The Inverse Moment Problem for Convex Polytopes

**Nick Gravin · Jean Lasserre ·
Dmitrii V. Pasechnik · Sinai Robins**

Abstract We present a general and novel approach for the reconstruction of any convex d-dimensional polytope P, assuming knowledge of finitely many of its integral moments. In particular, we show that the vertices of an N-vertex convex polytope in $\mathbb{R}^d$ can be reconstructed from the knowledge of $O(DN)$ axial moments (w.r.t. to an unknown polynomial measure of degree D), in $d + 1$ distinct directions in general position. Our approach is based on the collection of moment formulas due to Brion, Lawrence, Khovanskii–Pukhlikov, and Barvinok that arise in the discrete geometry of polytopes, combined with what is variously known as Prony's method, or the Vandermonde factorization of finite rank Hankel matrices.

Keywords Inverse moment problem · Polytopes ·
Brion–Lawrence–Khovanskii–Pukhlikov–Barvinok formula · Axial moments

1 Introduction

The *inverse* problem of recognizing an object from its given moments is a fundamental and important problem in both applied and pure mathematics. For example, this problem arises quite often in computer tomography, inverse potentials, signal processing, and statistics and probability. In computer tomography, for instance, the

N. Gravin · D.V. Pasechnik (✉) · S. Robins
School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore, Singapore
e-mail: dima@ntu.edu.sg

J. Lasserre
LAAS-CNRS, 7 Avenue du Colonel Roche, 31 077 Toulouse Cedex 4, France

N. Gravin
Steklov Institute of Mathematics at St. Petersburg, 27 Fontanka, St. Petersburg 191023, Russia

X-ray images of an object can be used to estimate the moments of the underlying mass distribution, from which one seeks to recover the shape of the object that appear on some given images. In gravimetry applications, the measurements of the gravitational field can be converted into information concerning the moments, from which one seeks to recover the shape of the source of the anomaly.

The goal of this paper is to present a general and novel approach for the reconstruction of any convex d-dimensional polytope P, from knowledge of its moments. Our approach is quite different from the quadrature-based approach that is currently used in the literature. Our starting point is the collection of moment formulas, due to Brion–Barvinok–Khovanskii–Lawrence–Pukhlikov (in what follows referred for brevity as BBaKLP) that arises in the discrete geometry of polytopes, and is valid for all dimensions [1, 2, 8, 15], and [7, Chap. 10]. We then set up a matrix equation involving a variable Vandermonde matrix, with an associated Hankel matrix whose kernel helps us reconstruct the vertices of P. We are also able to reconstruct the vertices of a convex polytope with variable density, using similar methods [17].

This new approach permits us to reconstruct *exactly* the vertices of P, using very few moments, relative to the vertex description of P. While the computation of integrals over polytopes has received attention recently (see e.g. [4]), our work appears to be the first to provide tools to treat the inverse moment problem in general.

A nice feature of our algorithm is that we do not need to know a priori the number of vertices of P, only a rough upper bound for their number. The algorithm automatically retrieves the number of vertices of P as the rank of a certain explicit Hankel matrix.

In fact, a surprising corollary is that we only require $O(Nd)$ moments in order to reconstruct all of the N vertices of $P \subset \mathbb{R}^d$. Suppose we are solving the inverse moment problem in the context of an unknown density function ρ. An interesting consequence of our algorithm is that even though ρ is unknown, we may easily adapt our algorithm to recover the vertices of P in $O(Nd^o d)$ steps, where d^o is an upper bound on the degree of ρ.

Now suppose we simply solve the direct problem of writing down the moments of a given vertex set of a known polytope, with a known polynomial density function ρ. In this direct problem, it would take $\binom{d^o+d}{d}$ data to describe the polynomial ρ function, because the space of possible polynomials ρ has this dimension. However, for the inverse problem, where ρ is unknown, perhaps a counter-intuitive consequence of our algorithm is that we only require $O(Nd^o d)$ data to recover the vertex set of P, which might be smaller than $\binom{d^o+d}{d}$.

In the existing literature on inverse problems from moments, one immediately encounters a sharp distinction between the 2-dimensional case and the general d-dimensional case, with $d > 2$. While in the former case a well-known quadrature formula allows us to solve the problem exactly for so-called quadrature domains, where for the latter case one has to "slice up" the domain of interest into thin 2-dimensional pieces, solve the resulting 2-dimensional problems, and patch up an approximate solution from these 2-dimensional solutions. On the other hand, in the recent work of Cuyt et al. [9] the authors can approximately recover a general n-dimensional shape by using an interesting property of multi-dimensional Padé approximants.

For $\mathbf{z} \in \mathbb{R}^d$ and each non-negative integer j, we define the jth *moment* of P with respect to the density ρ by

$$\mu_j(\mathbf{z}) := \mu_{j,\rho}(\mathbf{z}) := \int_P \langle \mathbf{x}, \mathbf{z} \rangle^j \rho(\mathbf{x}) \, d\mathbf{x}.$$

In this text we restrict ourselves to any density function ρ which is given by a polynomial measure, and which does not vanish on the vertices $\mathrm{Vert}(P)$ of P.

We note that only in the appendix, when we give proofs of the known BBaKLP moment formulas below, we will need to replace the real vector $\mathbf{z}$ by a complex vector, in order to allow convergence of some Fourier–Laplace transforms of cones, but otherwise $\mathbf{z}$ will always be a real vector. We say that $\mathbf{z}$ is in *general position* if it is chosen at random from the continuous Gaussian distribution on $\mathbb{R}^d$.

Our main result may be formulated as follows.

Main Theorem *Let $P \subset \mathbb{R}^d$ be a d-dimensional polytope with N vertices, and suppose we are only given the data in the form of $O(d_\rho N)$ moments $\mu_{j,\rho}(\mathbf{z})$, for an unknown density $\rho \in \mathbb{R}[\mathbf{x}]$ of degree d_ρ, and for each of $d+1$ vectors $\mathbf{z} \in \mathbb{R}^d$ in general position. Then the data determine P uniquely, using the following algorithm*:

1. *Given $2m - 1 \geq 2N + 1$ moments $c_1, \ldots, c_{2m-1}$ for $\mathbf{z}$, construct a square Hankel matrix $\mathbf{H}(c_1, \ldots, c_{2m-1})$.*
2. *Find the vector $v = (a_0, \ldots, a_{M-1}, 1, 0, \ldots, 0)$ in $\mathrm{Ker}(\mathbf{H})$ with the minimal possible M. It turns out that the number of vertices N is in fact equal to M.*
3. *The set of roots $\{x_i(\mathbf{z}) = \langle \mathbf{v}_i, \mathbf{z} \rangle | \mathbf{v}_i \in \mathrm{Vert}(P)\}$ of the polynomial $p_\mathbf{z}(t) = t^N + \sum_{i=0}^{N-1} a_i t^i$ then equals the set of projections of $\mathrm{Vert}(P)$ onto $\mathbf{z}$.*

By contrast with a choice of a general position vector $\mathbf{z}$, we also define, for a simple polytope P, a *generic vector* $\mathbf{z} \in \mathbb{Q}^d$ to be a vector that lies in the complement of the finite union of hyperplanes which are orthogonal to all of the edges of P. For non-simple polytopes P, we will later extend this definition of a generic vector $\mathbf{z} \in \mathbb{Q}^d$, in Sect. 7.

We furthermore prove in Sect. 8 that the vertex set $\mathrm{Vert}(P) \subset \mathbb{Q}^d$ of any rational convex polytope P can be found in polynomial time with a probability arbitrary close to 1, from the exact measurements of $O(d_\rho N)$ moments in carefully chosen $2d - 1$ random generic directions $\mathbf{z} \in \mathbb{Q}^d$.

In Sect. 6, we indicate how $\mathrm{Vert}(P) \subset \mathbb{R}^d$ can also be efficiently approximated even when the data are noisy.

One punchline of the proof is that an appropriate scaling of the sequence of the moments $\mu_{j,\rho}(\mathbf{z})$ $(j = 0, 1, \ldots)$ for a fixed $\mathbf{z}$ is a finite sum of exponential functions, and thus satisfies a linear recurrence relation (cf. e.g. [19, Theorem 4.1.1(iii)]). Then an application of what is variously known as Prony's method, or Vandermonde factorization of a finite rank Hankel matrix (cf. e.g. [5]), allows one to find $\langle \mathbf{z}, \mathbf{v} \rangle$ for $\mathbf{v} \in \mathrm{Vert}(P)$. As these methods are scattered along quite a number of sources, we have chosen to present a self-contained exposition for clarity and for ease of efficient implementation.

Reconstructing $\mathrm{Vert}(P)$ from the $\langle \mathbf{z}, \mathbf{v} \rangle$ is then relatively straightforward, provided that we know these projections for sufficiently many $\mathbf{z}$ in general position. For the

latter, we present an exact procedure as well as a parametric one—the latter with the focus being less noise-sensitive.

The remainder of the paper is organized as follows. In Sect. 2, we define the objects we are dealing with, as well as the appropriate background for ease of reading. We also give the known formulas for the moments of simple polytopes. In Sect. 3 we construct a polynomial whose roots correspond to the projections of the vertices onto directions $\mathbf{z}$ in general positions, by using the moment formulas and an associated Hankel matrix. In Sect. 4 we extend the latter to the case of unknown polynomial measures. In Sects. 5 and 6, we extend the algorithm from Sects. 3 and 4, which deals with simple polytopes, to all convex polytopes. This completes the proof of the first claim of Main Theorem. In Sect. 4 we also discuss the question of reconstructing ρ after Vert(P) is found.

In Sect. 8 we use univariate polynomials to paste together the projections retrieved from Sect. 3 to build up all of the coordinates of each vertex, not just their projections, completing the proof of the second claim of Main Theorem. In Appendix 9 we outline some proofs of the known BBaKLP moment formulas from Sect. 2, using Fourier techniques.

2 Definitions and Moment Formulas for Convex, Rational Polytopes

Here we describe an explicit set of formulas for the moments of any convex polytope $P \subset \mathbb{R}^d$. We begin with some combinatorial-geometric definitions of the objects involved. To fix notation, our convex polytope P will always have N vertices. We say that P is *simple* if each vertex $\mathbf{v}$ of P is incident with exactly d edges of P. We first treat the case of a simple convex polytope and then later, in Sect. 5 we provide an extension to non-simple convex polytopes.

There is an elegant and useful formulation, originally due to BBaKLP [15], for the moments of any simple polytope in $\mathbb{R}^d$, in terms of its vertex and edge data. Specifically, let the set of all vertices of P be given by Vert(P). For each $\mathbf{v} \in \text{Vert}(P)$, we consider a fixed set of vectors, parallel to the edges of P that are incident with $\mathbf{v}$, and call these edge vectors $w_1(\mathbf{v}), \ldots, w_d(\mathbf{v})$. Geometrically, the polyhedral cone generated by the non-negative real span of these edges at $\mathbf{v}$ is called the tangent cone at $\mathbf{v}$, and is written as $K_{\mathbf{v}}$. For each simple tangent cone $K_{\mathbf{v}}$, we let $|\det K_{\mathbf{v}}|$ be the volume of the parallelepiped formed by the d edge vectors $w_1(\mathbf{v}), \ldots, w_d(\mathbf{v})$. Thus, $|\det K_{\mathbf{v}}| = |\det(w_1(\mathbf{v}), \ldots, w_d(\mathbf{v}))|$, the determinant of this parallelepiped.

