ell}, f = f_{k\ell}$$

in order to simplify the used notation.

Proof of Proposition 5.1 The first statement is easy. Assume that $k \neq \ell$. To prove that f is irreducible under this assumption, note that f is homogeneous with respect to the grading where $\deg(x) = 1, \deg(y) = 2$ and $\deg(z) = 3$. It follows that if f is reducible, then

$$Az^2 + B(x, y)z + C(x, y) = f = A(z + ax^3 + bxy)(z + cx^3 + dxy)$$

for some a, b, c, d . However, this would imply that the coefficient

$$-(k - \ell)^2(k + \ell)$$

of C at y^3 equals 0. This is a contradiction. So f is irreducible. □

Proof of Theorem 5.2 Note that we have $x, z \in [-(k + \ell), (k + \ell)]$ and $y \in [0, (k + \ell)]$ for all points

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\}.$$

So we let

$$(x, y, z) \in [-(k + \ell), (k + \ell)] \times [0, (k + \ell)] \times [-(k + \ell), (k + \ell)]$$

be a point and find out when it is contained in

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\}.$$

We start by looking at the first two coordinates. So we solve the system of equations

$$\begin{aligned} x &= ks + \ell t, \\ y &= ks^2 + \ell t^2 \end{aligned}$$

under the conditions that $-1 \leq s \leq t \leq 1$. Solving the system, we find that

$$(ks, \ell t) = \left(\frac{kx \pm \sqrt{k\ell D(x, y)}}{k + \ell}, \frac{\ell x \mp \sqrt{k\ell D(x, y)}}{k + \ell} \right).$$

So we need to assume that $k\ell D(x, y) \geq 0$. Adding the condition $s \leq t$, we get

$$(ks, \ell t) = \left(\frac{kx - \sqrt{k\ell D(x, y)}}{k + \ell}, \frac{\ell x + \sqrt{k\ell D(x, y)}}{k + \ell} \right)$$

and so the conditions $-1 \leq s$ and $t \leq 1$ translate to

$$\sqrt{k\ell D(x, y)} \leq k(k + \ell + x), \ell(k + \ell - x).$$

As $x \in [-(k + \ell), (k + \ell)]$, these conditions are equivalent to

$$k\ell D(x, y) \leq k^2(k + \ell + x)^2, \ell^2(k + \ell - x)^2.$$

Now, also consider the third coordinate $z = ks^3 + \ell t^3$. One can check that $f(x, y, z) = 0$. So if $k = \ell$, then we have

$$z = \frac{-B(x, y)}{2A}$$

by Proposition 5.1 and we are done. So assume that $k \neq \ell$. Then there are a priori two possibilities for z given x and y . However, given s and t , it becomes clear that only one possibility remains. So we just need to find an inequality that selects the correct root of $f(x, y, -)$. One can check that

$$k^2 \ell^2 (k + \ell)^3 \left(z - \frac{-B(x, y)}{2A} \right) = (k^2 - \ell^2) \sqrt{k\ell D(x, y)}^3.$$

So we find that

$$z \leq \frac{-B(x, y)}{2A}$$

when $k < \ell$ and

$$z \geq \frac{-B(x, y)}{2A}$$

when $k > \ell$. This concludes the proof. □

6 The sets \mathcal{B}_n^+ and \mathcal{B}_n^-

We are now ready to prove Theorem 2.1 and the Main Theorem. Let $n \geq 3$ be an integer. Recall the following notation from Sect. 2.

- We have

$$\mathcal{C}_{k,a}^+ = \left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

$$\mathcal{C}_{\ell,b}^- = \left\{ \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 \leq s \leq t \leq 1 \right\} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

for all integers $k, \ell \geq 1$ and $a, b \geq 0$.

