July 7, 2009

PHASE RETRIEVAL FOR CHARACTERISTIC FUNCTIONS OF CONVEX BODIES AND RECONSTRUCTION FROM COVARIOGRAMS

GABRIELE BIANCHI, RICHARD J. GARDNER, AND MARKUS KIDERLEN

Abstract. We propose strongly consistent algorithms for reconstructing the characteristic function 1_K of an unknown convex body K in $\mathbb{R}^n$ from possibly noisy measurements of the modulus of its Fourier transform $\widehat{1_K}$. This represents a complete theoretical solution to the Phase Retrieval Problem for characteristic functions of convex bodies. The approach is via the closely related problem of reconstructing K from noisy measurements of its covariogram, the function giving the volume of the intersection of K with its translates. In the many known situations in which the covariogram determines a convex body, up to reflection in the origin and when the position of the body is fixed, our algorithms use $O(k^2)$ noisy covariogram measurements to construct a convex polytope P_k that approximates K or its reflection $-K$ in the origin. (By recent uniqueness results, this applies to all planar convex bodies, all three-dimensional convex polytopes, and all symmetric and most (in the sense of Baire category) arbitrary convex bodies in all dimensions.) Two methods are provided, and both are shown to be strongly consistent, in the sense that, almost surely, the minimum of the Hausdorff distance between P_k and $\pm K$ tends to zero as k tends to infinity.

1. Introduction

The *Phase Retrieval Problem* of Fourier analysis involves determining a function f on $\mathbb{R}^n$ from the modulus $|\widehat{f}\,|$ of its Fourier transform $\widehat{f}$. This problem arises naturally and frequently in various areas of science, such as X-ray crystallography, electron microscopy, optics, astronomy, and remote sensing, in which only the magnitude of the Fourier transform can be measured and the phase is lost. (Sometimes, as when reconstructing an object from its far-field diffraction pattern, it is the squared modulus $|\widehat{f}\,|^2$ that is directly measured.) Indeed, as Rosenblatt [40] remarks, the Phase Retrieval Problem "arises in all experimental uses of diffracted electromagnetic radiation for determining the intrinsic detailed structure of a diffracting object." It is no surprise, therefore, that the literature is vast; see the surveys [30], [32], [34], and [40], as well as the articles [10] and [19] and the references given there.

Phase retrieval is fundamentally under-determined without additional constraints, which usually take the form of an a priori assumption that f has a particular support or distribution of values. An important example is when $f = 1_K$, the characteristic function of a convex

---

1991 *Mathematics Subject Classification.* Primary: 42–04, 42B10, 52–04, 52A20; secondary: 52B11.

Key words and phrases. Algorithm, autocorrelation, convex body, convex polytope, covariogram, geometric tomography, image analysis, least squares, phase retrieval, quasicrystal, set covariance.

Supported in part by U.S. National Science Foundation grant DMS-0603307.

body K in $\mathbb{R}^n$. In this setting, phase retrieval is very closely related to a geometric problem involving the *covariogram* of a convex body K in $\mathbb{R}^n$. This is the function g_K defined by

$$g_K(x) = V_n\left(K \cap (K + x)\right),$$

for $x \in \mathbb{R}^n$, where V_n denotes n-dimensional Lebesgue measure and $K + x$ is the translate of K by the vector x. It is also sometimes called the *set covariance* and is equal to the *autocorrelation* of 1_K, that is,

$$g_K = 1_K * 1_{-K},$$

where $*$ denotes convolution and $-K$ is the reflection of K in the origin. Taking Fourier transforms, we obtain the relation

$$\widehat{g_K} = \widehat{1_K}\,\widehat{1_{-K}} = \widehat{1_K}\,\overline{\widehat{1_K}} = \left|\widehat{1_K}\right|^2. \tag{1}$$

This connects the Phase Retrieval Problem, restricted to characteristic functions of convex bodies, to the problem of determining a convex body from its covariogram. Both the definition of covariogram and this connection extend to arbitrary measurable sets, but the reason for restricting to convex bodies will become clear.

The covariogram was introduced by Matheron in his book [36] on random sets. He showed that for a fixed $u \in S^{n-1}$, the directional derivatives $\partial g_K(tu)/\partial t$, for all $t > 0$, of the covariogram of a convex body K in $\mathbb{R}^n$ yield the distribution of the lengths of all chords of K parallel to u. This explains the utility of the covariogram in fields such as stereology, geometric tomography, pattern recognition, image analysis, and mathematical morphology, where information about an unknown object is to be retrieved from chord length measurements; see, for example, [15], [20], and [43]. The covariogram has also played an increasingly important role in analytic convex geometry. For example, it was used by Rogers and Shephard in proving their famous difference body inequality (see [44, Theorem 7.3.1]), by Gardner and Zhang [26] in the theory of radial mean bodies, and by Tsolomitis [45] in his study of convolution bodies, which via the work of Schmuckenschläger [42] and Werner [47] allows a covariogram-based definition of the fundamental notion of affine surface area.

Here we effectively solve the following three problems. In each, K is a convex body in $\mathbb{R}^n$.

Problem 1 (Reconstruction from covariograms). Construct an approximation to K from a finite number of noisy (i.e., taken with error) measurements of g_K.

Problem 2 (Phase retrieval for characteristic functions of convex bodies: squared modulus). Construct an approximation to K (or, equivalently, to 1_K) from a finite number of noisy measurements of $|\widehat{1_K}|^2$.

Problem 3 (Phase retrieval for characteristic functions of convex bodies: modulus). Construct an approximation to K from a finite number of noisy measurements of $|\widehat{1_K}|$.

In order to discuss our results, we must first discuss the corresponding uniqueness problems. In view of (1), these are equivalent, so we shall focus on the covariogram. It is easy to see that g_K is invariant under translations of K and reflection of K in the origin. Let $\mathcal{K}_o^n$ be the class of convex bodies in $\mathbb{R}^n$ and let $\mathcal{U}^n$ be the class of convex bodies in $\mathbb{R}^n$ that are determined, up to translation and reflection in the origin, by their covariograms. Much work has gone into understanding the class $\mathcal{U}^n$. In fact, Matheron [38] himself asked the following question, known as the *Covariogram Problem*, to which he conjectured an affirmative answer when $n = 2$.

Is a convex body in $\mathbb{R}^n$ determined, among all convex bodies and up to translation and reflection in the origin, by its covariogram? In other words, is $\mathcal{U}^n = \mathcal{K}_o^n$?

The focus on covariograms of convex bodies is natural. One reason is that Mallows and Clark [35] constructed non-congruent convex polygons whose overall chord length distributions (allowing the directions of the chords to vary as well) are equal, thereby answering a related question of Blaschke. Thus the information provided by the covariogram cannot be weakened too much. Moreover, there exist non-congruent non-convex polygons, even (see [22, p. 394]) horizontally- and vertically-convex polyominoes, with the same covariogram, indicating that the convexity assumption also cannot be significantly weakened.

Let $\mathcal{P}^n$ be the class of n-dimensional convex polytopes in $\mathbb{R}^n$ and let $\mathcal{K}_s^n$ be the class of centrally symmetric convex bodies in $\mathbb{R}^n$. A short history of the Covariogram Problem begins with Nagel [39] (see also [7]), who proved that $\mathcal{P}^2 \subset \mathcal{U}^2$. (Even this is by no means easy.) Bianchi, Segala, and Volčič [10] showed that planar C^2 convex bodies of positive Gauss curvature belong to $\mathcal{U}^2$. Their approach utilizes the asymptotic behavior of Fourier transforms of characteristic functions of convex bodies, the subject of many studies since the original work of Haviland and Wintner [28]. Averkov and Bianchi [4] finally proved that $\mathcal{U}^2 = \mathcal{K}_o^2$, confirming Matheron's conjecture. Recently Bianchi [9] showed that $\mathcal{P}^3 \subset \mathcal{U}^3$, by a long and intricate argument. On the other hand, it is easy to see that $\mathcal{K}_s^n \subset \mathcal{U}^n$. (In the symmetric case, convexity is not essential; see [22, Proposition 4.4] for this result, due to Cabo and Jensen.) Goodey, Schneider, and Weil [27] proved that most (in the sense of Baire category) convex bodies in $\mathbb{R}^n$ belong to $\mathcal{U}^n$. Nevertheless, the Covariogram Problem in general has a negative answer, as Bianchi [8] demonstrated by constructing examples showing that $\mathcal{P}^n \not\subset \mathcal{U}^n$ for $n \geq 4$. It is still unknown whether $\mathcal{U}^3 = \mathcal{K}_o^3$.

Interest in the Covariogram Problem extends far beyond geometry. For example, Adler and Pyke [1] ask whether the distribution of the difference $X - Y$ of independent random variables X and Y, uniformly distributed over a convex body K, determines K up to translations and reflection in the origin. Up to a constant, the convolution $1_K * 1_{-K} = g_K$ is just the probability density of $X - Y$, so the question is equivalent to the Covariogram Problem. In [2], the Covariogram Problem also appears in deciding the equivalence of measures induced by Brownian processes for different base sets.

None of the above uniqueness proofs provide a method for actually reconstructing a convex body from its covariogram. We are aware of only two papers dealing with the reconstruction problem: Schmitt [41] gives an explicit reconstruction procedure for a convex polygon when no pair of its edges are parallel, an assumption removed in an algorithm due to Benassi and D'Ercole [6]. In both these papers, all the exact values of the covariogram are supposed to be available.

In contrast, our first set of algorithms take as input only a finite number of values of the covariogram of an unknown convex body K_0. Moreover, these measurements are corrupted by errors, modeled by Gaussian noise of mean zero and a fixed variance. It is assumed that K_0 is determined by its covariogram, has its centroid at the origin, and is contained in a known bounded region of $\mathbb{R}^n$, which for convenience we take to be the unit cube $C_0^n = [-1/2, 1/2]^n$. We provide two different methods for reconstructing, for each suitable $k \in \mathbb{N}$, a convex polytope P_k that approximates K_0 or its reflection $-K_0$. Each method involves two algorithms, an initial algorithm that produces suitable outer unit normals to the facets of P_k, and a common main algorithm that goes on to actually construct P_k.