The following results of BBaKLP [15] give the moments of a simple polytope P in terms of the local vertex and tangent cone data that we described above. For each integer $j \geq 0$, we have

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d)!} \sum_{\mathbf{v} \in \text{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^{j+d} D_{\mathbf{v}}(\mathbf{z}), \tag{1}$$

where

$$D_{\mathbf{v}}(\mathbf{z}) := \frac{|\det K_{\mathbf{v}}|}{\prod_{k=1}^d \langle w_k(\mathbf{v}), \mathbf{z} \rangle}, \tag{2}$$

for each $\mathbf{z} \in \mathbb{R}^d$ such that the denominators in $D_{\mathbf{v}}(\mathbf{z})$ do not vanish. Moreover, we also have the following companion identities:

$$0 = \sum_{v \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^j D_{\mathbf{v}}(\mathbf{z}), \tag{3}$$

for each $0 \le j \le d - 1$. Thus, for example, if $\mathbf{z} = (1, 0, \ldots, 0)$, (1) and (3) deal with the first coordinate of each of the vertices $\mathbf{v} \in \mathrm{Vert}(P)$. We also note that all of these formulas involve only homogeneous, rational functions of $\mathbf{z} = (z_1, \ldots, z_d)$.

In the more general case of non-simple polytopes, we may triangulate each tangent cone into simple cones, thereby getting a slightly more general form of (1) above, namely:

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d)!} \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^{j+d} \tilde{D}_{\mathbf{v}}(\mathbf{z}), \tag{4}$$

where each $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ is a rational function that now comes from the non-simple tangent cone at $\mathbf{v}$. We note that $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ is in fact a sum of the relevant rational functions $D_{\mathbf{v}}(\mathbf{z})$ that are associated to each simple cone in the triangulation of the non-simple tangent cone $K_{\mathbf{v}}$.

Throughout the paper, we will mainly work in the context of a continuous domain for our choices of admissible $\mathbf{z}$ vectors. To be precise, we say that a vector $\mathbf{z}$ is in *general position* if none of the following conditions is true:

(a) $\mathbf{z}$ is a zero or a pole of $\tilde{D}_{\mathbf{v}}(\mathbf{z})$, for any $\mathbf{v} \in \mathrm{Vert}(P)$.
(b) There exist two vertices $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{Vert}(P)$ such that $\langle \mathbf{v}_1, \mathbf{z} \rangle = \langle \mathbf{v}_2, \mathbf{z} \rangle$.

In the penultimate section, we indicate how to implement our algorithm by transitioning all of our formulas to a rational context, and picking our $\mathbf{z}$ vectors to lie in a finite, rational d-dimensional cube.

The goal here is to reconstruct the polytope P from a given sequence of moments $\{\mu_j(\mathbf{z}) \mid j = 1, 2, 3, \ldots\}$. That is, we wish to find an explicit algorithm that locates the vertices v of the polytope P, in terms of the moments of P. To emphasize the fact that the moment equations above can be put into matrix form, we define our scaled vector of moments by

$$(c_1, \ldots, c_{k+1}) = \left(0, \ldots, 0, \frac{d!(-1)^d}{0!} \mu_0, \frac{(1+d)!(-1)^d}{1!} \mu_1, \ldots, \frac{k!(-1)^d}{(k-d)!} \mu_{k-d} \right), \tag{5}$$

so that the vector $\mathbf{c} = (c_1, \ldots, c_{k+1})$ has zeros in the first d coordinates, and scaled moments in the last $k + 1 - d$ coordinates. Thus, putting the moment identities (1) and (3) above into matrix form, we have

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \langle \mathbf{v}_1, \mathbf{z} \rangle & \langle \mathbf{v}_2, \mathbf{z} \rangle & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle \\ \langle \mathbf{v}_1, \mathbf{z} \rangle^2 & \langle \mathbf{v}_2, \mathbf{z} \rangle^2 & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle^2 \\ \vdots & \vdots & \ldots & \vdots \\ \langle \mathbf{v}_1, \mathbf{z} \rangle^k & \langle \mathbf{v}_2, \mathbf{z} \rangle^k & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle^k \end{pmatrix} \begin{pmatrix} D_{\mathbf{v}_1}(\mathbf{z}) \\ \vdots \\ D_{\mathbf{v}_N}(\mathbf{z}) \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_{k+1} \end{pmatrix}. \tag{6}$$

Recalling that we seek to find the vertices of the convex polytope P with these given scaled moments c_i, we answer this question completely, giving an efficient algorithm to recover the vertices of such an object P.

We will treat each $D_{\mathbf{v}_i}(\mathbf{z})$ as a nonzero constant, which we have not yet discovered, and each $\langle \mathbf{v}_j, \mathbf{z} \rangle$ as a variable, for a fixed real vector $\mathbf{z} \in \mathbb{R}^d$. Moreover, we realize below that, given our algorithm, only finitely many moments $\mu_1(\mathbf{z}), \ldots, \mu_M(\mathbf{z})$ are needed in order to completely recover the full vertex set Vert(P), a rather useful fact for applications.

We recall that our jth moment of P is defined, for the uniform measure $\rho \equiv 1$, by

$$\mu_j(\mathbf{z}) = \int_P \langle \mathbf{x}, \mathbf{z} \rangle^j \, d\mathbf{x}. \tag{7}$$

We note that $\mu_0(\mathbf{z}) = \text{Vol}(P)$, the volume of P with respect to the usual Lebesgue measure.

It is very natural to study moments in this form, because they are "basis-free" and also appear as moments of inertia in physical applications. It is worth noting that there are other types of moments in the literature, and we mention some connections here. For each integer vector $\mathbf{m}$, we define

$$\mu_{\mathbf{m}} = \int_P \mathbf{x}^{\mathbf{m}} \, d\mathbf{x}, \tag{8}$$

with the usual convention that $\mathbf{x}^{\mathbf{m}} = \prod_{i=1}^d x_i^{m_i}$ and $|\mathbf{m}| = m_1 + \cdots + m_d$. The usual application of the binomial theorem gives us a trivial relation between these moments:

$$\langle \mathbf{z}, \mathbf{x} \rangle^k = \sum_{\substack{m_1, \ldots, m_d: \\ m_1 + \cdots + m_d = k}} \binom{k}{m_1, \ldots, m_d} z_1^{m_1} \cdots z_d^{m_d} x_1^{m_1} \cdots x_d^{m_d}. \tag{9}$$

In fact, given Vert(P) and $\mu_{|\mathbf{m}|}(\mathbf{z})$ as a function of $\mathbf{z}$, we can also compute $\mu_{\mathbf{m}}$, as following Lemma shows. Its proof is trivial , but it nevertheless offers an interesting relation between the moments (7) and (8).

Lemma 1 *Let* $\mathbf{m} \in \mathbb{Z}_+^d$, Vert$(P)$, *and* $\mu_{|\mathbf{m}|}(\mathbf{z})$ *be given. Then*

$$|m|! \mu_{\mathbf{m}} = \frac{\partial^{|\mathbf{m}|}}{\partial \mathbf{z}^{\mathbf{m}}} \mu_{|\mathbf{m}|}(\mathbf{z}).$$

3 The Inverse Moment Problem for Polytopes—Computing Projections of Vert(P)

In this section we show how, for a given general position vector $\mathbf{z}$, to retrieve the projections $\langle \mathbf{v}, \mathbf{z} \rangle$ for each vertex $\mathbf{v}$ of P, using a certain Hankel matrix that we define below. For the sake of convenience we let $x_i = \langle \mathbf{v}_i, \mathbf{z} \rangle$, for each $1 \leq i \leq N$. Thus, our

goal for this section is to find all x_i, given a number of moments. Due to our choice of $\mathbf{z}$, we may assume that $x_i \neq x_j$ for $i \neq j$. From (6) we have

$$
\begin{pmatrix}
1 & 1 & \ldots & 1 \\
x_1 & x_2 & \ldots & x_N \\
x_1^2 & x_2^2 & \ldots & x_N^2 \\
\vdots & \vdots & \ldots & \vdots \\
x_1^k & x_2^k & \ldots & x_N^k
\end{pmatrix}
\begin{pmatrix}
D_{\mathbf{v}_1}(\mathbf{z}) \\
\vdots \\
D_{\mathbf{v}_N}(\mathbf{z})
\end{pmatrix}
=
\begin{pmatrix}
c_1 \\
\vdots \\
c_{k+1}
\end{pmatrix},
\tag{10}
$$

where $\mathbf{c}$ is defined by (5) above. To streamline notation further, we define a $(k+1) \times N$ Vandermonde matrix $\mathbf{V}_k(x_1, \ldots, x_N)$, with ijth entry equal to x_j^{i-1}:

$$
\mathbf{V}_k(x_1, \ldots, x_N) =
\begin{pmatrix}
1 & 1 & \ldots & 1 \\
x_1 & x_2 & \ldots & x_N \\
x_1^2 & x_2^2 & \ldots & x_N^2 \\
\vdots & \vdots & \ldots & \vdots \\
x_1^k & x_2^k & \ldots & x_N^k
\end{pmatrix}.
\tag{11}
$$

We also define a column vector $\mathbf{D}(\mathbf{z}) = (D_{\mathbf{v}_1}(\mathbf{z}), \ldots, D_{\mathbf{v}_N}(\mathbf{z}))^\top$, so that (6) reads

$$
\mathbf{V}_k(x_1, \ldots, x_N) \cdot \mathbf{D}(\mathbf{z}) = \mathbf{c}.
$$

We may multiply both sides of (10) on the left by a row vector $\mathbf{a} = (a_0, a_1, \ldots, a_k)$. First, we see that

$$
\mathbf{a} \cdot \mathbf{V}_k(x_1, x_2, \ldots, x_N) = \big(q_{\mathbf{a}}(x_1), q_{\mathbf{a}}(x_2), \ldots, q_{\mathbf{a}}(x_N)\big), \quad \text{where } q_{\mathbf{a}}(t) = \sum_{\ell=0}^{k} a_\ell t^\ell.
$$

Therefore, taking $\mathbf{a}$ to be the coefficient vector of the polynomial

$$
p_{\mathbf{z}}(t) = \prod_{i=1}^{N} (t - x_i) = \prod_{\mathbf{v} \in \mathrm{Vert}(P)} \big(t - \langle \mathbf{v}, \mathbf{z} \rangle\big) = t^N + \sum_{i=0}^{N-1} a_i t^i,
\tag{12}
$$

and multiplying (10) by $\mathbf{a}$, we obtain the identity $0 = \mathbf{a} \cdot \mathbf{c}$. Moreover, for each $0 \leq \ell \leq k - N$ we substitute for $\mathbf{a}$ the vector $\mathbf{a}_\ell$ corresponding to $t^\ell p_{\mathbf{z}}(t)$, to obtain zero in (10), when multiplying on the left by $\mathbf{a}_\ell$. We thus obtain $k - N + 1$ equations of the form

$$
\mathbf{a}_\ell \cdot \mathbf{c} = 0.
\tag{13}
$$

As ℓ increases, the coefficient vector of $t^\ell p_{\mathbf{z}}(t)$ gets shifted to the right, and it is convenient to capture all of its shifts simultaneously by the $m \times m$ Hankel matrix

$\mathbf{H} := \mathbf{H}(c_1, \ldots, c_{2m-1})$, where we fix $m \geq N + 1$, defined by

$$\mathbf{H}(c_1, \ldots, c_{2m-1}) = \begin{pmatrix} c_1 & c_2 & \cdots & c_m \\ c_2 & c_3 & \cdots & c_{m+1} \\ \vdots & \vdots & \cdots & \vdots \\ c_m & c_{m+1} & \cdots & c_{2m-1} \end{pmatrix}. \tag{14}$$

Theorem 1 *The Hankel matrix $\mathbf{H}$ has rank N and its kernel is spanned by the $m - N$ linearly independent vectors*

$$\mathbf{a}_\ell = (\underbrace{0, \ldots, 0}_{\ell \text{ times}}, a_0, \ldots, a_{N-1}, 1, \underbrace{0, \ldots, 0}_{m-N-1-\ell}), \quad 0 \leq \ell \leq m - N - 1. \tag{15}$$

Proof For each ℓ in the range $0 \leq \ell \leq 2m - 2 - N$ we use (13), with a vector $\mathbf{a}_\ell$ of length $2m - 1$. Putting all of these equations together in a more compact form, we can write $\mathbf{a}_\ell \mathbf{H} = 0$, where now the length of $\mathbf{a}_\ell$ is m.