- We have $\mathcal{B}_n^+ = \bigcup_{k=1}^{n-1} \mathcal{C}_{k,n-k-1}^+$ and $\mathcal{B}_n^- = \bigcup_{\ell=1}^{n-1} \mathcal{C}_{\ell,n-\ell-1}^-$.
- The set \mathcal{B}_n^b consists of all points $(x, y) \in \mathbb{R}^2$ such that $ny \geq x^2$ and

$$y \leq n - 1 + (x + 2i - (n - 1))^2$$

for each $i \in \{0, \dots, n - 1\}$.

- The projection map $\pi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ sends $(x, y, z) \mapsto (x, y)$.

We start by listing some properties of \mathcal{B}_n^+ and \mathcal{B}_n^- .

Proposition 6.1 *Let $1 \leq k \leq n - 1$ be an integer.*

(a) *The map*

$$\alpha_k : \{(s, t) \mid -1 \leq s \leq t \leq 1\} \rightarrow \pi(\mathcal{C}_{k,n-k-1}^+),$$

$$(s, t) \mapsto k \begin{pmatrix} s \\ s^2 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \end{pmatrix} + (n - k - 1) \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

is a bijection.

- (b) The boundary of $\pi(C_{k,n-k-1}^+)$ is the union of the following three sets:
 $\{\alpha_k(-1, t) \mid -1 \leq t \leq 1\}, \{\alpha_k(s, s) \mid -1 \leq s \leq 1\}, \{\alpha_k(s, 1) \mid -1 \leq s \leq 1\}.$
- (c) We have $\pi(B_n^+) = B_n^b.$
- (d) The projection map

$$B_n^+ \rightarrow B_n^b, \\ (x, y, z) \mapsto (x, y),$$

is a bijection.

Proof To see (a), note that the map clearly is surjective. For injectivity, one has to solve $\alpha_k(s, t) = (x, y)$ for s, t under the condition that $s \leq t$. This yields at most one solution for all (x, y) . For (b), note that the Jacobian of the map α_k has full rank at all points (s, t) with $-1 < t < s < 1$. From (b) follows that the boundary of $\pi(B_n^+)$ is the union of

$$\left\{ n \binom{s}{s^2} \mid -1 \leq s \leq 1 \right\}$$

and

$$\left\{ i \binom{-1}{1} + \binom{t}{t^2} + (n - i - 1) \binom{1}{1} \mid -1 \leq t \leq 1 \right\}$$

for $i = 0, \dots, n - 1$. So the set itself is indeed given by the inequalities defining B_n^b . Finally, to see (d), it suffices to note that $\pi(C_{k,n-k-1}^+ \cap C_{k+1,n-k}^+)$ is equal to

$$\left\{ (k + 1) \binom{s}{s^2} + (n - k - 1) \binom{1}{1} \mid -1 \leq s \leq 1 \right\}$$

for $k = 1, \dots, n - 2$. □

Proposition 6.2 Let $1 \leq \ell \leq n - 1$ be an integer.

- (a) The map
 $\beta_\ell : \{(s, t) \mid -1 \leq s \leq t \leq 1\} \rightarrow \pi(C_{\ell,n-\ell-1}^-),$
 $(s, t) \mapsto \binom{s}{s^2} + \ell \binom{t}{t^2} + (n - \ell - 1) \binom{-1}{1},$
- is a bijection.
- (b) The boundary of $\pi(C_{\ell,n-\ell-1}^-)$ is the union of the following three sets:
 $\{\beta_\ell(-1, t) \mid -1 \leq t \leq 1\}, \{\beta_\ell(t, t) \mid -1 \leq t \leq 1\}, \{\beta_\ell(s, 1) \mid -1 \leq s \leq 1\}.$
- (c) We have $\pi(B_n^-) = B_n^b.$
- (d) The projection map

$$\mathcal{B}_n^- \rightarrow \mathcal{B}_n^b, \\ (x, y, z) \mapsto (x, y),$$

is a bijection.