In the first method, the covariogram of K_0 is measured, multiple times, at the origin and at vectors $(1/k)u_i$, $i = 1, \dots, k$, where the u_i's are mutually nonparallel unit vectors that span $\mathbb{R}^n$. From these measurements, the initial Algorithm NoisyCovBlaschke constructs an o-symmetric convex polytope Q_k that approximates ∇K_0, the so-called Blaschke body of K_0. (See Section 2 for definitions and notation.) The crucial property of ∇K_0 is that when K_0 is a convex polytope, each of its facets is parallel to some facet of ∇K_0. It follows that the outer unit normals to the facets of P_k can be taken to be among those of Q_k. Algorithm NoisyCovBlaschke utilizes the known fact that $-\partial g_{K_0}(tu)/\partial t$, evaluated at $t = 0$, equals the brightness function value $b_{K_0}(u)$, that is, the $(n-1)$-dimensional volume of the orthogonal projection of K_0 in the direction u. This connection allows most of the work to be done by a very efficient algorithm designed earlier by Gardner and Milanfar (see [24]) that reconstructs a o-symmetric convex body from finitely many noisy measurements of its brightness function.

The second method achieves the same goal with a quite different approach. This time the covariogram of K_0 is measured once at each point in a cubic array in $2C_0^n = [-1, 1]^n$ of side length $1/k$. From these measurements, the initial Algorithm NoisyCovDiff(φ) constructs an o-symmetric convex polytope Q_k that approximates $DK_0 = K_0 + (-K_0)$, the difference body of K_0. The set DK_0 has precisely the same property as ∇K_0, that when K_0 is a convex polytope, each of its facets is parallel to some facet of ∇K_0. Furthermore, DK_0 is just the support of g_{K_0}. The known property that $g_{K_0}^{1/n}$ is concave (a consequence of the Brunn-Minkowski inequality [21, Section 11]) can therefore be combined with techniques from multiple regression. Algorithm NoisyCovDiff(φ) employs a Gasser-Müller type kernel estimator for g_{K_0}, with suitable kernel function φ, bandwidth, and threshold parameter.

The output Q_k of either initial algorithm forms part of the input to the main common Algorithm NoisyCovLSQ. The covariogram of K_0 is now measured again, once at each point in a cubic array in $2C_0^n = [-1, 1]^n$ of side length $1/k$. Using these measurements, Algorithm NoisyCovLSQ finds a convex polytope P_k, each of whose facets is parallel to some facet of Q_k, whose covariogram fits best the measurements in the least squares sense.

Much effort is spent in proving that these algorithms are strongly consistent. Whenever $K_0 \in \mathcal{U}^n$, we show that, almost surely,

$$\min\{\delta(K_0, P_k), \delta(-K_0, P_k)\} \to 0$$

as $k \to \infty$, where δ denotes Hausdorff distance. (If $K_0 \notin \mathcal{U}^n$, a rare situation in view of the uniqueness results discussed above, the algorithms still construct a sequence (P_k) whose accumulation points exist and have the same covariogram as K_0.) From a theoretical point of view, this completely solves Problem 1. Naturally, the consistency proof leans heavily on results and techniques from analytic convex geometry, including the Bourgain-Campi-Lindenstrauss stability result for projection bodies, as well as a suitable version of the Strong Law of Large Numbers.

With algorithms for Problem 1 in hand, we move to Problem 2, assuming that K_0 is an unknown convex body satisfying the same conditions as before. The basic idea is simple enough: Use (1) and the measurements of $|\widehat{1_{K_0}}|^2$ at points in a suitable cubic array to approximate g_{K_0} via its Fourier series, and feed the resulting values into the algorithms for Problem 1. However, two major technical obstacles arise. The new estimates of g_{K_0} are corrupted by noise that now involves dependent random variables, and a new deterministic error appears as well. A substitute for the Strong Law of Large Numbers must be proved, and the deterministic error controlled using Fourier analysis and the fortunate fact that g_{K_0} is Lipschitz. In the end the basic idea works, assuming that for suitable $1/2 < \gamma < 1$, measurements of $|\widehat{1_{K_0}}|^2$ are taken at the points in $(1/k^{\gamma})\mathbb{Z}^n$ contained in the cubic window $[-k^{1-\gamma}, k^{1-\gamma}]^n$, whose size increases with k at a rate depending on the parameter γ. The three resulting algorithms, Algorithm NoisyMod^{2}LSQ, Algorithm NoisyMod^{2}Blaschke, and Algorithm NoisyMod^{2}Diff(φ), are stated in detail and, with suitable restrictions on γ, proved to be strongly consistent under the same hypotheses as for Problem 1.

Our final three algorithms, Algorithm NoisyModLSQ, Algorithm NoisyModBlaschke, and Algorithm NoisyModDiff(φ) cater for Problem 3. Again there is a basic simple idea, namely, to take two independent measurements at each of the points in the same cubic array as in the previous paragraph, multiply the two, and feed the resulting values into the algorithms for Problem 2. No serious extra technical difficulties arise, and we are able to prove that the three new algorithms are strongly consistent under the same hypotheses as for Problem 2. This provides a complete theoretical solution to the Phase Retrieval Problem for characteristic functions of convex bodies.

To summarize:

For Problem 1, use *either* Algorithm NoisyCovBlaschke *or* Algorithm NoisyCovDiff(φ) and then Algorithm NoisyCovLSQ.

For Problem 2, use *either* Algorithm NoisyMod^{2}Blaschke *or* Algorithm NoisyMod^{2}Diff(φ) and then Algorithm NoisyMod^{2}LSQ.

For Problem 3, use *either* Algorithm NoisyModBlaschke *or* Algorithm NoisyModDiff(φ) and then Algorithm NoisyModLSQ.

In some of the algorithms, the cubic array of measurement points is a matter of convenience; it should be possible to use a wide variety of different sets of measurement points, with appropriate adjustments in the consistency proofs.

We remark that Corollary 5.7 provides a rate of convergence for Algorithm NoisyCovDiff(φ) and hence for the two related algorithms for phase retrieval, but we do not establish rates of convergence for the other algorithms. It should be possible to apply the theory of empirical processes to this end, as was done in [24] for the brightness function algorithm, but at present there is an obstacle: No stability versions of the uniqueness results for the Covariogram

Problem are available. In view of the difficulty of these uniqueness results, proving such stability versions will presumably be very challenging.

The present paper deals solely with theory. However, working algorithms are anticipated and implementation is already underway with some promising initial results. This and the effect of the regularization technique, which preliminary investigations indicate allow the restriction on the parameter γ to be considerably relaxed, will be the subject of a future study. We believe our algorithms will find applications. For example, Baake and Grimm [5] explain how the problem of finding the atomic structure of a quasicrystal from its X-ray diffraction image involves recovering a subset of $\mathbb{R}^n$ called a window from its covariogram, and note that this window is in many cases a convex body.

The paper is organized as follows. Section 2 deals with definitions and notation, after which Section 3 presents the main Algorithm NoisyCovLSQ for Problem 1 and its strong consistency, established in Theorem 3.10. In Section 4, Algorithm NoisyCovBlaschke is stated with proof of strong consistency in Theorem 4.5; the latter requires the assumption that the vectors u_i, $i = 1, \dots, k$, are part of an infinite sequence (u_i) that is in a sense evenly spread out in S^{n-1}, but this restriction is a weak one. In Section 5, Algorithm NoisyCovDiff(φ) is set out and proved to be strongly consistent in Theorem 5.6. Treatment of phase retrieval begins in Section 6. Problem 2 is the focus of Section 7, where we present Algorithm NoisyMod^{2}LSQ, Algorithm NoisyMod^{2}Blaschke, and Algorithm NoisyMod^{2}Diff(φ), and prove strong consistency theorems for them. The final Section 8 serves the same purpose for Algorithm NoisyModLSQ, Algorithm NoisyModBlaschke, and Algorithm NoisyModDiff(φ), which cater for Problem 3.

2. Definitions and notation

As usual, S^{n-1} denotes the unit sphere, B^n the unit ball, o the origin, and $|\cdot|$ the norm in Euclidean n-space $\mathbb{R}^n$. We shall also write $C_0^n = [-1/2, 1/2]^n$ throughout. The standard orthonormal basis for $\mathbb{R}^n$ will be denoted by $\{e_1, \dots, e_n\}$. A *direction* is a unit vector, that is, an element of S^{n-1}. If u is a direction, then $u^\perp$ is the $(n-1)$-dimensional subspace orthogonal to u and l_u is the line through the origin parallel to u. If $x, y \in \mathbb{R}^n$, then $x \cdot y$ is the inner product of x and y, and $[x, y]$ is the line segment with endpoints x and y.

We denote by ∂A, $\operatorname{int} A$ and $\operatorname{diam} A$ the *boundary*, *interior*, and *diameter* of a set A, respectively. The notation for the usual (orthogonal) *projection* of A on a subspace S is $A|S$. A set is *o-symmetric* if it is centrally symmetric, with center at the origin.

If X is a metric space and $\varepsilon > 0$, a finite set $\{x_1, \dots, x_m\}$ is called an *ε-net* in X if for every point x in X, there is an $i \in \{1, \dots, m\}$ such that x is within a distance ε of x_i.

We write V_k for k-dimensional Lebesgue measure in $\mathbb{R}^n$, where $k = 1, \dots, n$, and where we identify V_k with k-dimensional Hausdorff measure. If K is a k-dimensional convex subset of $\mathbb{R}^n$, then $V(K)$ is its *volume* $V_k(K)$. Define $\kappa_n = V(B^n)$. The notation dz will always mean $dV_k(z)$ for the appropriate $k = 1, \dots, n$.