It remains to show that the vectors $\mathbf{a}_\ell$ generate the full kernel Ker($\mathbf{H}$) of $\mathbf{H}$. Let $\mathbf{b}' \in$ Ker($\mathbf{H}$). Without loss of generality, there exists an $L < N$ such that $\mathbf{b}' = (b_0, \ldots, b_{L-1}, 1, 0, \ldots, 0)$, because we may use the various vectors $\mathbf{a}_\ell$, which lie in the kernel of $\mathbf{H}$ to get the appropriate zeros in this $\mathbf{b}'$ vector.

Now let us define a number of row vectors of the size $2m - 1$:

$$\mathbf{b}_\ell = (\underbrace{0, \ldots, 0}_{\ell \text{ times}}, b_0, \ldots, b_{L-1}, 1, \underbrace{0, \ldots, 0}_{2m-2-L-\ell}), \quad 0 \leq \ell \leq 2m - L - 2. \tag{16}$$

By definition of the Hankel matrix and since $m > L + 1$, we have $\mathbf{b}_\ell \cdot \mathbf{c} = 0$. Consider the polynomial $p_\mathbf{b}(t) = b_0 + b_1 t + \cdots + b_{L-1} t^{L-1} + t^L$ corresponding to $\mathbf{b}_0$.

Taking $k = 2m - 2$ in (10), we multiply both sides of (10) on the left by $\mathbf{b}_\ell$. Hence, we get $\mathbf{b}_\ell \cdot \mathbf{V}_{2m-2}(x_1, \ldots, x_N) \cdot \mathbf{D} = 0$. Therefore, for every $0 \leq \ell \leq 2m - L - 2$ we have

$$\left(x_1^\ell p_\mathbf{b}(x_1), \ldots, x_N^\ell p_\mathbf{b}(x_N) \right) \cdot \mathbf{D} = 0. \tag{17}$$

Combining the first N of the latter equations into a matrix form (note that $N - 1 < 2m - L - 2$) we get

$$\begin{pmatrix} p_\mathbf{b}(x_1) & \cdots & p_\mathbf{b}(x_N) \\ x_1 p_\mathbf{b}(x_1) & \cdots & x_N p_\mathbf{b}(x_N) \\ x_1^2 p_\mathbf{b}(x_1) & \cdots & x_N^2 p_\mathbf{b}(x_N) \\ \vdots & \cdots & \vdots \\ x_1^{N-1} p_\mathbf{b}(x_1) & \cdots & x_N^{N-1} p_\mathbf{b}(x_N) \end{pmatrix} \begin{pmatrix} D_{\mathbf{v}_1}(\mathbf{z}) \\ \vdots \\ D_{\mathbf{v}_N}(\mathbf{z}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

which can be rewritten as

$$
\begin{pmatrix}
1 & \cdots & 1 \\
x_1 & \cdots & x_N \\
x_1^2 & \cdots & x_N^2 \\
\vdots & \cdots & \vdots \\
x_1^{N-1} & \cdots & x_N^{N-1}
\end{pmatrix}
\begin{pmatrix}
p_{\mathbf{b}}(x_1) & 0 & \cdots & 0 \\
0 & p_{\mathbf{b}}(x_2) & \cdots & 0 \\
\vdots & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & p_{\mathbf{b}}(x_N)
\end{pmatrix}
\begin{pmatrix}
D_{\mathbf{v}_1}(\mathbf{z}) \\
\vdots \\
D_{\mathbf{v}_N}(\mathbf{z})
\end{pmatrix}
=
\begin{pmatrix}
0 \\
\vdots \\
0
\end{pmatrix}.
$$

Since $\mathbf{V}_{N-1}(x_1, \ldots, x_N)$ is invertible, we get

$$
\begin{pmatrix}
p_{\mathbf{b}}(x_1) D_{\mathbf{v}_1}(\mathbf{z}) \\
\vdots \\
p_{\mathbf{b}}(x_N) D_{\mathbf{v}_N}(\mathbf{z})
\end{pmatrix}
=
\begin{pmatrix}
0 \\
\vdots \\
0
\end{pmatrix}.
$$

As $L < N$ and $p_{\mathbf{b}}(t) \neq 0$, we deduce that $x_1, \ldots, x_N$ cannot all be roots of $p_{\mathbf{b}}(t)$. It remains to mention that $D_{\mathbf{v}_i}(\mathbf{z}) \neq 0$ for every $1 \leq i \leq N$, by the choice of the vector $\mathbf{z}$ in general position. We therefore arrive at a contradiction. □

Once we construct the kernel of $\mathbf{H}$, we will pick a vector $(a_0, \ldots, a_{N-1}, 1, 0, \ldots, 0)$ in $\mathrm{Ker}(\mathbf{H})$, and then define the polynomial $p_{\mathbf{z}}(t) = a_0 + a_1 t + \cdots + a_{N-1} t^{N-1} + t^N$. We note that this is the unique vector with the largest number of zeros on the right (in algebraic terms, all the remaining vectors in the kernel can be obtained as coefficients of polynomials in the principal ideal $(p_{\mathbf{z}}) \subset \mathbb{C}[t]$). By Theorem 1, the roots $x_i (= \langle \mathbf{v}_i, \mathbf{z} \rangle)$ of this polynomial are precisely the projections $\langle \mathbf{v}_i, \mathbf{z} \rangle$ that we are seeking:

$$
p_{\mathbf{z}}(t) = a_0 + a_1 t + \cdots + a_{N-1} t^{N-1} + t^N = \prod_{\mathbf{v} \in \mathrm{Vert}(P)} \left(t - \langle \mathbf{v}, \mathbf{z} \rangle \right). \tag{18}
$$

In summary we have proved the following:

Theorem 2 *Given the moments* (7) *for a direction* $\mathbf{z} \in \mathbb{R}^d$ *in general position, all the projections* $\langle \mathbf{v}, \mathbf{z} \rangle$, $\mathbf{v} \in \mathrm{Vert}(P)$ *are the real roots of the univariate polynomial* $p_{\mathbf{z}}$ *defined in* (18).

Finding the kernel of $\mathbf{H}$ and then computing the coefficients of $p_{\mathbf{z}}(t)$ can be done efficiently in polynomial time. After having computed the projections onto $\mathbf{z}$ of all the vertices, the next step is to find the projections on each of the d coordinates of all N vertices of P. However, there is still an inherent ambiguity in this process because we will not know from which vertex a specific projection came from. We resolve this problem in Sect. 6 and also in alternative way in Sect. 8 by using univariate representations.

Remark 3.1

(a) An analog of the BBaKLP formula for $d = 2$ was known for quite a long time (see e.g. P. Davis [10]), and the system of equations corresponding to (10) was solved

by what is known as Prony's method, see e.g. Elad, Milanfar, and Golub [12, 13]. The solution method described above can also be considered as a variation of Prony's method.

(b) Importantly, the quantities $D_{\mathbf{v}_i}(\mathbf{z})$ play no role for computing the projections $\langle \mathbf{v}_i, \mathbf{z} \rangle$! This is why we will be able to extend the present methodology to general convex polytopes P (i.e., non necessarily simple).

4 Polynomial Density

In this section we address the case of non-uniform measures. That is, our moments are now defined as

$$\mu_j(\mathbf{z}) = \int_P \langle \mathbf{x}, \mathbf{z} \rangle^j \rho(x) \, d\mathbf{x}, \tag{19}$$

where the density function ρ is a homogeneous polynomial of fixed known degree d^o. We note that, intuitively, if ρ is not a homogeneous polynomial the change of a physical scale (e.g. meters to centimeters) will cause complicated changes in the formulas for moments. Therefore, the case of a homogeneous polynomial measure is a very natural one, and we begin with this case in order to develop the proper formulas for it. We then notice, in the next subsection, that the results for the general case of a polytope with any polynomial density follows exactly the same analysis as the case of the homogeneous density.

To set notation, we let P be a convex polytope with a density function $\rho(\mathbf{x})$. We separate ρ into its homogeneous polynomial pieces, by writing $\rho(\mathbf{x}) = \sum_{s=0}^{d^o} \rho_s(\mathbf{x})$, where $\rho_s(\mathbf{x})$ is a homogeneous polynomial of degree s. We will require the physically natural assumption that $\rho(x) > 0$ for each $x \in P$, and in fact we will only need the assumption $\rho(\mathbf{v}) \neq 0$ for $\mathbf{v} \in \text{Vert}(P)$.

We define $\mathbf{V}_k = \mathbf{V}_k(\langle \mathbf{v}_1, \mathbf{z} \rangle, \dots, \langle \mathbf{v}_N, \mathbf{z} \rangle) = \mathbf{V}_k(x_1, \dots, x_N)$, the standard Vandermonde matrix. We further define the lth derivative of the Vandermonde matrix, namely $\mathbf{V}_k^{(l)}$, whose ijth entry is equal to $(i-1) \cdot (i-2) \cdots (i-l) x_j^{i-1-l}$:

$$\mathbf{V}_k^{(l)}(x_1, \dots, x_N) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \\ l! & l! & \dots & l! \\ \vdots & \vdots & \dots & \vdots \\ \frac{k!}{(k-l)!} x_1^{k-l} & \frac{k!}{(k-l)!} x_2^{k-l} & \dots & \frac{k!}{(k-l)!} x_N^{k-l} \end{pmatrix}. \tag{20}$$

As mentioned above, we first assume here that $\rho(\mathbf{x})$ is a homogeneous polynomial of degree d^o. However, in the following subsection we will discuss how the following formulas also work in the more general case of variable but non-homogeneous polynomial density measures. We recall the moment formulas for variable density,

for a simple polytope P, from Theorem 9 in the Appendix:

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d+d^o)!} \sum_{\mathbf{v} \in \text{Vert}(P)} \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \langle \mathbf{v}, \mathbf{z} \rangle^{j+d+d^o} D_{\mathbf{v}}(\mathbf{z}), \qquad (21)$$

where

$$D_{\mathbf{v}}(\mathbf{z}) := \frac{|\det K_{\mathbf{v}}|}{\prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z} \rangle}, \qquad (22)$$

and the identity is valid for each $\mathbf{z} \in \mathbb{C}^d$ such that the denominators in $D_{\mathbf{v}}(\mathbf{z})$ do not vanish. In addition, we also have the following companion identities:

$$0 = \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \sum_{\mathbf{v} \in \text{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^j D_{\mathbf{v}}(\mathbf{z}), \qquad (23)$$

for each $0 \le j \le d + d^o - 1$.