Proof The proofs are similar to those of Proposition 6.1. □

The decomposition of \mathcal{B}_n^b as a union of the projections of $\mathcal{C}_{1,n-2}^+, \dots, \mathcal{C}_{n-1,0}^+$ is visualized in Fig. 2. We note that the decomposition of \mathcal{B}_n^b as a union of the projections of $\mathcal{C}_{1,n-2}^-, \dots, \mathcal{C}_{n-1,0}^-$ looks similar but is mirrored along the vertical axis.

We can now prove Theorem 2.1.

Proof of Theorem 2.1 We already know that (b) holds by Propositions 6.1 and 6.2. We know that $\mathcal{B}_n^+, \mathcal{B}_n^- \subseteq \mathcal{A}_{3,n}$, we know that the boundary of $\mathcal{A}_{3,n}$ is contained in $\mathcal{B}_n^+ \cup \mathcal{B}_n^-$ by Theorem 4.9 and we know that the projection maps

$$\mathcal{B}_n^+ \rightarrow \mathcal{B}_n^b, \quad \text{and} \quad \mathcal{B}_n^- \rightarrow \mathcal{B}_n^b, \\ (x, y, z) \mapsto (x, y), \quad (x, y, z) \mapsto (x, y),$$

are bijections by Propositions 6.1 and 6.2. Together these statements imply (a). Let $(x, y) \in \mathcal{B}_n^b$ be a point. Then there exist unique numbers $z^+, z^- \in \mathbb{R}$ such that $(x, y, z^+) \in \mathcal{B}_n^+$ and $(x, y, z^-) \in \mathcal{B}_n^-$ by Propositions 6.1 and 6.2. Our goal is to prove that $z^+ \geq z^-$ with equality if and only if (x, y) lies on the boundary of \mathcal{B}_n^b . Let $z \in \mathbb{R}$ be a real number. From (a) and (b) it is clear that $(x, y, z) \in \mathcal{A}_{3,n}$ if and only if z lies between z^+ and z^- . So $z^+ = z^-$ when (x, y) lies on the boundary of \mathcal{B}_n^b . And, to prove that $z^+ > z^-$ otherwise, it suffices to show that there exists a $z \in \mathbb{R}$ such that $z < z^+$ and $(x, y, z) \in \mathcal{A}_{3,n}$. Now, let

$$p = k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + (n - k - 1) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathcal{C}_{k,n-k-1}^+$$

be a point where $-1 \leq s \leq t \leq 1$ and recall Lemmas 4.2 and 4.6. If $-1 < s < t < 1$ and $k = 1$, then there is a point in $\mathcal{A}_{3,3}$ below

$$\begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

and hence a point in $\mathcal{A}_{3,n}$ below p . If $-1 < s < t \leq 1$ and $k \geq 2$, then there is a point in $\mathcal{A}_{3,3}$ below

$$2 \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix}$$

and hence a point in $\mathcal{A}_{3,n}$ below p . Taking into account how the sets $\mathcal{C}_{k,n-k-1}^+$ intersect, we find that there is a point in $\mathcal{A}_{3,n}$ below p unless $s = -1, (k, t) = (1, 1)$ or $(s, k) = (t, n - 1)$, which are exactly the cases where p projects to the boundary of \mathcal{B}_n^b . This proves (c) and (d). Finally, using (a), (c), and Propositions 6.1 and 6.2, we see that the boundary of $\mathcal{A}_{3,n}$ is the disjoint union of several (but not all) sets of the form

$$\left\{ k \begin{pmatrix} s \\ s^2 \\ s^3 \end{pmatrix} + \ell \begin{pmatrix} t \\ t^2 \\ t^3 \end{pmatrix} \mid -1 < s < t < 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

where $k, \ell, a, b \geq 0$ have sum n . Given a point of the boundary, the number s is unique when $k > 0$ and the number t is unique when $\ell > 0$. Together with Proposition 3.1, this shows (e). □

Finally, we prove the Main Theorem.