If E and F are sets in $\mathbb{R}^n$, then

$$E + F = \{x + y : x \in E, y \in F\}$$

denotes their *Minkowski sum* and

$$E \ominus F = \{x \in \mathbb{R}^n : F + x \subset E\} \tag{2}$$

their *Minkowski difference*.

Let $\mathcal{K}^n$ be the class of compact convex sets in $\mathbb{R}^n$. A *convex body* in $\mathbb{R}^n$ is a compact convex set with nonempty interior. Let $\mathcal{K}^n_o$ be the class of convex bodies in $\mathbb{R}^n$ and let $\mathcal{K}^n(A)$ (or $\mathcal{K}^n_o(A)$) be the class of compact convex sets (or convex bodies, respectively) contained in the subset A of $\mathbb{R}^n$. The notation $\mathcal{K}^n(r,R)$ will be used for the class of convex bodies containing rB^n and contained in RB^n, where $0 < r < R$. The treatise of Schneider [44] is an excellent general reference for convex geometry.

If $K \in \mathcal{K}^n$, then

$$K^* = \{x \in \mathbb{R}^n : x \cdot y \le 1 \text{ for all } y \in K\}$$

is the *polar set* of K. The function

$$h_K(x) = \max\{x \cdot y : y \in K\},$$

for $x \in \mathbb{R}^n$, is the *support function* of K and

$$b_K(u) = V(K|u^\perp),$$

for $u \in S^{n-1}$, its *brightness function*. Any $K \in \mathcal{K}^n$ is uniquely determined by its support function. We can regard h_K as a function on S^{n-1}, since $h_K(x) = |x| h_K(x/|x|)$ for $x \ne o$. The *Hausdorff distance* $\delta(K,L)$ between two sets $K, L \in \mathcal{K}^n$ can then be conveniently defined by

$$\delta(K,L) = \|h_K - h_L\|_\infty,$$

where $\|\cdot\|_\infty$ denotes the supremum norm on S^{n-1}.

The *surface area measure* $S(K,\cdot)$ of a convex body K is defined for Borel subsets E of S^{n-1} by

$$S(K,E) = V_{n-1}\left(g^{-1}(K,E)\right), \tag{3}$$

where $g^{-1}(K,E)$ is the set of points in ∂K at which there is an outer unit normal vector in E. Every surface area measure is *balanced*, that is,

$$\int_{S^{n-1}} u \, dS(K,u) = o. \tag{4}$$

Let $S(K) = S(K, S^{n-1})$. Then $S(K)$ is the *surface area* of K. The *Blaschke body* ∇K of a convex body K is the unique o-symmetric convex body satisfying

$$S(\nabla K,\cdot) = \frac{1}{2} S(K,\cdot) + \frac{1}{2} S(-K,\cdot). \tag{5}$$

The *projection body* of $K \in \mathcal{K}^n$ is the o-symmetric set $\Pi K \in \mathcal{K}^n$ defined by

$$h_{\Pi K} = b_K. \tag{6}$$

Cauchy's projection formula states that for any $u \in S^{n-1}$,

$$h_{\Pi K}(u) = b_K(u) = \frac{1}{2} \int_{S^{n-1}} |u \cdot v| \, dS(K,v), \tag{7}$$

and Cauchy's surface area formula is

$$S(K)=\frac{1}{\kappa_{n-1}}\int_{S^{n-1}}b_K(u)du; \tag{8}$$

see [20, (A.45) and (A.49), p. 408]. By (5) and (7), we have

$$b_{\nabla K}=b_K, \tag{9}$$

and it can be shown (see [20, p. 116]) that ∇K is the unique o-symmetric convex body with this property.

Let K be a convex body in $\mathbb{R}^n$ and let $u\in S^{n-1}$. The *(parallel) X-ray of* K in the direction u is the function X_uK defined by

$$X_uK(x)=\int_{l_u+x}1_K(y)dy,$$

for $x\in u^\perp$, where 1_K denotes the *characteristic function* of K. The *difference body* of K is the o-symmetric convex body $DK=K+(-K)$. Now define

$$E_K(t,u)=\{y\in u^\perp : X_uK(y)\ge t\} \tag{10}$$

and

$$a_K(t,u)=V\big(E_K(t,u)\big), \tag{11}$$

for $t\ge 0$ and $u\in S^{n-1}$. Note that if $u\in S^{n-1}$, then $E_K(0,u)=K|u^\perp$ and $a_K(0,u)=b_K(u)$.

The function

$$g_K(x)=V(K\cap(K+x)),$$

for $x\in\mathbb{R}^n$, is called the *covariogram* of K. Note that $g_K(o)=V(K)$, and that we have $g_K(x)=0$ if and only if $x\notin \operatorname{int} DK$, so the support of g_K is DK. Also, $g_K^{1/n}$ is concave on its support; see, for example, [26, Lemma 3.2].

Let $x=tu$, where $t\ge 0$ and $u\in S^{n-1}$, and define $g_K(t,u)=g_K(tu)$. The simple relationship

$$g_K(t,u)=\int_t^\infty a_K(s,u)\,ds \tag{12}$$

was noticed by Matheron [36, p. 86] in the form

$$\frac{\partial g_K(t,u)}{\partial t}=-a_K(t,u). \tag{13}$$

Let μ and ν be finite nonnegative Borel measures in S^{n-1}. Define

$$d_P(\mu,\nu)=\inf\{\varepsilon>0:\mu(E)\le\nu(E_\varepsilon)+\varepsilon,\ \nu(E)\le\mu(E_\varepsilon)+\varepsilon,\ E\text{ Borel in }S^{n-1}\}, \tag{14}$$

where

$$E_\varepsilon=\{u\in S^{n-1}:\exists v\in E:|u-v|<\varepsilon\}.$$

Then d_P is a metric called the *Prohorov metric*. As S^{n-1} is a Polish space, it is enough to take the infimum in (14) over the class of *closed* sets. In addition, if $\mu(S^{n-1})=\nu(S^{n-1})$, then

$$d_P(\mu,\nu)=\inf\{\varepsilon>0:\mu(E)\le\nu(E_\varepsilon)+\varepsilon,\ E\text{ Borel in }S^{n-1}\}; \tag{15}$$

see [17]. Now define

$$d_D(\mu,\nu)=\sup\left\{\left|\int_{S^{n-1}} f\,d(\mu-\nu)\right| : \|f\|_{BL}\le 1\right\}, \tag{16}$$

where for any real-valued function f on S^{n-1} we define

$$\|f\|_L=\sup_{u\neq v}\frac{|f(u)-f(v)|}{|u-v|} \quad\text{and}\quad \|f\|_{BL}=\|f\|_\infty+\|f\|_L.$$

It can be shown that d_D is a metric, sometimes called the *Dudley metric*. By [17, Corollary 2], we have the relation

$$d_D(\mu,\nu)\le 2d_P(\mu,\nu), \tag{17}$$

for finite nonnegative Borel measures μ and ν in S^{n-1}.

We need a condition on a sequence (u_i) in S^{n-1} stronger than denseness in S^{n-1}. To this end, for $u\in S^{n-1}$ and $0<t\le 2$, let

$$C_t(u)=\{v\in S^{n-1} : |u-v|<t\}$$

be the open spherical cap with center u and radius t. We call (u_i) *evenly spread* if for all $0<t<2$, there is a constant $c=c(t)>0$ and an $N=N(t)$ such that

$$|\{u_1,\dots,u_k\}\cap C_t(u)|\ge ck, \tag{18}$$

for all $u\in S^{n-1}$ and $k\ge N$. Often, we will apply this notion to the symmetrization

$$(u_i^*)=(u_1,-u_1,u_2,-u_2,u_3,-u_3,\dots)$$

of a sequence (u_i).

We adopt a standard definition of the Fourier transform $\widehat{f}$ of a function f on $\mathbb{R}^n$, namely

$$\widehat{f}(x)=\int_{\mathbb{R}^n} f(y)e^{-ix\cdot y}\,dy.$$

If f and g are real-valued functions on $\mathbb{N}$, then, as usual, $f=O(g)$ means that there is a constant c such that $f(k)\le cg(k)$ for sufficiently large k. The notation $f\sim g$ will mean that $f=O(g)$ and $g=O(f)$.

3. The main algorithm for reconstruction from covariograms

We shall assume throughout that the unknown convex body K_0 is contained in the cube $C_0=[-1/2,1/2]^n$, with its centroid at the origin. This assumption can be justified on both purely theoretical and purely practical grounds. If the measurements are exact, then from the covariogram, a convex polytope can be constructed that contains a translate of K_0. On the other hand, in practise, an unknown object whose covariogram is to be measured is contained in some known bounded region. In either case, one may as well suppose that K_0 is contained in C_0^n, and since in the situations we consider, the covariogram determines K_0 up to translation and reflection in the origin, we can also fix the centroid at the origin.

Algorithm NoisyCovLSQ

Input: Natural numbers $n \geq 2$ and k; noisy covariogram measurements

$$M_{ik} = g_{K_0}(x_{ik}) + N_{ik}, \tag{19}$$

of an unknown convex body $K_0 \subset C_0^n$ whose centroid is at the origin, at the points x_{ik}, $i = 1, \dots, I_k = (2k+1)^n$ in the cubic array $2C_0^n \cap (1/k)\mathbb{Z}^n$, where the N_{ik}'s are independent normal $N(0, \sigma^2)$ random variables; an o-symmetric convex polytope Q_k in $\mathbb{R}^n$, stochastically independent of the measurements M_{ik}, that approximates either ∇K_0 or DK, in the sense that, almost surely,

$$\lim_{k\to\infty} \delta(Q_k, \nabla K_0) = 0, \qquad \text{or} \qquad \lim_{k\to\infty} \delta(Q_k, DK_0) = 0. \tag{20}$$

Task: Construct a convex polytope P_k that approximates K_0, up to reflection in the origin.