We now repeat the same procedure of putting the new moment formulas above into matrix form, as in (5). Here, the definition of the vector $\mathbf{c}$ is only slightly different, namely:

$$(c_1, \ldots, c_{k+1}) = (-1)^d \left(0, \ldots, 0, \frac{(d+d^o)!}{0!}\mu_0, \frac{(1+d+d^o)!}{1!}\mu_1, \ldots, \right.$$
$$\left. \frac{k! \cdot \mu_{k-d-d^o}}{(k-d-d^o)!}\right). \qquad (24)$$

We arrive at the following interesting matrix ODE for moments with homogeneous polynomial density:

$$\rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \left[\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \langle \mathbf{v}_1, \mathbf{z} \rangle & \langle \mathbf{v}_2, \mathbf{z} \rangle & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle \\ \langle \mathbf{v}_1, \mathbf{z} \rangle^2 & \langle \mathbf{v}_2, \mathbf{z} \rangle^2 & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle^2 \\ \vdots & \vdots & \ldots & \vdots \\ \langle \mathbf{v}_1, \mathbf{z} \rangle^k & \langle \mathbf{v}_2, \mathbf{z} \rangle^k & \ldots & \langle \mathbf{v}_N, \mathbf{z} \rangle^k \end{pmatrix} \begin{pmatrix} D_{\mathbf{v}_1}(\mathbf{z}) \\ \vdots \\ D_{\mathbf{v}_N}(\mathbf{z}) \end{pmatrix} \right]$$
$$= \begin{pmatrix} c_1 \\ \vdots \\ c_{k+1} \end{pmatrix}, \qquad (25)$$

where the differentiation is taken separately for each entry of the vector on the left hand side.

One may check that a single partial derivative of a matrix product obeys the same rule as the derivative of a product of two functions, that is, $\frac{\partial}{\partial x}(M_1(x) \cdot M_2(x)) = \frac{\partial}{\partial x}(M_1(x) \cdot M_2(x)) + M_1(x) \cdot \frac{\partial}{\partial x} M_2(x)$.

We compute a partial derivative $\frac{\partial}{\partial z_i}$ of $\mathbf{V}_k(\langle \mathbf{v}_1, \mathbf{z} \rangle, \ldots, \langle \mathbf{v}_N, \mathbf{z} \rangle)$:

$$
\frac{\partial}{\partial z_i} \mathbf{V}_k = \begin{pmatrix} 0 & \ldots & 0 \\ \mathbf{v}_1^{(i)} & \ldots & \mathbf{v}_N^{(i)} \\ 2\mathbf{v}_1^{(i)} \langle \mathbf{v}_1, \mathbf{z} \rangle & \ldots & 2\mathbf{v}_N^{(i)} \langle \mathbf{v}_N, \mathbf{z} \rangle \\ \vdots & \ldots & \vdots \\ k\mathbf{v}_1^{(i)} \langle \mathbf{v}_1, \mathbf{z} \rangle^{k-1} & \ldots & k\mathbf{v}_N^{(i)} \langle \mathbf{v}_N, \mathbf{z} \rangle^{k-1} \end{pmatrix}
$$

$$
= \mathbf{V}_k^{(1)} \cdot \begin{pmatrix} \mathbf{v}_1^{(i)} & 0 & \ldots & 0 \\ 0 & \mathbf{v}_2^{(i)} & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \mathbf{v}_N^{(i)} \end{pmatrix}.
$$

By repeating the partial derivative in each variable z_i, we arrive at

$$
\rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \mathbf{V}_k = \mathbf{V}_k^{(d^o)} \cdot \begin{pmatrix} \rho(\mathbf{v}_1) & 0 & \ldots & 0 \\ 0 & \rho(\mathbf{v}_2) & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \rho(\mathbf{v}_N) \end{pmatrix}. \tag{26}
$$

Now expanding the matrix ODE formula (25), and using the product rule for differentiation of matrices, we may write it in the following form:

$$
\sum_{i=0}^{d^o} \mathbf{V}_k^{(i)} \cdot \begin{pmatrix} f_1^{(i)}(\mathbf{z}) \\ \vdots \\ f_N^{(i)}(\mathbf{z}) \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_{k+1} \end{pmatrix}, \tag{27}
$$

where each entry $f_j^{(i)}(\mathbf{z})$ is a rational function of $\mathbf{z}$, and the highest vector term, comprised of the rational functions $f_j^{(d^o)}(\mathbf{z})$, has the nice form

$$
\begin{pmatrix} f_1^{(d^o)}(\mathbf{z}) \\ \vdots \\ f_N^{(d^o)}(\mathbf{z}) \end{pmatrix} = \begin{pmatrix} \rho(\mathbf{v}_1) & 0 & \ldots & 0 \\ 0 & \rho(\mathbf{v}_2) & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \rho(\mathbf{v}_N) \end{pmatrix} \cdot \begin{pmatrix} D_{\mathbf{v}_1}(\mathbf{z}) \\ \vdots \\ D_{\mathbf{v}_N}(\mathbf{z}) \end{pmatrix}. \tag{28}
$$

For the proof of the following theorem we construct a certain vector as follows. Define the polynomial

$$
p_{\mathbf{z}}(t) = \prod_{\mathbf{v} \in \mathrm{Vert}(P)} \left(t - \langle \mathbf{v}, \mathbf{z} \rangle\right)^{d^o+1} = t^{N(d^o+1)} + \sum_{i=0}^{(d^o+1)N-1} a_i t^i, \tag{29}
$$

We define the vector $\mathbf{a}_\ell$ to be the coefficient vector of the polynomial $t^\ell p_{\mathbf{z}}(t)$.

Theorem 3 *The Hankel $m \times m$ matrix $\mathbf{H}$, with $m \geq (d^o + 1)N + 1$ corresponding to the moment formulas with variable density, has rank $(d^o + 1)N$, and its kernel is spanned by the linearly independent vectors $\mathbf{a}_\ell$.*

Proof We repeat the procedure that we used in Sect. 3, using a corresponding $m \times m$ Hankel matrix and its kernel, but this time the dimension is $m \geq (d^o + 1)N + 1$. Similarly to the case of uniform density $\rho(x) = 1$, we may again multiply both sizes of (27) on the left by a row vector $\mathbf{a}_0 = (a_0, a_1, \ldots, a_k)$. First, we see that

$$\mathbf{a}_0 \cdot \mathbf{V}_k^{(i)}(x_1, x_2, \ldots, x_N) = \left(p_{\mathbf{z}}^{(i)}(x_1), p_{\mathbf{z}}^{(i)}(x_2), \ldots, p_{\mathbf{z}}^{(i)}(x_N) \right),$$

where $p_{\mathbf{z}}^{(i)}(t)$ is ith derivative of $p_{\mathbf{z}}(t)$.

Now, multiplying (27) by $\mathbf{a}_0$, we obtain the identity $0 = \mathbf{a}_0 \cdot \mathbf{c}$. Similarly, for each $0 \leq \ell \leq k - N(d^o + 1)$, we substitute for $\mathbf{a}_0$ the vector $\mathbf{a}_\ell$ corresponding to $t^\ell p_{\mathbf{z}}(t)$, to obtain $0 = \mathbf{a}_\ell \cdot \mathbf{c}$. Hence the vector $\mathbf{a}_0$ lies in the kernel of $\mathbf{H}$.

On the other hand, we now claim that no other vector $\mathbf{b}$ different from those spanned by $\mathbf{a}_\ell$ could be in Ker($\mathbf{H}$). If, contrary to hypothesis, we could find such a vector $\mathbf{b}$, we may assume without loss of generality that $\mathbf{b} = (b_0, \ldots, b_l, 1, 0, \ldots, 0)$, with $l < (d^o + 1)N - 1$, by reducing it with appropriate linear combinations of $\mathbf{a}_\ell$.

Recall that $\mathbf{c} = (c_1, \ldots, c_{k+1})$, where $k \geq 2m - 2 \geq 2(d^o + 1)N$. Let us consider polynomial $p_{\mathbf{b}}(t)$ with coefficients of $\mathbf{b}$. Now let $\mathbf{b}_\ell$ corresponds to the polynomials $t^\ell p_{\mathbf{b}}(t)$, for $0 \leq \ell \leq m$. Then we have $\mathbf{b}_\ell \cdot \mathbf{c} = 0$, because $\mathbf{b}$ is in the Ker($\mathbf{H}$) and each vector $\mathbf{b}_\ell$ has the same entries as $\mathbf{b}$ only shifted by ℓ to the right.

Since a degree of $p_{\mathbf{b}}(t)$ is smaller than that of $p_{\mathbf{z}}(t)$, we have $p_{\mathbf{z}}(t) \nmid p_{\mathbf{b}}(t)$. Therefore, there exists $\mathbf{v} \in \text{Vert}(P)$ such that $(t - \langle \mathbf{z}, \mathbf{v} \rangle)^{d^o+1} \nmid p_{\mathbf{b}}(t)$. Without loss of generality, we may assume that $\mathbf{v} = \mathbf{v}_1$. We now construct a polynomial $q(t)$ by multiplying $p_{\mathbf{b}}(t)$ by sufficiently many linear factors of the form $(t - \langle \mathbf{z}, \mathbf{v} \rangle)$, where $\mathbf{v}$ varies over all of the vertices of $\text{Vert}(P)$. We will treat the particular vertex $\mathbf{v}_1$ differently, by multiplying by a slightly different power of $(t - \langle \mathbf{z}, \mathbf{v}_1 \rangle)$, to insure that a certain derivative, explicated below, does not vanish at x_1, thus giving us a nonzero vector in the kernel of $\mathbf{H}$. The desired polynomial $q(t)$ satisfies the following properties:

(1) $p_{\mathbf{b}}(t) | q(t)$.
(2) $(t - \langle \mathbf{z}, \mathbf{v}_1 \rangle)^{d^o+1} \nmid q(t)$.
(3) $(t - \langle \mathbf{z}, \mathbf{v}_1 \rangle)^{d^o} | q(t)$.
(4) $(t - \langle \mathbf{z}, \mathbf{v} \rangle)^{d^o+1} | q(t)$, for $\forall \mathbf{v} \in \text{Vert}(P) : \mathbf{v} \neq \mathbf{v}_1$.
(5) $\deg(q) \leq \deg(p) + N(d^o + 1)$.

We now write the coefficients of polynomial $q(t)$ as a vector $\mathbf{b}^o$. Next, we multiply (27) on each side by the row vector $\mathbf{b}^o$.

$$\sum_{i=0}^{d^o} \mathbf{b}^o \cdot \mathbf{V}_k^{(i)} \cdot \begin{pmatrix} f_1^{(i)}(\mathbf{z}) \\ \vdots \\ f_N^{(i)}(\mathbf{z}) \end{pmatrix} = \mathbf{b}^o \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_{k+1} \end{pmatrix}. \tag{30}$$

The vector $\mathbf{b}^o$ may be represented as a linear combination of vectors $\mathbf{b}_\ell$, where $0 \leq \ell \leq m$. Therefore, we get $\mathbf{b}^o \cdot \mathbf{c} = 0$.