Proof of the Main Theorem Fix a point $(x, y, z) \in \mathbb{R}^3$. The following conditions are equivalent:

- (a) We have $(x, y) \in \mathcal{B}_n^b$.
- (b) We have $(x, y) \in \pi(\mathcal{C}_{k, n-k-1}^+)$ for some $k \in \{1, \dots, n-1\}$.
- (c) We have $(x, y) \in \pi(\mathcal{C}_{\ell, n-\ell-1}^-)$ for some $\ell \in \{1, \dots, n-1\}$.

Take $k, \ell \in \{1, \dots, n-1\}$. Then, using Proposition 6.1, we see that

$$\pi(\mathcal{C}_{k, n-k-1}^+) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \begin{array}{l} y \leq n-1 + (x+k-(n-k-1))^2 \\ y \geq n-k-1 + (k+1)^{-1}(x-(n-k-1))^2 \\ y \leq n-k+k^{-1}(x-(n-k))^2 \end{array} \right\}$$

and we similarly get

$$\pi(\mathcal{C}_{\ell, n-\ell-1}^-) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \begin{array}{l} y \leq n-1 + (x-\ell+(n-\ell-1))^2 \\ y \geq n-\ell-1 + (\ell+1)^{-1}(x+(n-\ell-1))^2 \\ y \leq n-\ell+\ell^{-1}(x+(n-\ell))^2 \end{array} \right\}$$

using Proposition 6.2. Assume that $(x, y) \in \mathcal{B}_n^b$ and that k, ℓ are as in (b) and (c). Using Theorem 2.1(d), we need to find conditions that express that $z^- \leq z \leq z^+$. We have

$$\begin{aligned} f_{k1}(x-(n-k-1), y-(n-k-1), z^+-(n-k-1)) &= 0, \\ (n-k-1) + \frac{-B_{k1}(x-(n-k-1), y-(n-k-1))}{2A_{k1}} &\leq z^+ \end{aligned}$$

by Theorem 5.2. So $z \leq z^+$ when

$$z \leq (n-k-1) + \frac{-B_{k1}(x-(n-k-1), y-(n-k-1))}{2A_{k1}} =: \theta$$

or

$$f_{k1}(x-(n-k-1), y-(n-k-1), z-(n-k-1)) \leq 0.$$

Note here that the polynomial $f_{k1}(x, y, -)$ has degree 2 in z , that its leading coefficient is positive, that z^+ is its highest root and that it attains its minimum at θ . This is visualized in Fig. 3. We also have

$$f_{1\ell}(x + (n - \ell - 1), y - (n - \ell - 1), z^- + (n - \ell - 1)) = 0,$$

$$-(n - \ell - 1) + \frac{-B_{1\ell}(x + (n - \ell - 1), y - (n - \ell - 1))}{2A_{1\ell}} \geq z^-$$

by Theorem 5.2 and from this we conclude that $z \geq z^-$ if and only if

$$z \geq -(n - \ell - 1) + \frac{-B_{1\ell}(x + (n - \ell - 1), y - (n - \ell - 1))}{2A_{1\ell}}$$

or

$$f_{1\ell}(x + (n - \ell - 1), y - (n - \ell - 1), z + (n - \ell - 1)) \leq 0.$$

This leads to the semi-algebraic description of the Main Theorem. □

7 Higher dimensions

The Main Theorem provides a semi-algebraic description of the set $\mathcal{A}_{3,n}$ for each integer $n \geq 3$. So, a natural question to ask is: can we use the same proof strategy to find a semi-algebraic description of the sets $\mathcal{A}_{k,n}$ for $k > 3$? At the moment, there still are some obstacles to doing so, which we discuss in this section.