Action:

1. Compute the outer normals $\{\pm u_j : j = 1, \dots, s\}$ of Q_k.

2. For any vector $a = (a_1^+, a_1^-, a_2^+, a_2^-, \dots, a_s^+, a_s^-)$, where $a_j^+, a_j^- \geq 0$, $j = 1, \dots, s$, such that $\sum_{j=1}^s (a_j^+ - a_j^-)u_j = o$, let $P(a) = P(a_1^+, a_1^-, a_2^+, a_2^-, \dots, a_s^+, a_s^-)$ be the convex polytope with centroid at the origin, outer facet normals in $\{\pm u_j : j = 1, \dots, s\}$ and such that the face with normal u_j (or $-u_j$) has $(n-1)$-dimensional measure a_j^+ (or a_j^-, respectively), $j = 1, \dots, s$.

Solve the following least squares problem:

$$\min \sum_{i=1}^{I_k} \left(M_{ik} - g_{P(a)\cap C_0^n}(x_{ik})\right)^2 \tag{21}$$

over the variables $a_1^+, a_1^-, a_2^+, a_2^-, \dots, a_s^+, a_s^-$, subject to the constraints

$$\sum_{j=1}^s (a_j^+ - a_j^-)u_j = o$$

and

$$a_j^+, a_j^- \geq 0, \ j = 1, \dots, s.$$

These constraints guarantee that the output will correspond to a convex polytope.

3. Let a set of optimal values be $\hat{a}_1^+, \hat{a}_1^-, \hat{a}_2^+, \hat{a}_2^-, \dots, \hat{a}_s^+, \hat{a}_s^-$, and call the corresponding polytope $P(\hat{a})$. Then the output polytope P_k is the translate of $P(\hat{a}) \cap C_0^n$ that has its centroid at the origin. Note that in this case $-P_k$ also corresponds to a set of optimal values obtained by switching a_j^+ and a_j^-, $j = 1, \dots, s$.

Lemma 3.1. *Let $0 < r < R$ and let $Q \in \mathcal{K}^n(r, R)$ be an o-symmetric convex polytope. Then there are facets of Q with outer unit normal vectors $u_1, \dots, u_n$ such that*

$$|\det(u_1, \dots, u_n)| > (r/R)^{n(n-1)/2}. \tag{22}$$

Proof. The polar body Q^* of Q is contained in $\mathcal{K}^n(1/R,1/r)$ and has its vertices in the directions of the outer normals to the facets of Q, so it suffices to prove that there are vertices $v_1,\dots,v_n$ of Q^* such that with $u_i=v_i/|v_i|$, (22) holds.

The proof will be by induction on n. Let $n=2$. We may assume that Q^* has a vertex, v_1 say, on the positive x_2-axis. Since $Q^*\in\mathcal{K}^2(1/R,1/r)$, there must be another vertex v_2 of Q^* with distance at least $1/R$ from the x_2-axis, and by the symmetry of Q^*, such that also $v_2\cdot e_2\ge 0$. If α is the angle between v_1 and v_2, we must then have $\theta\le\alpha\le\pi/2$, where θ is the angle between the vectors $(0,1/r)$ and $\left(1/R,\sqrt{(1/r^2)-(1/R^2)}\right)$. Then, if $u_i=v_i/|v_i|$ for $i=1,2$, we have

$$|\det(u_1,u_2)|=\sin\alpha\ge\sin\theta=r/R,$$

which proves (22) for $n=2$.

Suppose that (22) holds with n replaced by $n-1$ and let $Q^*\in\mathcal{K}^n(1/R,1/r)$. We may assume that Q^* has a vertex, v_1 say, on the positive x_n-axis, so that $v_1/|v_1|=e_n$. Since $Q^*|e_n^\perp\in\mathcal{K}^{n-1}(1/R,1/r)$ (where we are identifying $e_n^\perp$ with $\mathbb{R}^{n-1}$), by the inductive hypothesis, there are vertices $w_2,\dots,w_n$ of $Q^*|e_n^\perp$ such that if $z_i=w_i/|w_i|$, $i=2,\dots,n$, then

$$|\det(z_2,\dots,z_n)|\ge(r/R)^{(n-1)(n-2)/2}. \tag{23}$$

Let v_i be a vertex of Q^* such that $v_i|e_n^\perp=w_i$, $i=2,\dots,n$, and let $u_i=v_i/|v_i|$, $i=1,\dots,n$. By the symmetry of Q^*, we may also assume that $v_i\cdot e_n\ge 0$ for $i=2,\dots,n$. Let α_i be the angle between v_i and w_i, for $i=2,\dots,n$. Using the fact that $Q^*|e_n^\perp\in\mathcal{K}^{n-1}(1/R,1/r)$, we see that each v_i, $i=2,\dots,n$ has distance at least $1/R$ from the x_n-axis. Therefore $\cos\alpha_i\ge\sin\theta=r/R$ for $i=2,\dots,n$. Then, using (23) and noting that $u_1=e_n$ and $u_i=u_i|e_n^\perp+(u_i\cdot e_n)e_n$ for $i=2,\dots,n$, we obtain

$$\begin{aligned}|\det(u_1,\dots,u_n)| &= |\det(u_2|e_n^\perp,\dots,u_n|e_n^\perp)|\\ &= |\det(z_2,\dots,z_n)|\prod_{i=2}^n\cos\alpha_i\\ &\ge (r/R)^{(n-1)(n-2)/2}(r/R)^{n-1}=(r/R)^{n(n-1)/2}.\end{aligned}$$

□

Lemma 3.2. *Let $K\in\mathcal{K}^n(r,R)$, let $0<\varepsilon<\kappa_{n-1}r^{n-1}/2$, and let L be a convex body containing the origin in $\mathbb{R}^n$ such that*

$$d_P(S(K,\cdot),S(L,\cdot))<\varepsilon. \tag{24}$$

Then there is a constant a_1 depending only on ε, r, and R such that $L\subset a_1B^n$. If L is o-symmetric, there is also a constant $a_0>0$ depending only on ε, r, and R such that $a_0B^n\subset L$.

Proof. Note that for any $u\in S^{n-1}$, the function $f(v)=|u\cdot v|/2$, $v\in S^{n-1}$ satisfies $\|f\|_{BL}=1$. Then, using (6), (7), (16), (17), and (24), we obtain

$$|h_{\Pi K}(u)-h_{\Pi L}(u)|=|b_K(u)-b_L(u)|\le d_D(S(K,\cdot),S(L,\cdot))\le 2d_P(S(K,\cdot),S(L,\cdot))<2\varepsilon,$$

for each $u\in S^{n-1}$.

Since $K \in \mathcal{K}^n(r, R)$, we have $\Pi K \in \mathcal{K}^n\left(\kappa_{n-1} r^{n-1}, \kappa_{n-1} R^{n-1}\right)$, so $\Pi L \in \mathcal{K}^n(\kappa_{n-1} r^{n-1} - 2\varepsilon, \kappa_{n-1} R^{n-1} + 2\varepsilon)$. Now exactly the same argument as in the proof of Lemma 4.2 of [25], beginning with formula (16) in that paper, yields the existence of a_1 and a_0. (The assumption of o-symmetry made in [25] is only needed for the latter. Explicit values for a_0 and a_1 can be given in terms of ε, r, and R, but we do not need them here.) $\square$

Lemma 3.3. *Let K be a convex body in $\mathbb{R}^n$. Then there is an $\varepsilon_0 > 0$ such that for all $0 < \varepsilon < \varepsilon_0$, if Q is an o-symmetric convex polytope in $\mathbb{R}^n$ such that either*

$$d_P(S(\nabla K, \cdot), S(Q, \cdot)) < \varepsilon \tag{25}$$

or

$$d_P(S(DK, \cdot), S(Q, \cdot)) < \varepsilon, \tag{26}$$

then there is a constant $c_1 > 0$ depending only on K and a convex polytope J whose facets are each parallel to some facet of Q, such that

$$d_P(S(K, \cdot), S(J, \cdot)) < c_1\varepsilon. \tag{27}$$

Proof. We choose $\varepsilon_0 > 0$ so that Lemma 3.2 holds when ε is replaced by ε_0 and K is replaced by either ∇K or DK, as appropriate. Let $0 < \varepsilon < \varepsilon_0$.

Let $\pm u_1, \dots, \pm u_s$ be the outer unit normals to the facets of Q and for $i = s+1, \dots, 2s$, let $u_i = -u_{i-s}$. Set $I = \{1, \dots, 2s\}$.

Suppose that (25) holds. By (14), $S(\nabla K, E) < S(Q, E_\varepsilon) + \varepsilon$ for each Borel subset E of S^{n-1}. If $E_\varepsilon \cap \cup_{i\in I}\{u_i\} = \emptyset$, we have $S(Q, E_\varepsilon) = 0$. This implies that $S(\nabla K, E) < \varepsilon$ and so by (5),

$$S(K, E) < 2\varepsilon. \tag{28}$$

If instead (26) holds, then (14) implies that $S(DK, E) < S(Q, E_\varepsilon) + \varepsilon$ for each Borel subset E of S^{n-1}. Then, if $E_\varepsilon \cap \cup_{i\in I}\{u_i\} = \emptyset$, we have $S(DK, E) < \varepsilon$. By [44, (5.1.17), p. 275],

$$S(DK, E) = S(K + (-K), E) = S(K, E) + \sum_{j=1}^{n-1} \binom{n-1}{j} S(K, n-1-j; -K, j, E),$$

where $S(K, n-1-j; -K, j, \cdot)$ denotes the mixed area measure of $n-1-j$ copies of K and j copies of $-K$. Since all these terms are nonnegative, we obtain $S(K, E) < \varepsilon$ and so (28) holds again.

For $i \in I$, let

$$V_i = \{u \in S^{n-1} : |u - u_i| \le |u - u_j| \text{ for each } j \in I,\ j \ne i\}$$

be the Voronoi cell in S^{n-1} containing u_i. Choose Borel sets W_i such that $\operatorname{relint} V_i \subset W_i \subset V_i$ for each i and $W_i \cap W_j = \emptyset$ for $i \ne j$, so that $\{W_i : i \in I\}$ forms a partition of S^{n-1}.