On the other hand, since $\prod_{i=1}^{N}(t-x_i)^{d^o}|q(t)$, we have $\mathbf{b}^o \cdot \mathbf{V}_k^{\ell} = 0$ for each $0 \leq \ell < d^o$. Then

$$\mathbf{b}^o \cdot \mathbf{V}_k^{(d^o)} = \big(q^{(d^o)}(x_1), \ldots, q^{(d^o)}(x_N)\big),$$

where $x_j = \langle \mathbf{z}, \mathbf{v}_j \rangle$. We have $q^{(d^o)}(x_1) = \gamma \neq 0$, by property ((2)), and $q^{(d^o)}(x_i) = 0$ for each $2 \leq i \leq N$, because $\prod_{i=2}^{N}(t-x_i)^{d^o+1}|q(t)$. Therefore, we get

$$(\gamma, 0, \ldots, 0) \cdot \begin{pmatrix} \rho(\mathbf{v}_1) & 0 & \ldots & 0 \\ 0 & \rho(\mathbf{v}_2) & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \rho(\mathbf{v}_N) \end{pmatrix} \cdot \begin{pmatrix} D_{\mathbf{v}_1}(\mathbf{z}) \\ \vdots \\ D_{\mathbf{v}_N}(\mathbf{z}) \end{pmatrix} = 0. \qquad (31)$$

Thus $\gamma \cdot \rho(\mathbf{v}_1) \cdot D_{\mathbf{v}_1}(\mathbf{z}) = \mathbf{b}^o \cdot \mathbf{c} = 0$, where none of the quantities γ, $\rho(\mathbf{v}_1)$ and $D_{\mathbf{v}_1}(\mathbf{z})$ is zero, so that we have arrived at a contradiction. $\qquad \square$

Therefore, we have proved the following result, the analog of Theorem 2 for the homogeneous polynomial density case.

Theorem 4 *Given moments* (19) *for a direction* $\mathbf{z} \in \mathbb{R}^d$ *in general position and where* ρ *is a unknown homogeneous polynomial of degree* d^0, *all projections* $\langle \mathbf{v}, \mathbf{z} \rangle$, $\mathbf{v} \in \mathrm{Vert}(P)$, *are the real roots of the univariate polynomial* $p_{\mathbf{z}}$ *defined in* (29).

4.1 Non-homogeneous Measure

We start with the moment formulas for a polytope with variable, but homogeneous density, namely (54). Now we let d^o be the maximal degree of the monomials of $\rho(x)$. Then the formula (21) can be rewritten as follows:

$$\sum_{s=0}^{d^o} \rho_s(\nabla \mathbf{z}) t^{-s} \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \sum_{j=0}^{\infty} \frac{\langle \mathbf{v}, \mathbf{z} \rangle^j}{j!} (-1)^d D_{\mathbf{v}}(\mathbf{z}) t^{j-d} = \sum_{j=0}^{\infty} \frac{\mu_j}{j!} t^j. \qquad (32)$$

Following the same reasoning that was used for the homogeneous variable density case, we first collect all the coefficients of t^{j-d-d^o} on both sides of (32), to get

$$\sum_{s=0}^{d^o} \rho_s(\nabla \mathbf{z}) \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \frac{j(j-1) \cdots (j-d^o+s+1)}{j!} \langle \mathbf{v}, \mathbf{z} \rangle^{j-d^o+s} \cdot D_{\mathbf{v}}(\mathbf{z}) = \frac{c_{j+1}}{j!}, \qquad (33)$$

where $c_{j+1} = (-1)^d \frac{j! \cdot \mu_{j-d-d^o}}{(j-d-d^o)!}$, as in the formula (24). Next, we put everything into a matrix form and get

$$\sum_{s=0}^{d^o} \rho_s(\nabla \mathbf{z}) \cdot \big[\mathbf{V}_k^{(d^o-s)}(x_1, \ldots, x_d) \cdot \mathbf{D}\big] = \begin{pmatrix} c_1 \\ \vdots \\ c_{k+1} \end{pmatrix}. \qquad (34)$$

The latter matrix ODE can be brought into the same form as (27), with exactly the same coefficient of $\mathbf{V}_k^{do}(x_1, \ldots, x_N)$ that appears in (28). Therefore, our method works for general polynomial density measures as well, with precisely the same algorithm.

5 General Convex Polytopes

In the previous discussion we considered only simple polytopes, because the BBaKLP formula takes a particularly nice simple form when P is a simple polytope. However, it is natural to extend our approach to non-simple polytopes. Indeed, it is always possible to triangulate P, that is, decompose P into a union of non overlapping simplices, without adding any extra vertices (see, for example, [7, Theorem 3.1]).

We now fix one such triangulation of P, and denote it by $\mathbf{T}(P)$. We may then rewrite the formula for each moment $\mu_j(\mathbf{z})$ as follows:

$$\mu_j(\mathbf{z}) = \int_P \langle \mathbf{x}, \mathbf{z} \rangle^j \, d\mathbf{x} = \sum_{\Delta \in \mathbf{T}(P)} \int_\Delta \langle \mathbf{x}, \mathbf{z} \rangle^j \, d\mathbf{x}. \tag{35}$$

Triangulating the general convex polytope P into simplices, we reduce the general moment problem to the moment problem for each simplex Δ of the triangulation. Although triangulations may be expensive to construct in practice, we only need to consider a theoretical non-vanishing result, given in Lemma 2 below, for any such triangulation. Given such a triangulation, we may then apply the formulas (1) and (3) to each of the simplices Δ in the equation above:

$$\begin{aligned}
\mathbf{c}_j(\mathbf{z}) &= \sum_{\Delta \in \mathbf{T}(P)} \sum_{\mathbf{v} \in \mathrm{Vert}(\Delta)} \langle \mathbf{v}, \mathbf{z} \rangle^j D_{\mathbf{v}}(\Delta, \mathbf{z}) \\
&= \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^j \sum_{\Delta \in \{\mathbf{T}(P) | \mathbf{v} \in \mathrm{Vert}(\Delta)\}} D_{\mathbf{v}}(\Delta, \mathbf{z}),
\end{aligned}$$

where we have interchanged the order of summation in the last equality above. We now define $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ for this fixed triangulation $\mathbf{T}(P)$ by

$$\tilde{D}_{\mathbf{v}}(\mathbf{z}) := \sum_{\Delta \in \{\mathbf{T}(P) | \mathbf{v} \in \mathrm{Vert}(\Delta)\}} D_{\mathbf{v}}(\Delta, \mathbf{z}). \tag{36}$$

Then we have

$$\mathbf{c}_j(\mathbf{z}) = \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^j \tilde{D}_{\mathbf{v}}(\mathbf{z}). \tag{37}$$

This gives us

$$\frac{(j+d)!(-1)^d}{j!} \mu_j(\mathbf{z}) = \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z} \rangle^{j+d} \tilde{D}_{\mathbf{v}}(\mathbf{z}). \tag{38}$$

Note that in Sect. 3 we never used the explicit formula for $D_{\mathbf{v}}(\mathbf{z})$. The only fact we exploited was that $D_{\mathbf{v}}(\mathbf{z}) \neq 0$ for a general position vector $\mathbf{z}$. Therefore, we can apply the same approach for non-simple polytopes, if we are able to prove that $\tilde{D}_{\mathbf{v}}(\mathbf{z}) \neq 0$ for a general position vector $\mathbf{z}$.

Lemma 2 *For any vertex* $\mathbf{v} \in \mathrm{Vert}(P)$, *any fixed triangulation* $\mathbf{T}(P)$ *and a general position vector* $\mathbf{z}$ *we have* $\tilde{D}_{\mathbf{v}}(\mathbf{z}) \neq 0$.

Proof We begin by noting that $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ is a finite linear combination of rational functions of $\mathbf{z}$. In fact, according to the Lemma 8.3 and Chap. 9 of [3], $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ is a rational function that is the analytic continuation, in $\mathbf{z}$, of the function

$$\hat{1}_{K_{\mathbf{v}} - \mathbf{v}}(\mathbf{z}) = \int_{K_{\mathbf{v}}} e^{\langle \mathbf{z}, x - \mathbf{v} \rangle} \, d\mathbf{x},$$

when this integral converges. We define the dual cone to $K_{\mathbf{v}} - \mathbf{v}$ as follows: $K_{\mathbf{v}}^* := \{\mathbf{y} \in \mathbb{R}^d \mid \langle \mathbf{y}, \mathbf{x} \rangle < 0, \text{ for all } \mathbf{x} \in K_{\mathbf{v}} - \mathbf{v}\}$. Indeed, the latter integral converges for all $\mathbf{z}$ lying in the interior of the dual cone $K_{\mathbf{v}}^*$. Since $K_{\mathbf{v}}$ is a tangent cone of a convex polytope, the dual cone $K_{\mathbf{v}}^*$ is non-empty. Clearly $e^{\langle \mathbf{z}, x \rangle}$ is positive for all $x \in K_{\mathbf{v}} - \mathbf{v}$, if $z \in K_{\mathbf{v}}^*$. We obtain the result that $\hat{1}_{K_{\mathbf{v}} - \mathbf{v}}(\mathbf{z}) > 0$ for all such z, and we may therefore conclude that the analytic continuation of $\hat{1}_{K_{\mathbf{v}} - \mathbf{v}}(\mathbf{z})$ cannot vanish.   □

6 An Exact Algorithm

In Sect. 3 we have learned how to find the projections of vertices of P onto a general position axis $\mathbf{z}$. A short summary of the procedure for such a randomly picked $\mathbf{z} \in \mathbb{R}^d$ is as follows:

Algorithm 1 Computing projections

---
(1) Given $2m - 1 \geq 2N + 1$ moments $c_1, \ldots, c_{2m-1}$ for $\mathbf{z}$, construct a square Hankel matrix $\mathbf{H}(c_1, \ldots, c_{2m-1})$.

(2) Find the vector $v = (a_0, \ldots, a_{M-1}, 1, 0, \ldots, 0)$ in $\mathrm{Ker}(\mathbf{H})$ with the minimal possible M. It turns out that the number of vertices $N = M$.

(3) The set of roots $\{x_i(\mathbf{z}) = \langle \mathbf{v}_i, \mathbf{z} \rangle \mid \mathbf{v}_i \in \mathrm{Vert}(P)\}$ of polynomial $p_{\mathbf{z}}(t) = a_0 + a_1 t + \cdots + a_{N-1} t^{N-1} + t^N$ then equals the set of projections of $\mathrm{Vert}(P)$ onto $\mathbf{z}$.

Remark 6.1 Note that N is an essential part of the input. One cannot rule out existence of another polytope P' with $|\mathrm{Vert}(P')| > N$ and the same moments, up to certain degree.

Remark 6.2 If we work in the context of exact measurements, with rational vertices and rational choices of $\mathbf{z}$ vectors, then $p_{\mathbf{z}}$ has only rational roots. In this rational

context, we may analyze the complexity issues involved by using the LLL-algorithm due to Lenstra, Lenstra, and Lovász [16], because now the rational roots of $p_\mathbf{z}$ can be found in time which is polynomial in N and in the bitsize of Vert(P).