Following the same strategy as for $k = 3$, we would again start by trying to find a description of the boundary of $\mathcal{A}_{k,n}$. One can check that the statement and proof of Proposition 3.1 carry over in a straightforward fashion for $k > 3$, which yields a superset of the boundary. After this, one would again need to exclude points from this superset when they do not in fact lie on the boundary. In view of Theorem 2.1(d), proving that a point in $\mathcal{A}_{3,n}$ does not lie on the boundary can be done by showing that there are points in $\mathcal{A}_{3,n}$ above and below it. So an analogue of Theorem 2.1(d) for higher dimensions would be very useful. This leads to the following conjecture, which holds for $k \leq 3$.

Conjecture 7.1 *Let (x_1, \dots, x_k) be a point in $\mathcal{A}_{k,n}$. Then the set*

$$\{y \in \mathbb{R} \mid (x_1, \dots, x_{k-1}, y) \in \mathcal{A}_{k,n}\}$$

is a closed interval.

Another approach might be through a generalization of Theorem 2.1(e). The boundary of $\mathcal{A}_{k,n}$ is contained in the union of the sets

$$\left\{ \ell_1 \begin{pmatrix} t_1 \\ t_1^2 \\ \vdots \\ t_1^k \\ 1 \end{pmatrix} + \dots + \ell_{k-1} \begin{pmatrix} t_{k-1} \\ t_{k-1}^2 \\ \vdots \\ t_{k-1}^k \\ 1 \end{pmatrix} \mid -1 < t_1 < \dots < t_{k-1} < 1 \right\} + a \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + b \begin{pmatrix} -1 \\ (-1)^2 \\ \vdots \\ (-1)^k \end{pmatrix}$$

over all integers $\ell_1, \dots, \ell_{k-1}, a, b \geq 0$ that sum to n . The uniqueness of the representation of each point on the boundary would imply that the boundary of $\mathcal{A}_{k,n}$ is a disjoint union of

some of these sets. It would also be a tool to eliminate some of these sets from consideration. This leads to our second conjecture, which also holds for $k \leq 3$.

Conjecture 7.2 *Every point on the boundary of $\mathcal{A}_{k,n}$ can be written as*

$$\begin{pmatrix} t_1 \\ t_1^2 \\ \vdots \\ t_1^k \end{pmatrix} + \dots + \begin{pmatrix} t_n \\ t_n^2 \\ \vdots \\ t_n^k \end{pmatrix}$$

for some tuple $(t_1, \dots, t_n) \in [-1, 1]^n$. The set $\{t_1, \dots, t_n\} \setminus \{-1, 1\}$ has at most $k - 1$ elements and the tuple (t_1, \dots, t_n) is unique up to permutation of its entries.

Apart from finding the boundary of $\mathcal{A}_{k,n}$, there is also the problem of describing it semi-algebraically. When one would attempt this, the main obstacle to overcome is, in our opinion, finding an analogue of Theorem 5.2. For $k = 4$, this means we need to solve the following problem.

Problem 7.3 *Determine a semi-algebraic description of the set*

$$\left\{ \ell_1 \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \\ t_1^4 \end{pmatrix} + \ell_2 \begin{pmatrix} t_2 \\ t_2^2 \\ t_2^3 \\ t_2^4 \end{pmatrix} + \ell_3 \begin{pmatrix} t_3 \\ t_3^2 \\ t_3^3 \\ t_3^4 \end{pmatrix} \mid -1 \leq t_1 \leq t_2 \leq t_3 \leq 1 \right\}$$

given the integers $\ell_1, \ell_2, \ell_3 \geq 1$.