Let $a_i = S(K, W_i)$ and let $w = \sum_{i\in I} a_i u_i$. Since $S(K, \cdot)$ is balanced (cf. (4)), we have

$$\begin{aligned} w = \sum_{i\in I} a_i u_i &= \sum_{i\in I} u_i \int_{W_i} dS(K,u) - \int_{S^{n-1}} u\, dS(K,u) \\ &= \sum_{i\in I} \int_{W_i} (u_i - u)\, dS(K,u). \end{aligned}$$

For each $u \in S^{n-1}$ and $t > 0$, let $C_t(u) = \{v \in S^{n-1} : |u - v| \le t\}$. Let $W = \cup_{i\in I}(W_i \setminus C_\varepsilon(u_i))$. Then $u_i \notin W_\varepsilon$ for $i \in I$, so (28) implies that $S(K, W) < 2\varepsilon$. Using this, we obtain

$$\begin{aligned} |w| &= \left| \sum_{i\in I} \int_{W_i \cap C_\varepsilon(u_i)} (u_i - u)\, dS(K,u) + \sum_{i\in I} \int_{W_i \setminus C_\varepsilon(u_i)} (u_i - u)\, dS(K,u) \right| \\ &\le \sum_{i\in I} \int_{W_i \cap C_\varepsilon(u_i)} |u_i - u|\, dS(K,u) + 2\int_W dS(K,u) \\ &< \varepsilon S(K, S^{n-1}) + 4\varepsilon = (S(K) + 4)\varepsilon. \end{aligned} \tag{29}$$

Since Q is o-symmetric, we can apply Lemma 3.2 (with K and L replaced by ∇K (or DK) and Q, respectively) and Lemma 3.1 to conclude that there exist outer unit normal vectors $u_{i_1}, \dots, u_{i_n}$ to facets of Q such that $|\det(u_{i_1}, \dots, u_{i_n})| > c_2$, where c_2 depends only on K. In particular, $u_{i_1}, \dots, u_{i_n}$ forms a basis for $\mathbb{R}^n$, so there exist real numbers $b_{i_1}, \dots, b_{i_n}$ such that

$$-w = \sum_{j=1}^{n} b_{i_j} u_{i_j}.$$

Replacing u_{i_j} by $-u_{i_j}$, if necessary, we may assume that $b_{i_j} > 0$ for $j = 1, \dots, n$. By Cramer's rule, we obtain $b_{i_j} \le |w|/|\det(u_{i_1}, \dots, u_{i_n})| < |w|/c_2$, for $j = 1, \dots, n$. Define $b_i = 0$ for each $i \in I$ such that $i \notin \{i_1, \dots, i_n\}$. Then, by (29),

$$\sum_{i\in I} b_i \le n|w|/c_2 < c_3\varepsilon, \tag{30}$$

where c_3 depends only on K.

Let

$$\mu_0 = \sum_{i\in I} a_i \delta_{u_i} \text{ and } \mu_1 = \sum_{i\in I} b_i \delta_{u_i},$$

and let $\mu = \mu_0 + \mu_1$. Then the support of μ is not contained in a great sphere, and since

$$\int_{S^{n-1}} u\, d\mu(u) = \sum_{i\in I} (a_i + b_i) u_i = w - w = o,$$

μ is balanced. By Minkowski's existence theorem [20, Theorem A.3.2], there is a convex polytope J such that $S(J, \cdot) = \mu$. By its definition, each facet of J is parallel to a facet of Q.

It remains to prove (27). Using (30), we obtain

$$\begin{aligned} d_P(S(J,\cdot),S(K,\cdot)) &= d_P(\mu_0+\mu_1,S(K,\cdot)) \le d_P(\mu_0+\mu_1,\mu_0)+d_P(\mu_0,S(K,\cdot)) \\ &= d_P(\mu_1,0)+d_P(\mu_0,S(K,\cdot)) < c_3\varepsilon + d_P(\mu_0,S(K,\cdot)), \end{aligned}$$

where 0 is the zero measure in S^{n-1}. In view of $\mu_0(S^{n-1}) = S(K,S^{n-1})$ and (15), it is therefore enough to find a constant c_4, depending only on K, such that

$$\mu_0(E) < S(K,E_{c_4\varepsilon}) + c_4\varepsilon, \tag{31}$$

for any Borel set E in S^{n-1}. Let $X = \cup\{W_i : u_i \in E\} \setminus E_\varepsilon$. We have

$$\begin{aligned} S(K,E_\varepsilon) &\ge S\left(K,E_\varepsilon \cap (\cup\{W_i : u_i \in E\})\right) \\ &= \sum\{S(K,W_i) : u_i \in E\} - S(K,X) = \mu_0(E) - S(K,X). \end{aligned} \tag{32}$$

If $x \in X$, then for some i with $u_i \in E$ we have $x \in W_i$, and so $|x-u_i| \ge \varepsilon$ since $x \notin E_\varepsilon$. Moreover, if $j \ne i$, then $|u_j - x| \ge |u_i - x| \ge \varepsilon$. Hence $\cup_{i\in I}\{u_i\} \cap X_\varepsilon = \emptyset$, and by (28), we have $S(K,X) < 2\varepsilon$. Now (32) implies that (31) holds with $c_4 = 2$. □

For a fixed finite set $z_1,\dots,z_q$ of points in $\mathbb{R}^n$, define a pseudonorm $|\cdot|_q$ by

$$|f|_q = \left(\frac{1}{q}\sum_{i=1}^{q} f(z_i)^2\right)^{1/2}, \tag{33}$$

where f is any real-valued function on $\mathbb{R}^n$. For a convex body K contained in C_0^n, vector $\mathbf{z}_q = (z_1,\dots,z_q)$ of the points $z_1,\dots,z_q$ in $\mathbb{R}^n$, and vector $\mathbf{X}_q = (X_1,\dots,X_q)$ of random variables $X_1,\dots,X_q$, let

$$\Psi(K,\mathbf{z}_q,\mathbf{X}_q) = \frac{1}{q}\sum_{i=1}^{q} g_K(z_i)X_i. \tag{34}$$

Lemma 3.4. *Let $k \in \mathbb{N}$ and let $K_0 \subset C_0^n$ be a convex body with its centroid at the origin. Suppose that P_k is an output from Algorithm NoisyCovLSQ as stated above. Let $P(a)$ be any convex polytope admissible for the minimization problem (21). Then*

$$|g_{K_0} - g_{P_k}|_{I_k}^2 \le 2\Psi(P_k,\mathbf{x}_{I_k},\mathbf{N}_{I_k}) - 2\Psi(P(a)\cap C_0^n,\mathbf{x}_{I_k},\mathbf{N}_{I_k}) + \left|g_{K_0} - g_{P(a)\cap C_0^n}\right|_{I_k}^2, \tag{35}$$

where for each $k \in \mathbb{N}$, $|\cdot|_{I_k}$ and $\Psi(K,\mathbf{x}_{I_k},\mathbf{N}_{I_k})$ are defined by (33) and (34), respectively, with $q = I_k$, $\mathbf{x}_{I_k} = (x_{1k},\dots,x_{I_k k})$, and $\mathbf{N}_{I_k} = (N_{1k},\dots,N_{I_k k})$.

Proof. If $P(\hat{a}) \cap C_0^n$ is a solution of (21), then since $g_{P_k} = g_{P(\hat{a})\cap C_0^n}$, we obtain

$$\sum_{i=1}^{I_k} (M_{ik} - g_{P_k}(x_{ik}))^2 \le \sum_{i=1}^{I_k} \left(M_{ik} - g_{P(a)\cap C_0^n}(x_{ik})\right)^2,$$

Substituting for M_{ik} from (19) and rearranging, we obtain

$$\begin{aligned}\sum_{i=1}^{I_k}\left(g_{K_0}(x_{ik})-g_{P_k}(x_{ik})\right)^2 \;\le\;& 2\sum_{i=1}^{I_k} g_{P_k}(x_{ik})N_{ik}-2\sum_{i=1}^{I_k} g_{P(a)\cap C_0^n}(x_{ik})N_{ik}+\\ &+\sum_{i=1}^{I_k}\left(g_{K_0}(x_{ik})-g_{P(a)\cap C_0^n}(x_{ik})\right)^2.\end{aligned}$$

In view of (33) and (34), this is the required inequality. □

Let K be any convex body in $\mathbb{R}^n$ and let $\varepsilon > 0$. The *inner parallel body* $K \ominus \varepsilon B^n$ is the Minkowski difference of K and εB^n as defined in (2). Then

$$K \ominus \varepsilon B^n = \bigcap_{y\in\varepsilon B^n}(K-y),$$

so the inner parallel body is convex. (It may be empty.) For further properties, see [44, pp. 133–137]. The following proposition is an immediate consequence of the fact that if K is a convex body in $\mathbb{R}^n$, then

$$V(K) - V(K \ominus \varepsilon B^n) < S(K)\varepsilon. \tag{36}$$

This follows directly from either an inequality of Sangwine-Yager or one of Brannen; see Theorem 1 or Corollary 2 of [14], respectively. The estimate (36) both generalizes and strengthens [23, Lemma 4.2], which concerns the case $n = 2$. The authors of the latter paper were unaware that an even stronger estimate for $n = 2$ was found earlier by Matheron [37].

Proposition 3.5. *If $K \subset C_0^n$ is a convex body and $\varepsilon > 0$, then*

$$V(K) - V(K \ominus \varepsilon B^n) < 2n\varepsilon.$$

Let $\mathcal{G}$ be the class of all nonnegative functions g on $\mathbb{R}^n$ with support in $2C_0^n$ that are the covariogram of some convex body contained in C_0^n, together with the function on $\mathbb{R}^n$ that is identically zero. Note that for each $g \in \mathcal{G}$ and $x \in \mathbb{R}^n$, $g(x) \le g_{C_0^n}(x) \le V(C_0^n) = 1$.