In this section, we describe below an exact algorithm to compute Vert(P) that runs in polynomial time given the latter assumptions. When the roots of $p_\mathbf{z}$ are not available exactly, the algorithm still works, producing approximate results. However, it seems nontrivial to control the precision of root-finding, as we need to find the roots of d univariate polynomials. In Sect. 8 we present a different procedure, where, in contrast, roots of only one polynomial parametrize Vert(P), and which conceivably is more robust against numerical errors.

We use the assumption that $\mathbf{z}$ is in general position (it suffices to require that $\mathbf{z}$ is not perpendicular to the lines uv, for $u, v \in$ Vert(P)) to maintain bijectivity of projection onto $\mathbf{z}$, as well as to avoid division by zero in the terms $D_{v_i}(\mathbf{z})$. Choosing $\mathbf{z}$ at random from the Gaussian distribution on $\mathbb{R}^d$, we get a $\mathbf{z}$ in general position with probability 1. Further, to reconstruct the locations of Vert(P) given the projections of vertices on a number of axes we match all projections of the same vertex as follows.

- Take d linearly independent vectors $\mathbf{z}_1, \ldots, \mathbf{z}_d$, each chosen in general position.
- For every $2 \leq i \leq d$ match projections of Vert(P) onto $\mathbf{z}_i$ with projections onto $\mathbf{z}_1$.

  (1) Pick a general position vector $\mathbf{z} = \alpha \mathbf{z}_1 + \beta \mathbf{z}_i$ in the plane generated by $\mathbf{z}_1$ and $\mathbf{z}_i$.
  (2) Compute the coefficients of the polynomial $p_\mathbf{z}(t)$ using extra $2N + 1$ moments in direction $\mathbf{z}$.
  (3) For each pair of projections $x_j(\mathbf{z}_1)$, $x_k(\mathbf{z}_i)$ onto $\mathbf{z}_1$ and $\mathbf{z}_i$ match them whenever $p_\mathbf{z}(\alpha x_j + \beta x_k) = 0$, for $1 \leq j, k \leq N$.
  (4) With probability 1 all vertices will be matched correctly, that is, $x_k(\mathbf{z}_i)$ is matched with $x_k(\mathbf{z}_1)$.

- For each $1 \leq k \leq N$ reconstruct $v_k \in$ Vert(P) from its projections $x_k(\mathbf{z}_i)$ for $1 \leq i \leq d$.

Indeed, the degree N polynomial

$$p_\mathbf{z}(t) = \prod_k \big(t - \alpha x_k(\mathbf{z}_1) - \beta x_k(\mathbf{z}_i) \big)$$

has N distinct roots. We evaluate it at the N^2 values $\alpha x_j(\mathbf{z}_1) + \beta x_\ell(\mathbf{z}_i)$. With probability 1, by choice of α and β, $p_\mathbf{z}$ will only vanish when $x_j(\mathbf{z}_1)$ and $x_\ell(\mathbf{z}_i)$ correspond to the projections of the same vertex. (In fact, this part is easy to de-randomize: fixing $\alpha = 1$ and choosing more that N^3 different values of β gives one a "good" pair α, β.)

Note that in total we have used $(2d - 1)(2N + 1 - d)$ distinct moments, while the description of vertices of P requires $d \cdot N$ real numbers. That is, our procedure is quite frugal in terms of the moment's measurements.

As claimed in Main Theorem, we can still improve on the latter (albeit the corresponding procedure is not polynomial time any more). Indeed, we only have moments for $d + 1$ directions $\mathbf{z}_1, \ldots, \mathbf{z}_d$, $\mathbf{z} = \sum_j \alpha_j \mathbf{z}_j$ in general position, we can still carry

out a similar procedure, although one would need to compute $\binom{N}{d}$ test values (for all the possible d-fold matchings) of

$$p_{\mathbf{z}_0}(t) = \prod_k \left(t - \sum_{j=1}^d \alpha_j x_k(\mathbf{z}_j) \right).$$

7 An Analysis of Our Algorithm in the Rational Case

In Sect. 6 we described our algorithm under the global assumption that each direction $\mathbf{z}$ is chosen at random from the continuous domain $\mathbb{R}^d$, thus getting a general position vector $\mathbf{z}$ with probability 1. However, in any practical implementation, all the coordinates of $\mathbf{z}$ have to be rational numbers with bounded denominators and numerators. In this case the probability that $\mathbf{z}$ does not lie in general position will be strictly smaller than 1. In what follows we describe a way to pick our $\mathbf{z}$-directions and argue that the probability for choosing a "bad set" of $\mathbf{z}$-directions (which are not in general position) is indeed small.

We will always pick our $\mathbf{z}$ vectors to be rational vectors, with denominator equal to r, and lying in the unit cube $[0, 1]^d$. If we knew the vertex description of a simple polytope P, we would only need to make sure that $\mathbf{z}$ lies in the complement of the finite union of hyperplanes that are orthogonal to all lines between any two vertices of P. We call such a rational $\mathbf{z}$ a *generic* vector. The probability of picking such a generic $\mathbf{z}$ tends to 1 as $r \to \infty$.

We now extend the definition of a generic vector $\mathbf{z}$ to a non-simple polytope P. In this case, in addition to our previous restriction that $\mathbf{z}$ is not orthogonal to any line between vertices of P, in particular to the edges of P, it might occur that $\mathbf{z}$ is a zero of the rational function $\tilde{D}_{\mathbf{v}}(\mathbf{z})$, defined by (36) in Sect. 5, and we need to avoid such a choice of $\mathbf{z}$. Hence we define a generic vector in the general case of non-simple polytopes to be a vector that is simultaneously not orthogonal to any line between vertices of P, and also not a zero of any rational function $\tilde{D}_{\mathbf{v}}(\mathbf{z})$. In particular, we shall avoid zeros and poles of the complex function $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ in $\mathbf{z}$.

In what follows, we refer to the algorithm of Sect. 6. By the Schwartz–Zippel Lemma [11, 18, 20], we have an upper bound for the probability that the numerator and denominator of the multivariable rational function $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ vanishes for a random rational $\mathbf{z} \in [0, 1]^d$, where $\mathbf{z}$ has denominator r. In fact, by our construction, we have r^d such rational vectors $\mathbf{z}$, and the Schwartz–Zippel Lemma tells us the following: for sufficiently large prime r Prob[$\mathbf{z}$ is a zero of $\tilde{D}_{\mathbf{v}}(\mathbf{z})$] $\leq \frac{N}{r}$ and similarly Prob[$\mathbf{z}$ is a pole of $\tilde{D}_{\mathbf{v}}(\mathbf{z})$] $\leq \frac{N}{r}$. Indeed, both the numerator and the denominator of $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ are homogeneous polynomials in d variables $z_1, \ldots, z_d$ of degree at most N with integer coefficients; none of these polynomials vanish when taken over the finite field $\mathbb{F}_r$, for all sufficiently large r.

We remark that our algorithm picks either arbitrary generic vectors (we pick them uniformly at random from the rational unit cube), or takes an integer linear combination of two independent random vectors. In the former case by taking r of order $2^{poly(N,d)}$ one can make the above probabilities for all $\tilde{D}_{\mathbf{v}}(\mathbf{z})$ to be negligibly small.

In the latter case, we need to be more careful, as the sum of two random vectors uniformly distributed over the rational unit cube is no longer a random vector distributed uniformly over the unit cube. However, we may now consider the vector $\alpha \mathbf{z}_1 + \beta \mathbf{z}_i$, as well as the numerator and denominator of $\tilde{D}_{\mathbf{v}}(\mathbf{z})$, over the finite field $\mathbb{F}_r$. We note that, once we fix $0 < \alpha < r$ and $0 < \beta < r$, the linear combination of two independent, uniformly distributed vectors, namely $\alpha \mathbf{z}_1 + \beta \mathbf{z}_i$, is again uniformly distributed over $\mathbb{F}_r^d$.

Therefore, we may assume that each particular direction $\mathbf{z}$ that appeared in the algorithm 1 is generic with a very high probability. On the other hand, a generic vector $\mathbf{z} = \alpha \mathbf{z}_1 + \beta \mathbf{z}_i$ in the plane spanned by $\mathbf{z}_1, \mathbf{z}_i$, matches the set of projections onto $\mathbf{z}_1$ and the set of projections onto $\mathbf{z}_i$ uniquely at very high probability. Indeed, given the projection onto $\mathbf{z}_1$ and $\mathbf{z}_i$ there are N^2 possible projections of Vert(P) onto the plane spanned by $\mathbf{z}_1$ and $\mathbf{z}_i$ and at most N^4 different lines between these points. In other words, there are altogether at most N^4 directions that do not help us match projections onto $\mathbf{z}_1$ and $\mathbf{z}_i$. In the algorithm we pick one of the r distinct directions for $\mathbf{z} = \alpha \mathbf{z}_1 + \beta \mathbf{z}_i$ for any fixed α. Thus the chance that our algorithm did make a mistake in a particular step is negligibly small.

8 Univariate Representations for Vert(P)

In this section, we present an alternative procedure that is conceivably more robust than the algorithm in Sect. 6, where given a finite collection of projections of the vertices, we presented an exact procedure to reconstruct them. That is, we were given some data described in Algorithm 1, assuming that Vert(P) $\subset \mathbb{Q}$ and the measurements are exact. When at least one of the latter assumptions does not hold, the polynomial $p_{\mathbf{z}}$, whose roots are projections of Vert(P), may not have rational roots. Even its coefficients might be known only approximately. Thus it might be hard to control numerical errors.

We construct *univariate representations* (see e.g. [6]) of $\mathbf{v} \in$ Vert(P). The latter are typically used to compute solutions of systems of multivariate polynomial equations—here this appears to be the first use of these representations for purposes other than solving systems of polynomial equations. That is, we will express the coordinates of $\mathbf{v} \in$ Vert(P) as univariate rational functions of ϑ, where ϑ is a root of $p_{\mathbf{a}}(t)$ in (18).