These sets are expected to be the building blocks for the boundary of $\mathcal{A}_{4,n}$, so a solution to this problem seems essential if we want to apply the same approach we used for $\mathcal{A}_{3,n}$. Using elimination theory, we find that the Zariski closure of this set is a hypersurface defined by a single polynomial $f_{\ell_1, \ell_2, \ell_3}(x_1, x_2, x_3, x_4)$. This polynomial is homogeneous of degree 24 with respect to the grading where $\deg(x_i) = i$ and has 169 terms. Its coefficients are symmetric polynomials in ℓ_1, ℓ_2, ℓ_3 of degree up to 18. When $\#\{\ell_1, \ell_2, \ell_3\} \leq 2$, the polynomial is a square. And, we have

$$f_{\ell, \ell, \ell}(x_1, x_2, x_3, x_4) = (-x_1^4 + 6\ell x_1^2 x_2 - 3\ell^2 x_2^2 - \ell^2 8x_1 x_3 + 6\ell^3 x_4)^6.$$

This suggests that we should first solve

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \ell_1 \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \end{pmatrix} + \ell_2 \begin{pmatrix} t_2 \\ t_2^2 \\ t_2^3 \end{pmatrix} + \ell_3 \begin{pmatrix} t_3 \\ t_3^2 \\ t_3^3 \end{pmatrix}$$

for t_1, t_2, t_3 and then solve $f_{\ell_1, \ell_2, \ell_3}(x_1, x_2, x_3, x_4) = 0$ for x_4 . As this only involves solving polynomial equations of degree ≤ 4 , this is theoretically doable. The problem however is to express the inequalities $-1 \leq t_1 \leq t_2 \leq t_3 \leq 1$ as polynomial inequalities in x_1, x_2, x_3, x_4 .

As an example, consider the case $\ell_1 = \ell_2 = \ell_3 = 1$. In this case, the set is contained in the hypersurface given by the equation

$$x_1^4 - 6x_1^2 x_2 + 3x_2^2 + 8x_1 x_3 - 6x_4 = 0,$$

which allows to eliminate the coordinate x_4 . So here, the problem consists of finding a semi-algebraic description of the set

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} t_1 \\ t_1^2 \\ t_1^3 \end{pmatrix} + \begin{pmatrix} t_2 \\ t_2^2 \\ t_2^3 \end{pmatrix} + \begin{pmatrix} t_3 \\ t_3^2 \\ t_3^3 \end{pmatrix} \mid -1 \leq t_1 \leq t_2 \leq t_3 \leq 1 \right\}$$

given $x_1, x_2, x_3 \in \mathbb{R}$.

If we can solve Problem 7.3, we still need to find analogues for the results in Sect. 6. These results rely on our complete understanding of the roots and extrema of parabolas. So to generalize these results, we probably need a similar level of understanding in the cases of cubics and quartics, which for now seems to be out of reach.

Acknowledgements Open Access funding provided by Projekt DEAL. The problem that this paper solves was brought to our attention by Bernd Sturmfels during the graduate student meeting on applied algebra and combinatorics held in Leipzig on 18–20 February 2019. We would like to thank him for doing so and we would like to thank the organizers of this meeting for making it possible. We would also like to thank Peter Sarnak for explaining the origin and relevance of the problem to us. Lastly, we would like to thank the anonymous referees for their precise reading of our paper and their helpful comments.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Chang, A., Mehrle, D., Miller, S.J., Reiter, T., Stahl, J., Yott, D.: Newman's conjecture in function fields. *J. Number Theory* **157**, 154–169 (2015)
2. Dou, Z.-L., Zhang, Q.: *Six Short Chapters on Automorphic Forms and L-functions*. Springer, Berlin (2012)
3. Hu, P.-C., Wu, A.-D.: Zero distribution of Dirichlet L -functions. *Ann. Acad. Sci. Fenn. Math.* **41**, 775–788 (2016)
4. Miller, G.L.: Riemann's hypothesis and tests for primality. *J. Comput. Syst. Sci.* **13**(3), 300–317 (1976)
5. Miller, S.J.: An orthogonal test of the L -functions Ratios conjecture. *Proc. Lond. Math. Soc.* **99**(2), 484–520 (2009)
6. Riemann, B.: Über die Anzahl der Primzahlen unter einer gegebenen Größe, *Monatsberichte der Berliner Akademie* (November 1859)
7. Rubinstein, M. O., Sarnak, P.: The underdetermined matrix moment Problem I, in preparation

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.