Lemma 3.6. *Let $0 < \varepsilon < 1$ be given. Then there is a finite set $\{(g_j^L, g_j^U) : j = 1,\dots,m\}$ of pairs of functions in $\mathcal{G}$ such that*

(i) $\|g_j^U - g_j^L\|_1 \le \varepsilon$ *for* $j = 1,\dots,m$ *and*
(ii) *for each $g \in \mathcal{G}$, there is an $j \in \{1,\dots,m\}$ such that $g_j^L \le g \le g_j^U$.*

Proof. Let $0 < \varepsilon < 1$ and let $c_5 = c_5(n) \ge 1$ be a constant, to be chosen later. Since $\mathcal{K}^n(C_0^n)$ with the Hausdorff metric is compact, there is an ε/c_5-net $\{K_1,\dots,K_m\}$ in $\mathcal{K}^n(C_0^n)$. For each $j = 1,\dots,m$, let $K_j^U = (K_j + (\varepsilon/c_5)B^n) \cap C_0^n$ and $K_j^L = K_j \ominus (\varepsilon/c_5)B^n$. Define $g_j^U = g_{K_j^U}$ and $g_j^L = g_{K_j^L}$, $j = 1,\dots,m$. Both g_j^U and g_j^L belong to $\mathcal{G}$, $j = 1,\dots,m$.

We first prove (ii). Let $g \in \mathcal{G}$. There is a $K \in \mathcal{K}^n(C_0^n)$ such that $g = g_K$. Choose $j \in \{1,\dots,m\}$ such that $\delta(K, K_j) \le \varepsilon/c_5$. Since $K \subset C_0^n$ and $K \subset K_j + (\varepsilon/c_5)B^n$, we have

$K \subset (K_j + (\varepsilon/c_5)B^n) \cap C_0^n = K_j^U$. Also, we have

$$(K_j \ominus (\varepsilon/c_5)B^n) + (\varepsilon/c_5)B^n \subset K_j \subset K + (\varepsilon/c_5)B^n,$$

yielding $K_j^L = K_j \ominus (\varepsilon/c_5)B^n \subset K$. These facts imply that $g_j^L \le g \le g_j^U$, as required.

It remains to prove (i). It is easy to prove (see, for example, [44, p. 411]) that for any convex body L in $\mathbb{R}^n$,

$$\int_{DL} g_L(x)\,dx = V(L)^2.$$

Applying this, Steiner's formula with quermassintegrals (see [20, (A.30), p. 404], basic properties of mixed volumes (see [20, (A.16) and (A.18), p. 399]) together with $K_j \subset C_0^n \subset (n/4)^{1/2}B^n$ and $c_5 \ge 1$, and Proposition 3.5 with ε replaced by ε/c_5, we obtain

$$\begin{aligned}
\|g_j^U - g_j^L\|_1 &= \int_{2C_0^n} \left(g_j^U(x) - g_j^L(x)\right)\,dx = V\left(K_j^U\right)^2 - V\left(K_j^L\right)^2 \le 2\left(V\left(K_j^U\right) - V\left(K_j^L\right)\right) \\
&\le 2\left(\left(V\left(K_j + \frac{\varepsilon}{c_5}B^n\right) - V(K_j)\right) + \left(V(K_j) - V\left(K_j \ominus \frac{\varepsilon}{c_5}B^n\right)\right)\right) \\
&\le 2\left(\kappa_n \sum_{i=1}^n \binom{n}{i}\left(\frac{n}{4}\right)^{(n-i)/2} + 2n\right)\left(\frac{\varepsilon}{c_5}\right) < \varepsilon,
\end{aligned}$$

provided that c_5 is chosen sufficiently large. □

By analogy with [46, Definition 2.2], we refer to a finite set $\{(g_j^L, g_j^U) : j = 1, \dots, m\}$ of pairs of functions in $\mathcal{G}$ satisfying (i) and (ii) of Lemma 3.6 as an *ε-net with bracketing* for the class $\mathcal{G}$.

The following proposition is a version of the strong law of large numbers. It is proved in detail in [23, Lemma 4.4], with $m_k = k$, and the variation stated here is established in the same way.

Proposition 3.7. *Let X_{ik}, $k \in \mathbb{N}$, $i = 1, \dots, m_k$, where $m_k \ge k$, be an independent family of random variables, each with zero mean. If there is a constant C such that*

$$E\left(X_{ik}^4\right) \le C, \qquad k \in \mathbb{N},\ i = 1, \dots, m_k, \tag{37}$$

then, almost surely,

$$\frac{1}{m_k}\sum_{i=1}^{m_k} X_{ik} \to 0 \tag{38}$$

as $k \to \infty$.

Lemma 3.8. *For every $k \in \mathbb{N}$, let x_{ik}, $i = 1, \dots, I_k$, be the points in the cubic array $2C_0^n \cap (1/k)\mathbb{Z}^n$. Let N_{ik}, $k \in \mathbb{N}$, $i = 1, \dots, I_k$, be independent normal $N(0, \sigma^2)$ random variables. Then, almost surely,*

$$\sup_{K \in \mathcal{K}^n(C_0^n)} \Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) \to 0$$

as $k \to \infty$, where for each $k \in \mathbb{N}$, $\Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k})$ is defined by (34) with $q = I_k$, $\mathbf{x}_{I_k} = (x_{1k}, \dots, x_{I_k k})$, and $\mathbf{N}_{I_k} = (N_{1k}, \dots, N_{I_k k})$.

Proof. Let $0 < \varepsilon < 1$ and let $\{(g_j^L, g_j^U) : j = 1, \dots, m\}$ be an ε-net with bracketing for $\mathcal{G}$, as provided by Lemma 3.6. Let $K \in \mathcal{K}^n(C_0^n)$ and let $g = g_K \in \mathcal{G}$. Choose $j \in \{1, \dots, m\}$ such that $g_j^L \le g \le g_j^U$. Define $N_{ik}^+ = \max\{N_{ik}, 0\}$ and $N_{ik}^- = N_{ik}^+ - N_{ik}$ for $k \in \mathbb{N}$ and $i = 1, \dots, I_k$. Then for $k \in \mathbb{N}$, we have

$$\begin{aligned}\Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) &= \frac{1}{I_k}\sum_{i=1}^{I_k} g(x_{ik}) N_{ik}^+ - \frac{1}{I_k}\sum_{i=1}^{I_k} g(x_{ik}) N_{ik}^- \\ &\le \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^U(x_{ik}) N_{ik}^+ - \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^L(x_{ik}) N_{ik}^- \\ &\le W_k(\varepsilon),\end{aligned}$$

where

$$W_k(\varepsilon) = \max_{j=1,\dots,m} \left\{ \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^U(x_{ik}) N_{ik}^+ - \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^L(x_{ik}) N_{ik}^- \right\} \tag{39}$$

is independent of K. Consequently,

$$\sup_{K \in \mathcal{K}^n(C_0^n)} \Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) \le W_k(\varepsilon), \tag{40}$$

for all $0 < \varepsilon < 1$.

Fix $j \in \{1, \dots, m\}$, and let

$$X_{ik} = g_j^U(x_{ik}) N_{ik}^+ - g_j^U(x_{ik}) E(N_{ik}^+),$$

for $k \in \mathbb{N}$ and $i = 1, \dots, I_k$. Since $g_j^U(x_{ik}) \le 1$, it is easy to check that the random variables X_{ik} satisfy the hypotheses of Proposition 3.7. By (38), we obtain, almost surely,

$$\lim_{k\to\infty} \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^U(x_{ik}) N_{ik}^+ = \lim_{k\to\infty} \frac{1}{I_k}\sum_{i=1}^{I_k} g_j^U(x_{ik}) E(N_{ik}^+) = \frac{E(N_{11}^+)}{2^n} \int_{2C_0^n} g_j^U(x)\, dx.$$

The same argument applies when X_{ik} is defined by $X_{ik} = g_j^L(x_{ik}) N_{ik}^- - g_j^L(x_{ik}) E(N_{jk}^-)$. Therefore, almost surely,

$$\lim_{k\to\infty} W_k(\varepsilon) = \frac{1}{2^n} \max_{j=1,\dots,m} \left\{ E(N_{11}^+) \int_{2C_0^n} g_j^U(x)\, dx - E(N_{11}^-) \int_{2C_0^n} g_j^L(x)\, dx \right\}.$$

Since the variable N_{11} has zero mean, $E(N_{11}^-) = E(N_{11}^+)$. Also, by Lemma 3.6(i) we have $\|g_j^U - g_j^L\|_1 \le \varepsilon$ and by Lemma 3.6(ii) we may assume that $g_j^U - g_j^L \ge 0$, for $i = 1, \dots, m$. We conclude that, almost surely,

$$\lim_{k\to\infty} W_k(\varepsilon) = \frac{1}{2^n} \max_{j=1,\dots,m} E(N_{11}^+) \int_{2C_0^n} (g_j^U(x) - g_j^L(x))\, dx \le E(N_{11}^+)\, \varepsilon / 2^n.$$