We introduce bivariate polynomials $f_{\mathbf{ab}} \in \mathbb{R}[s, t]$ defined by

$$(s, t) \mapsto f_{\mathbf{ab}}(s, t) = \prod_{\mathbf{v} \in \text{Vert}(P)} \left(t - \langle \mathbf{v}, \mathbf{a} + s\mathbf{b} \rangle \right), \quad \mathbf{a}, \mathbf{b} \in \mathbb{R}^d. \tag{39}$$

Upon transitioning to rational vectors $\mathbf{a}$ and $\mathbf{b}$, generic in the sense of Sect. 7, and with $\mathbf{a} \neq \mathbf{b}$, we can compute the coefficients of $f_{\mathbf{ab}}(s, t)$ by interpolating, with respect to s, the coefficients of the polynomials $f_{\mathbf{ab}}(s, t) = p_{\mathbf{a}+s\mathbf{b}}(t)$, with $s = 0, 1, \ldots, N$, and $p_{\mathbf{a}+s\mathbf{b}}$ in (18) computed using Theorem 1. Define

$$g_{\mathbf{ab}}(t) := \left. \frac{\partial f_{\mathbf{ab}}(s, t)}{\partial s} \right|_{s=0}. \tag{40}$$

Then

$$g_{\mathbf{ab}}(t) = - \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{b} \rangle \prod_{\mathbf{v} \neq \mathbf{u} \in \mathrm{Vert}(P)} \big(t - \langle \mathbf{u}, \mathbf{a} \rangle\big).$$

In particular for $\mathbf{w} \in \mathrm{Vert}(P)$ one obtains

$$g_{\mathbf{ab}}\big(\langle \mathbf{w}, \mathbf{a} \rangle\big) = - \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{b} \rangle \prod_{\mathbf{v} \neq \mathbf{u} \in \mathrm{Vert}(P)} \langle \mathbf{w} - \mathbf{u}, \mathbf{a} \rangle$$

$$= - \langle \mathbf{w}, \mathbf{b} \rangle \prod_{\mathbf{w} \neq \mathbf{u} \in \mathrm{Vert}(P)} \langle \mathbf{w} - \mathbf{u}, \mathbf{a} \rangle.$$

On the other hand, for $p_{\mathbf{a}}$ in (18), its derivative $p'_{\mathbf{a}}$ reads

$$p'_{\mathbf{a}}(t) = \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \prod_{\mathbf{v} \neq \mathbf{u} \in \mathrm{Vert}(P)} \big(t - \langle \mathbf{u}, \mathbf{a} \rangle\big)$$

and thus

$$p'_{\mathbf{a}}\big(\langle \mathbf{w}, \mathbf{a} \rangle\big) = \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \prod_{\mathbf{v} \neq \mathbf{u} \in \mathrm{Vert}(P)} \langle \mathbf{w} - \mathbf{u}, \mathbf{a} \rangle = \prod_{\mathbf{w} \neq \mathbf{u} \in \mathrm{Vert}(P)} \langle \mathbf{w} - \mathbf{u}, \mathbf{a} \rangle.$$

Hence

$$\langle \mathbf{w}, \mathbf{b} \rangle = \frac{g_{\mathbf{ab}}(\langle \mathbf{w}, \mathbf{a} \rangle)}{p'_{\mathbf{a}}(\langle \mathbf{w}, \mathbf{a} \rangle)} = \frac{g_{\mathbf{ab}}(\vartheta)}{p'_{\mathbf{a}}(\vartheta)}, \quad \text{for some } \vartheta \text{ s.t. } p_{\mathbf{a}}(\vartheta) = 0.$$

In particular, assuming that a set of basis vectors $\mathbf{e}_1, \ldots, \mathbf{e}_d$ of $\mathbb{R}^d$ are generic, we obtain

Theorem 5 *The set of vertices of P is given by*

$$\mathrm{Vert}(P) = \left\{ \left(\frac{g_{\mathbf{ae}_1}(\vartheta)}{p'_{\mathbf{a}}(\vartheta)}, \ldots, \frac{g_{\mathbf{ae}_d}(\vartheta)}{p'_{\mathbf{a}}(\vartheta)} \right) \,\Big|\, \text{for each } \vartheta \text{ s.t. } p_{\mathbf{a}}(\vartheta) = 0 \right\}, \quad (41)$$

provided that $\mathbf{a}, \mathbf{e}_1, \ldots, \mathbf{e}_d \in \mathbb{R}^d$ are 'sufficiently general' w.r.t. P—that is, the polynomial $p_{\mathbf{a}}(t)$ from (18) and the polynomials $g_{\mathbf{ae}_j}(t)$ from (40) have no multiple root.

We remark that the assumption of being "sufficiently general" in Theorem 5 is equivalent to the fact that each of the vectors $\mathbf{a}, \mathbf{e}_1, \ldots, \mathbf{e}_d$ does not lie in the discriminant varieties of the polynomial $p_{\mathbf{a}}(t)$ and the set of polynomials $g_{\mathbf{ae}_j}(t)$.

Assuming that computation is done with arbitrary precision, the vertices of P can be obtained by evaluating the vectors of rational functions in ϑ at the roots of $p_{\mathbf{a}}$, as in (41). Therefore, we have transformed the delicate computations of the roots of the polynomials $p_{\mathbf{z}}$ for all projections onto a number of axis vectors $\mathbf{z}$, into just one calculation given by (41).

We note that here we need to use $O(dN^2)$ moments, which is typically much less frugal than the method of Sect. 6, which only uses $O(dN)$ of them.

Remark 8.1 A similar computation of the univariate representation can be carried out even without the genericity assumptions, when the corresponding univariate polynomials have multiple roots. See [14] for details.

9 An Application to Physics

Here we discuss an application of our results to a classical problem of mathematical physics—reconstruction of an object from the potential of a field that it creates. For concreteness, we limit ourselves to the 3-dimensional potential of the gravitational field. The potential function $u(x) := u(x_1, x_2, x_3)$ of the gravitational field $F(x)$ is defined by

$$F(x) = \nabla u(x).$$

In turn, for a body $T \subset \mathbb{R}^3$ with density $\rho(x)$ the potential is given by

$$u(x) = \int_T \frac{\rho(t)}{\|x - t\|} \, dt, \quad \text{for any } x \notin T.$$

A typical physics problem is to reconstruct T and ρ from u, i.e. from the measurements of u. That is, we can assume that $\|x - t\|^{-1} = \sum_a f_a(x) t^a$ is an expansion in a Taylor series w.r.t. $t = (t_1, t_2, t_3)$, and the $f_a(x)$ depend upon x only. Then the expansion

$$u(x) = \sum_a f_a(x) \int_T t^a \rho(t) \, dt, \quad \text{for any } x \notin T$$

encodes information of the moments $\int_T t^a \rho(t) \, dt$ of the measure $\rho(t)$ supported on T. Thus reconstructing T and ρ from u is an inverse moment problem. For instance, when ρ is a polynomial and T is a polytope, the approach described in this paper can be applied to this inverse potential problem and will provide an exact reconstruction.

Appendix: Proof of the BBaKLP Identities for Moments of Polytopes

Here we recall the proof of the moment formulas of BBaKLP, as well as some useful facts that arise in combinatorial geometry, and which we have used in the present paper, but which may not be well-known yet to the mathematical community at large. Although some of the proofs here may not be completely self-contained, they give the reader the proper background for understanding where the moment formulas come from, and the tools that are used for handling them. For more detailed proofs of some of these results, the reader may consult the book [3], as well as the book [7, Corollary 11.9]. We begin with a very useful geometric identity, which has an inclusion-exclusion structure, due to Brianchon and Gram.

We let $1_P(x)$ denote the indicator function of any convex polytope P. For any d-dimensional convex polytope P, we have the following Brianchon–Gram identity:

$$1_P(\mathbf{x}) = \sum_{F \subset P} (-1)^{\dim(F)} 1_{K_F}(\mathbf{x}), \tag{42}$$

valid for all $\mathbf{x} \in \mathbb{R}^d$. Here we are using the tangent cone K_F at each face F of P.

Lemma 3

$$\hat{1}_P(\mathbf{x}) = \sum_{v \in \text{Vert}(P)} \hat{1}_{K_{\mathbf{v}}}(\mathbf{x}).$$

Proof We simply take the Fourier–Laplace transform of both sides of the Brianchon–Gram identity above, and we recall that it is defined by $\hat{f}(\mathbf{z}) := \int_{\mathbb{R}^d} f(\mathbf{x}) e^{\langle \mathbf{x}, \mathbf{z} \rangle} \, d\mathbf{x}$, valid for all $\mathbf{z} \in \mathbb{C}^d$ for which the integral converges. By definition, we have

$$\hat{1}_P(\mathbf{z}) = \int_P e^{\langle \mathbf{x}, \mathbf{z} \rangle} \, d\mathbf{x},$$

the Fourier–Laplace transform of the indicator function of P. It turns out that we may define the Fourier–Laplace transform $\hat{1}_{K_F}(x) = 0$, for any tangent cone K_F which contains a line (isomorphic to $\mathbb{R}^1$). Since all tangent cones K_F contain a line, except for the vertex tangent cones, we are left only with the Fourier–Laplace transforms of the vertex tangent cones. Precisely, we get

$$\hat{1}_P(\mathbf{x}) = \sum_{v \in \text{Vert}(P)} \hat{1}_{K_{\mathbf{v}}}(\mathbf{x}). \qquad \square$$

Using the theory of valuations, one can make the proof of the former Lemma more rigorous (see [3]). However, for the purposes of this appendix, it is not necessary to consider the subtle issues of convergence that arise here.

Lemma 4 *Let $K_{\mathbf{v}}$ be a vertex tangent cone of a simple polytope P. Then*

$$\hat{1}_{K_{\mathbf{v}}}(\mathbf{z}) = (-1)^d \, \frac{e^{\langle \mathbf{v}, \mathbf{z} \rangle} \det K_{\mathbf{v}}}{\prod_{k=1}^d \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z} \rangle},$$

for all $\mathbf{z} \in \mathbb{C}^d$ such that the denominator does not vanish.

Proof The main idea here is to use the fact that there is a linear transformation that maps the simple tangent cone $K_{\mathbf{v}}$ bijectively onto the positive orthant $K_{\text{orth}} := \{(x_1, \ldots, x_d) \in \mathbb{R}^d \mid x_j \geq 0\}$. To be explicit, let $K_{\mathbf{v}} - \mathbf{v} := K_0$ be the translated copy of our tangent cone $K_{\mathbf{v}}$, so that the vertex of K_0 lies at the origin. Let M be the invertible matrix whose columns are the d linearly independent edge vectors $\mathbf{w}_k(\mathbf{v})$ of $K_{\mathbf{v}}$. Then the linear transformation $T : K_{\text{orth}} \to K_{\mathbf{v}} - \mathbf{v}$, defined by $T(x) = Mx$, gives us the desired bijection from the positive orthant onto the translated tangent

cone $K_{\mathbf{v}} - \mathbf{v} := K_0$. Now we use the explicit computation for the Fourier–Laplace transform of the positive orthant K_{orth}, namely:

$$\hat{1}_{K_{\text{orth}}}(\mathbf{z}) = \prod_{j=1}^{d} \hat{1}_{\mathbb{R}_{\geq 0}}(z_j) = (-1)^d \prod_{j=1}^{d} \left(\frac{1}{z_j} \right).$$

Finally, the standard Fourier identity $\widehat{(f \circ T)}(\mathbf{z}) = |\det T| \hat{f}(T^t \mathbf{z})$, valid for any invertible linear transformation T, allows us to finish the computation:

$$
\begin{aligned}
\hat{1}_{K_{\mathbf{v}}}(\mathbf{z}) &= \hat{1}_{K_0 + \mathbf{v}}(\mathbf{z}) \\
&= e^{\langle \mathbf{v}, \mathbf{z} \rangle} \hat{1}_{K_0}(\mathbf{z}) \\
&= e^{\langle \mathbf{v}, \mathbf{z} \rangle} \hat{1}_{M(K_{\text{orth}})}(\mathbf{z}) \\
&= e^{\langle \mathbf{v}, \mathbf{z} \rangle} |\det M| \hat{1}_{K_{\text{orth}}}(M^t \mathbf{z}) \\
&= e^{\langle \mathbf{v}, \mathbf{z} \rangle} (-1)^d \det K_{\mathbf{v}} \prod_{j=1}^{d} \left(\frac{1}{\langle \mathbf{w}_k(\mathbf{v}), \mathbf{z} \rangle} \right). \qquad \square
\end{aligned}
$$

Theorem 6 *Let P be a simple convex polytope. An explicit formula for the Fourier–Laplace transform of P is given by*

$$\int_P e^{\langle \mathbf{x}, \mathbf{z} \rangle} d\mathbf{x} = (-1)^d \sum_{\mathbf{v} \in \text{Vert}(P)} \frac{e^{\langle \mathbf{v}, \mathbf{z} \rangle} \det K_{\mathbf{v}}}{\prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z} \rangle}, \qquad (43)$$

for all $\mathbf{z}$ that are not orthogonal to any edge of P.

Proof From Lemma 3, we know that the Fourier–Laplace transform of P is given by the sum of the Fourier–Laplace transforms of the vertex tangent cones $K_{\mathbf{v}}$, over all vertices $\mathbf{v}$ of P. Using Lemma 4 to rewrite the Fourier–Laplace transform of each vertex tangent cone explicitly, we are done. $\qquad \square$

Theorem 7 *For any convex polytope P and any polynomial $\rho \in \mathbb{R}[\mathbf{x}]$, there exist rational functions $q_{\mathbf{v}}(\mathbf{z})$ such that*

$$\int_P e^{\langle \mathbf{x}, \mathbf{z} \rangle} \rho(\mathbf{x}) d\mathbf{x} = \sum_{\mathbf{v} \in \text{Vert}(P)} e^{\langle \mathbf{v}, \mathbf{z} \rangle} q_{\mathbf{v}}(\mathbf{z}), \qquad (44)$$

for all $\mathbf{z}$ such that the function $e^{\langle \mathbf{v}, \mathbf{z} \rangle} q_{\mathbf{v}}(\mathbf{z})$ is analytic at $\mathbf{z}$.

Proof We may first employ the fact that every convex polytope P has a triangulation into some M simplices Δ_i, with no new vertices. We therefore have $\hat{1}_P(\mathbf{z}) = \sum_{i=1}^{M} \hat{1}_{\Delta_i}(\mathbf{z})$, because the d-dimensional Fourier transform vanishes on all of the lower-dimensional intersections of the various simplices Δ_i. We observe that

$$\int_P e^{\langle \mathbf{x}, \mathbf{z} \rangle} \rho(\mathbf{x}) \, d\mathbf{x} = \rho \left(\frac{\partial}{\partial z_1}, \dots, \frac{\partial}{\partial z_d} \right) \int_P e^{\langle \mathbf{x}, \mathbf{z} \rangle} \, d\mathbf{x}, \qquad (45)$$

because due to the compactness of P, differentiation under the integral sign is valid. Thus

$$\rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \int_P e^{\langle \mathbf{x}, \mathbf{z}\rangle} \, d\mathbf{x} = \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \sum_{i=1}^{M} \hat{1}_{\Delta_i}(\mathbf{z}). \tag{46}$$

Now by Theorem 6, applied to each simple polytope Δ_i, we finally have

$$\int_P e^{\langle \mathbf{x}, \mathbf{z}\rangle} \rho(\mathbf{x}) \, d\mathbf{x} = \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \sum_{i=1}^{M} (-1)^d \sum_{\mathbf{v} \in \mathrm{Vert}(\Delta_i)} \frac{e^{\langle \mathbf{v}, \mathbf{z}\rangle} \det K_{\mathbf{v}}}{\prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z}\rangle}, \tag{47}$$

giving us the desired conclusion upon applying the differential operator to each rational function. □

We recall from the introduction that the basis-free moments for uniform density were defined by

$$\mu_j(\mathbf{z}) := \int_P \langle \mathbf{x}, \mathbf{z}\rangle^j \, dx.$$

The following set of moment formulas can also be found in [8, Sect. 3.2], as well as in [7, Sect. 10.3].

Theorem 8 (Moments formula for uniform density) *Given a simple polytope P, with uniform density $\rho \equiv 1$, we have the moment formulas:*

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d)!} \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z}\rangle^{j+d} D_{\mathbf{v}}(\mathbf{z}), \tag{48}$$

for each integer $j \geq 0$, where

$$D_{\mathbf{v}}(\mathbf{z}) := \frac{|\det K_{\mathbf{v}}|}{\prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z}\rangle}, \tag{49}$$

for each $\mathbf{z} \in \mathbb{C}^d$ such that the denominators in $D_{\mathbf{v}}(\mathbf{z})$ do not vanish. Moreover, we also have the following companion identities:

$$0 = \sum_{v \in \mathrm{Vert}(P)} \langle \mathbf{v}, \mathbf{z}\rangle^j D_{\mathbf{v}}(\mathbf{z}), \tag{50}$$

for each $0 \leq j \leq d-1$.

Proof We begin with the explicit identity for the Fourier–Laplace transform of any convex polytope, namely (43), and we replace $\mathbf{z}$ by $t\mathbf{z}$, where $t > 0$ is now treated as a real variable:

$$\int_P e^{t\langle \mathbf{x}, \mathbf{z}\rangle} \, d\mathbf{x} = (-1)^d \sum_{\mathbf{v} \in \mathrm{Vert}(P)} \frac{e^{t\langle \mathbf{v}, \mathbf{z}\rangle} \det K_{\mathbf{v}}}{t^d \prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z}\rangle}.$$

Now we expand both sides in their Laurent series about $t = 0$, and equate the coefficient of t^j on both sides to obtain the desired moment identities. $\qquad\square$

Theorem 9 (Moments formula for polynomial density and any convex polytope) *Suppose we have a homogeneous polynomial density function $\rho(\mathbf{x})$, of degree d^o, defined over any convex polytope P. For each integer $j \geq 0$, we have the density moments formulas*

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d+d^o)!} \sum_{i=1}^{M} \sum_{\mathbf{v}\in\mathrm{Vert}(\Delta_i)} \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \langle \mathbf{v}, \mathbf{z}\rangle^{j+d+d^o} D_\mathbf{v}(\mathbf{z}), \quad (51)$$

where

$$D_\mathbf{v}(\mathbf{z}) := \frac{|\det K_\mathbf{v}|}{\prod_{k=1}^{d} \langle \mathbf{w}_k(\mathbf{v}), \mathbf{z}\rangle}. \tag{52}$$

These identities are valid for each $\mathbf{z} \in \mathbb{C}^d$ such that the denominators in $D_\mathbf{v}(\mathbf{z})$ do not vanish. In addition, we also have the following companion identities:

$$0 = \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \sum_{i=1}^{M} \sum_{\mathbf{v}\in\mathrm{Vert}(\Delta_i)} \langle \mathbf{v}, \mathbf{z}\rangle^{j} D_\mathbf{v}(\mathbf{z}), \tag{53}$$

for each $0 \leq j \leq d + d^o - 1$.

Proof We begin with (47), and replace $\mathbf{z}$ by $t\mathbf{z}$, for any fixed $t > 0$. Again, expanding both sides in their Laurent expansions about $t = 0$ gives us:

$$\sum_{j=0}^{\infty} \frac{\mu_j}{j!} t^j = \rho\left(\frac{\partial}{t \cdot \partial z_1}, \ldots, \frac{\partial}{t \cdot \partial z_d}\right) \sum_{i=1}^{M} \sum_{\mathbf{v}\in\mathrm{Vert}(\Delta_i)} \sum_{j=0}^{\infty} \frac{\langle \mathbf{v}, \mathbf{z}\rangle^j}{j!} (-1)^d D_\mathbf{v}(\mathbf{z}) t^{j-d}$$

$$= \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \sum_{i=1}^{M} \sum_{\mathbf{v}\in\mathrm{Vert}(\Delta_i)} \sum_{j=0}^{\infty} \frac{\langle \mathbf{v}, \mathbf{z}\rangle^j}{j!} (-1)^d D_\mathbf{v}(\mathbf{z}) t^{j-d-d^o}. \tag{54}$$

We now equate the coefficient of t^j, for each $j \geq 0$, on both sides of the former identity (54), to obtain the desired moment formulas for variable density:

$$\mu_j(\mathbf{z}) = \frac{j!(-1)^d}{(j+d+d^o)!} \sum_{i=1}^{M} \sum_{\mathbf{v}\in\mathrm{Vert}(\Delta_i)} \rho\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_d}\right) \langle \mathbf{v}, \mathbf{z}\rangle^{j+d+d^o} D_\mathbf{v}(\mathbf{z}). \tag{55}$$

Moreover, we also obtain the desired companion identities (53), by equating the first $d + d^o$ coefficients of (54), for each $0 \leq j \leq d + d^o - 1$. $\qquad\square$

References

1. Barvinok, A.I.: Calculation of exponential integrals. Zap. Nauč. Semin. POMI **192**(5), 149–162, 175–176 (1991)

2. Barvinok, A.I.: Exponential integrals and sums over convex polyhedra. Funkc. Anal. Prilozh. **26**(2), 64–66 (1992)
3. Barvinok, A.: Integer Points in Polyhedra. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich (2008)
4. Baldoni, V., Berline, N., De Loera, J.A., Köppe, M., Vergne, M.: How to integrate a polynomial over a simplex. Math. Comput. **80**(273), 297–325 (2011)
5. Boley, D.L., Luk, F.T., Vandevoorde, D.: Vandermonde factorization of a Hankel matrix. In: Scientific Computing, Hong Kong, 1997, pp. 27–39. Springer, Singapore (1997)
6. Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics, vol. 10. Springer, Berlin (2003). Revised version of the first edition online at http://perso.univ-rennes1.fr/marie-francoise.roy/
7. Beck, M., Robins, S.: Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra. Undergraduate Texts in Mathematics. Springer, New York (2007)
8. Brion, M.: Points entiers dans les polyèdres convexes. Ann. Sci. Éc. Norm. Super. **21**(4), 653–663 (1988)
9. Cuyt, A., Golub, G., Milanfar, P., Verdonk, B.: Multidimensional integral inversion, with applications in shape reconstruction. SIAM J. Sci. Comput. **27**(3), 1058–1070 (2005) (electronic)
10. Davis, P.J.: Triangle formulas in the complex plane. Math. Comput. **18**, 569–577 (1964)
11. Demillo, R.A., Lipton, R.T.: A probabilistic remark on algebraic program testing. Inf. Process. Lett. **7**(4), 192–195 (1978)
12. Elad, M., Milanfar, P., Golub, G.H.: Shape from moments—an estimation theory perspective. IEEE Trans. Signal Process. **52**(7), 1814–1829 (2004)
13. Golub, G.H., Milanfar, P., Varah, J.: A stable numerical method for inverting shape from moments. SIAM J. Sci. Comput. **21**(4), 1222–1243 (1999) (electronic)
14. Grigoriev, D., Pasechnik, D.V.: Polynomial-time computing over quadratic maps. I. Sampling in real algebraic sets. Comput. Complex. **14**(1), 20–52 (2005)
15. Lawrence, J.: Polytope volume computation. Math. Comput. **57**(195), 259–271 (1991)
16. Lenstra, A.K., Lenstra, H.W. Jr., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
17. Pukhlikov, A.V., Khovanskiĭ, A.G.: The Riemann–Roch theorem for integrals and sums of quasipolynomials on virtual polytopes. Algebra Anal. **4**(4), 188–216 (1992)
18. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. Assoc. Comput. Mach. **27**(4), 701–717 (1980)
19. Stanley, R.P.: Enumerative Combinatorics. Vol. 1. Cambridge Studies in Advanced Mathematics, vol. 49. Cambridge University Press, Cambridge (1997). With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original
20. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Symbolic and Algebraic Computation, EUROSAM'79, Internat. Sympos., Marseille, 1979. Lecture Notes in Comput. Sci., vol. 72, pp. 216–226. Springer, Berlin (1979)