This and (40) complete the proof. □

Lemma 3.9. *Let $K_0 \subset C_0^n$ be a convex body with its centroid at the origin. Suppose that P_k is an output from Algorithm NoisyCovLSQ as stated above. Then, almost surely,*

$$\lim_{k\to\infty} |g_{K_0} - g_{P_k}|_{I_k} = 0. \tag{41}$$

Proof. Let Q_k be the o-symmetric polytope from the input of Algorithm NoisyCovLSQ that satisfies, almost surely, (20). Fix a realization for which (20) holds. We may assume that

$$\lim_{k\to\infty} \delta(Q_k, \nabla K_0) = 0,$$

as the other case is completely analogous. By [44, Theorem 4.2.1], $S(Q_k,\cdot)$ converges weakly to $S(\nabla K_0,\cdot)$ as $k\to\infty$. By [11, Theorem 6.8], weak convergence is equivalent to convergence in the Prohorov metric, so $S(Q_k,\cdot)$ converges in the Prohorov metric to $S(\nabla K_0,\cdot)$ as $k\to\infty$. Now Lemma 3.3 ensures that if J_k is the convex polytope corresponding to Q_k in that lemma, then $S(J_k,\cdot)$ converges in the Prohorov metric to $S(K_0,\cdot)$ as $k\to\infty$. We may assume that the centroid of J_k is at the origin for each k. By Lemma 3.2 (with K and L replaced by K_0 and J_k, respectively), there are constants a_1 and $k_0\in\mathbb{N}$, depending only on K_0, such that $J_k \subset a_1 B^n$ for all $k \ge k_0$. By Blaschke's selection theorem and the fact that a convex body is determined up to translation by its surface area measure, the sequence (J_k) has an accumulation point and every such accumulation point must be a translate of K_0. But J_k and K_0 have their centroids at the origin and $K_0 \subset C_0^n$, so

$$\lim_{k\to\infty} \delta(K_0, J_k\cap C_0^n) = \lim_{k\to\infty} \delta(K_0, J_k) = 0.$$

(This consequence of the fact that $d_P(S(J_k,\cdot), S(K_0,\cdot)) \to 0$ as $k\to\infty$ can also be derived from a stability estimate of Hug and Schneider [29, Theorem 3.1], but we do not need the full force of that result here.) It follows from the continuity of volume that $\|g_{K_0} - g_{J_k\cap C_0^n}\|_\infty \to 0$ as $k\to\infty$ and hence that

$$\lim_{k\to\infty} \left|g_{K_0} - g_{J_k\cap C_0^n}\right|_{I_k} = 0. \tag{42}$$

Next, we observe that J_k can serve as the $P(a)$ in Lemma 3.4. By its definition, a translate of P_k is contained in C_0^n, and the quantity $\Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k})$ is unaffected by this translation. From Lemma 3.8 we obtain

$$\lim_{k\to\infty} \Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) = 0 \quad \text{and} \quad \lim_{k\to\infty} \Psi(J_k\cap C_0^n, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) = 0. \tag{43}$$

Now (41) follows directly from (35) (with $P(a)$ replaced by J_k), (42), and (43). □

Theorem 3.10. *Suppose that $K_0 \subset C_0^n$ is a convex body with its centroid at the origin. Suppose also that K_0 is determined, up to translation and reflection in the origin, among all convex bodies in $\mathbb{R}^n$, by its covariogram. If P_k, $k\in\mathbb{N}$, is an output from Algorithm NoisyCovLSQ as stated above, then, almost surely,*

$$\min\{\delta(K_0, P_k), \delta(-K_0, P_k)\} \to 0 \tag{44}$$

as $k\to\infty$.

Proof. By Lemma 3.9, almost surely,

$$\left|g_{K_0} - g_{P_k}\right|_{I_k} \to 0, \tag{45}$$

as $k \to \infty$. Fix a realization for which this statement holds. For each k, P_k has its centroid at the origin and is a translate of a subset of C_0^n, so $P_k \subset 2C_0^n$ and by Blaschke's selection theorem, (P_k) has an accumulation point, L, say. Note that L must also have its centroid at the origin.

Let $(P_{k'})$ be a subsequence converging to L. Then since $g_{K_0} - g_{P_{k'}}$ converges uniformly to $g_{K_0} - g_L$ as $k' \to \infty$, we have

$$\left|g_{K_0} - g_{P_{k'}}\right|^2_{M_{k'}} \to \frac{1}{2^n}\int_{2C_0^n} \left(g_{K_0}(x) - g_L(x)\right)^2 dx,$$

as $k' \to \infty$. From this and (45), we obtain $\|g_{K_0} - g_L\|_{L^2(2C_0^n)} = 0$ and hence $g_{K_0} = g_L$ on $2C_0^n$. As the support of g_{K_0} is contained in $2C_0^n$ and both $g_{K_0}^{1/n}$ and $g_L^{1/n}$ are concave on their supports, we have $g_{K_0} = g_L$ in $\mathbb{R}^n$. The hypothesis on K_0 now implies that $L = \pm K_0$. Since L was an arbitrary accumulation point of (P_k), we obtain (44). □

4. Approximating the Blaschke body via the covariogram

Algorithm NoisyCovBlaschke

Input: Natural numbers $n \geq 2$ and k; mutually nonparallel vectors $u_i \in S^{n-1}$, $i = 1, \dots, k$ that span $\mathbb{R}^n$; noisy covariogram measurements

$$M_{ij}^{(1)} = g_{K_0}(o) + N_{ij}^{(1)} \quad \text{and} \quad M_{ij}^{(2)} = g_{K_0}((1/k)u_i) + N_{ij}^{(2)},$$

for $i = 1, \dots, k$ and $j = 1, \dots, k^2$, of an unknown convex body $K_0 \subset C_0^n$ whose centroid is at the origin, where the $N_{ij}^{(m)}$'s are independent normal $N(0, \sigma^2)$ random variables.

Task: Construct an o-symmetric convex polytope Q_k that approximates the Blaschke body ∇K_0.

Action:

1. For $i = 1, \dots, k$ and $j = 1, \dots, k^2$, let

$$y_{ik} = \frac{1}{k^2}\sum_{j=1}^{k^2} k\left(M_{ij}^{(1)} - M_{ij}^{(2)}\right).$$

2. With the natural numbers $n \geq 2$ and k, and vectors $u_i \in S^{n-1}$, $i = 1, \dots, k$ use the sample means y_{ik} instead of noisy measurements of the brightness function $b_K(u_i)$ as input to Algorithm NoisyBrightLSQ (see [24, p. 1352]). The output of the latter algorithm is Q_k.

Lemma 4.1. *Let $r > 0$ and let K be a convex body with $rB^n \subset K$. If $0 < t \leq 2r$, then*

$$\left(1 - \frac{t}{2r}\right)^{n-1} b_K(u) \leq \frac{g_K(o) - g_K(tu)}{t} \leq b_K(u), \tag{46}$$

for all $u \in S^{n-1}$.

Proof. Let $u \in S^{n-1}$. By (12), we have

$$g_K(o) - g_K(tu) = \int_0^t a_K(s,u)\, ds.$$

From this and the fact that $a_K(\cdot, u)$ is decreasing, we obtain

$$a_K(t,u) \leq \frac{g_K(o) - g_K(tu)}{t} \leq a_K(0,u) = b_K(u). \tag{47}$$

The set

$$M = \operatorname{conv}\left((K|u^\perp) \cup [-ru, ru]\right)$$

is generally not a subset of K, but elementary geometry using $[-ru, ru] \subset K$ and (10) gives

$$\left(1 - \frac{t}{2r}\right)\left(K|u^\perp\right) = E_M(t,u) \subset E_K(t,u).$$

Taking the $(n-1)$-dimensional volumes of these sets and using (11) yields

$$\left(1 - \frac{t}{2r}\right)^{n-1} b_K(u) \leq a_K(t,u).$$

The lemma follows from the previous inequality and (47). $\square$

An inequality similar to (46) was derived in [31, Theorem 1] for $n = 2$.

For a fixed finite set $u_1, \dots, u_q$ of points in S^{n-1}, define a pseudonorm $|\cdot|_q$ by

$$|f|_q = \left(\frac{1}{q}\sum_{i=1}^{q} f(u_i)^2\right)^{1/2}, \tag{48}$$

where f is any real-valued function on S^{n-1}. For a convex body K contained in C_0^n, a sequence (u_i) in S^{n-1}, and a vector $\mathbf{X}_k = (X_{1k}, \dots, X_{kk})$ of random variables, let

$$\Psi(K, (u_i), \mathbf{X}_k) = \frac{1}{k}\sum_{i=1}^{k} b_K(u_i) X_{ik}.$$

The same notations were used for a technically different pseudonorm and function Ψ in the previous section, but this should cause no confusion.

Lemma 4.2. *Let K_0 be a convex body in $\mathbb{R}^n$ with centroid at the origin and such that $rB^n \subset K_0 \subset C_0^n$ for some $r > 0$. Let (u_i) be a sequence in S^{n-1}. If Q_k is an output* *from Algorithm NoisyCovBlaschke as stated above, then, almost surely, there is a constant* $c_6 = c_6(n, r)$ *such that*

$$|b_{K_0} - b_{Q_k}|_k^2 \le 2\Psi(Q_k, (u_i), \mathbf{X}_k) - 2\Psi(K_0, (u_i), \mathbf{X}_k) + \frac{c_6}{k}|b_{K_0} - b_{Q_k}|_k, \tag{49}$$

for all $k \in \mathbb{N}$.

Proof. For $i = 1, \ldots, k$, we have

$$y_{ik} = \frac{g_{K_0}(o) - g_{K_0}((1/k)u_i)}{1/k} + \frac{1}{k}\sum_{j=1}^{k^2}(N_{ij}^{(1)} - N_{ij}^{(2)}) = \mu_{ik} + X_{ik},$$

say, where the X_{ik}'s are independent normal $N(0, 2\sigma^2)$ random variables. Note that the y_{ik}'s are also independent. By (13),

$$\lim_{k\to\infty} \mu_{ik} = b_{K_0}(u_i).$$

In fact, the convergence is uniform. This is because for each $u \in S^{n-1}$, we have

$$b_{K_0}(u) \le b_{C_0^n}(u) \le b_{(\sqrt{n}/2)B^n}(u) = (n/4)^{(n-1)/2}\kappa_{n-1}$$

and

$$0 \le b_{K_0}(u) - \mu_{ik} \le \left(1 - \left(1 - \frac{1}{2rk}\right)^{n-1}\right) b_{K_0}(u) \le \frac{n-1}{2rk} b_{K_0}(u), \quad k \ge 1/(2r), \tag{50}$$

by Lemma 4.1, so there is a constant $c_7 = c_7(n, r)$ such that

$$0 \le b_{K_0}(u_i) - \mu_{ik} \le \frac{c_7}{k}, \tag{51}$$

for all $k \in \mathbb{N}$ and $i = 1, \ldots, k$.

By the formulation of Algorithms NoisyCovBlaschke and NoisyBrightLSQ (cf. [24, p. 1352]), Q_k minimizes

$$\sum_{i=1}^{k} \left(b_K(u_i) - y_{ik}\right)^2 \tag{52}$$

over the class of all o-symmetric convex bodies K in $\mathbb{R}^n$. By (9), for each convex body there is an o-symmetric convex body with the same brightness function. From this it follows that Q_k is actually a minimizer over the class of all convex bodies K in $\mathbb{R}^n$. Substituting $K = Q_k$ and $K = K_0$ in (52), we obtain

$$\sum_{i=1}^{k} \left(b_{Q_k}(u_i) - \mu_{ik} - X_{ik}\right)^2 \le \sum_{i=1}^{k} \left(b_{K_0}(u_i) - \mu_{ik} - X_{ik}\right)^2.$$

Rearranging and using (48), we obtain

$$|b_{K_0} - b_{Q_k}|_k^2 \le \frac{2}{k}\sum_{i=1}^{k} \left(b_{Q_k}(u_i) - b_{K_0}(u_i)\right)\left(X_{ik} - (b_{K_0}(u_i) - \mu_{ik})\right).$$

The definition of Ψ and Cauchy-Schwarz inequality yields

$$|b_{K_0}-b_{Q_k}|_k^2 \le 2\Psi(Q_k,(u_i),\mathbf{X}_k)-2\Psi(K_0,(u_i),\mathbf{X}_k)+2|b_{K_0}-b_{Q_k}|_k\left(\frac{1}{k}\sum_{i=1}^{k}(b_{K_0}(u_i)-\mu_{ik})^2\right)^{1/2}.$$

In view of (51), this proves (49) with $c_6 = 2c_7$. □

Lemma 4.3. *Suppose that the assumptions of Lemma 4.2 are satisfied with a sequence* (u_i) *such that* (u_i^*) *is evenly spread. Then, almost surely, there are constants* $c_8 = c_8(n, r, (u_i))$ *and* $N_1 = N_1((u_i))$ *such that*

$$S(Q_k) \le c_8, \tag{53}$$

for all $k \ge N_1$.

Proof. By the Cauchy-Schwarz inequality,

$$\Psi(Q_k,(u_i),\mathbf{X}_k)-\Psi(K_0,(u_i),\mathbf{X}_k) \le |b_{K_0}-b_{Q_k}|_k\left(\frac{1}{k}\sum_{i=1}^{k}X_{ik}^2\right)^{1/2}.$$

This and (49) imply that

$$|b_{K_0}-b_{Q_k}|_k \le 2\left(\frac{1}{k}\sum_{i=1}^{k}X_{ik}^2\right)^{1/2}+\frac{c_6}{k},$$

for all $k \in \mathbb{N}$. By Proposition 3.7 with m_k and X_{ik} replaced by k and $X_{ik}^2 - E\,(X_{11}^2)$, respectively, the right-hand side converges, almost surely. Thus, almost surely, there is a constant $c_9 = c_9(n, r)$ such that

$$|b_{K_0}-b_{Q_k}|_k \le c_9. \tag{54}$$

As (u_i^*) is evenly spread, we can apply [24, Lemma 7.1] with K and L replaced by ΠK_0 and ΠQ_k, respectively. Using this, the fact that $\Pi K_0 \subset \Pi C_0^n = 2C_0^n \subset \sqrt{n}B^n$ (see [20, p. 145]), and (6), we find that there are constants $c_{10} = c_{10}((u_i))$ and $N_1 = N_1((u_i))$ such that

$$b_{Q_k} \le c_{10}|b_{K_0}-b_{Q_k}|_k + 2\sqrt{n}, \tag{55}$$

for $k \ge N_1$. Finally, (53) follows directly from (54), (55), and (8). □

Lemma 4.4. *Suppose that the assumptions of Lemma 4.2 are satisfied with a sequence* (u_i) *such that* (u_i^*) *is evenly spread. Then, almost surely,*

$$\lim_{k\to\infty}|b_{K_0}-b_{Q_k}|_k = 0. \tag{56}$$

Proof. Due to (49) and (54), there is, almost surely, a constant $c_{11} = c_{11}(n, r, (u_i))$ such that

$$|b_{Q_k}-b_{K_0}|_k^2 \le 2\Psi(Q_k,(u_i),\mathbf{X}_k)-2\Psi(K_0,(u_i),\mathbf{X}_k)+\frac{c_{11}}{k}, \tag{57}$$

for all $k \ge N_1$. By Proposition 3.7 with $m_k = k$ and X_{ik} replaced by $b_{K_0}(u_i)X_{ik}$, the variable $\Psi(K_0,(u_i),\mathbf{X}_k)$ converges to zero, almost surely, as $k \to \infty$.

For $m \in \mathbb{N}$, let $\mathcal{H}_m = \{K \in \mathcal{K}^n : S(K) \leq m\}$. If we can show that for all $m \in \mathbb{N}$, almost surely,

$$\lim_{k\to\infty} \sup_{K\in\mathcal{H}_m} |\Psi(K,(u_i),\mathbf{X}_k)| = 0, \tag{58}$$

then by (53), almost surely,

$$\lim_{k\to\infty} \Psi(Q_k,(u_i),\mathbf{X}_k) = 0.$$

This and (57) will yield (56), completing the proof.

To prove (58), note first that by (7), we have

$$|\Psi(K,(u_i),\mathbf{X}_k)| = \left|\frac{1}{k}\sum_{i=1}^{k} b_K(u_i)X_{ik}\right| \leq \frac{1}{2}\int_{S^{n-1}} \left|\frac{1}{k}\sum_{i=1}^{k}|u_i\cdot v|X_{ik}\right| \, dS(K,v).$$

Since $S(K) = S(K,S^{n-1}) \leq m$ for $K \in \mathcal{H}_m$, it is enough to prove that, almost surely,

$$\lim_{k\to\infty} \sup_{v\in S^{n-1}} \left|\frac{1}{k}\sum_{i=1}^{k}|u_i\cdot v|X_{ik}\right| = 0. \tag{59}$$

This follows essentially from the uniform continuity of the function $|u_i \cdot v|$, $v \in S^{n-1}$, and the fact that S^{n-1} is compact. In fact, if (59) does not hold almost surely, then there is a $\delta > 0$ such that

$$\limsup_{k\to\infty} \sup_{v\in S^{n-1}} \frac{1}{k}\sum_{i=1}^{k}|u_i\cdot v|X_{ik} > \delta E\left(|X_{11}|\right) \tag{60}$$

with positive probability. Let $\{w_1,\dots,w_m\}$ be a $\delta/2$-net in S^{n-1}. For any realization and any $k \in \mathbb{N}$, there is a $v_k \in S^{n-1}$ such that

$$\frac{1}{k}\sum_{i=1}^{k}|u_i\cdot v_k|X_{ik} = \sup_{v\in S^{n-1}} \frac{1}{k}\sum_{i=1}^{k}|u_i\cdot v|X_{ik}. \tag{61}$$

Let A_j denote the set of all events such that an accumulation point of (v_k) has distance at most $\delta/2$ from w_j, $j = 1,\dots,m$. For a realization in A_j and any subsequence (k') of (k) such that $|v_{k'} - w_j| \leq \delta$ holds for sufficiently large k, we have, almost surely,

$$\limsup_{k'\to\infty} \left|\frac{1}{k'}\sum_{i=1}^{k'}|u_i\cdot v_{k'}|X_{ik'} - \frac{1}{k'}\sum_{i=1}^{k'}|u_i\cdot w_j|X_{ik'}\right| \leq \delta \limsup_{k'\to\infty} \frac{1}{k'}\sum_{i=1}^{k'}|X_{ik'}| = \delta E\left(|X_{11}|\right),$$

by Proposition 3.7. But Proposition 3.7, with m_k and X_{ik} replaced by k' and $|u_i \cdot w_j|X_{ik'}$, respectively, also implies that, almost surely, the second term on the left-hand side converges to zero, as $k' \to \infty$. In view of (61), this yields

$$\limsup_{k'\to\infty} \sup_{v\in S^{n-1}} \frac{1}{k'}\sum_{i=1}^{k'}|u_i\cdot v|X_{ik'} \leq \delta E\left(|X_{11}|\right),$$

for almost all events in A_j. As any sequence in S^{n-1} has at least one accumulation point, the latter inequality holds, almost surely, contradicting (60). □

Theorem 4.5. *Let $K_0 \subset C_0^n$ be a convex body with its centroid at the origin. Let (u_i) be a sequence in S^{n-1} such that (u_i^*) is evenly spread. If Q_k is an output from Algorithm NoisyCovBlaschke as stated above, then, almost surely,*

$$\lim_{k\to\infty} \delta(\nabla K_0, Q_k) = 0. \tag{62}$$

Proof. We have $o \in \operatorname{int} K_0$, so there is an $r > 0$ such that $rB^n \subset K_0$. By Lemmas 4.3 and 4.4, we can fix a realization for which both (53) and (56) are true. Using (6), we observe that (56) is equivalent to

$$\lim_{k\to\infty} |h_{\Pi K_0} - h_{\Pi Q_k}|_k = 0. \tag{63}$$

We also have $h_{\Pi Q_k} = b_{Q_k} \le S(Q_k)$, so by (53), the sets ΠQ_k are uniformly bounded. Exactly as in the proof of [24, Theorem 6.1], with K and P_k replaced by ΠK_0 and ΠQ_k, respectively, we can use the fact that $(u_1, -u_1, u_2, -u_2, \dots)$ is evenly spread to conclude that

$$\lim_{k\to\infty} \delta(\Pi K_0, \Pi Q_k) = 0. \tag{64}$$

Now $rB^n \subset K_0 \subset C_0^n$ yields $sB^n \subset \Pi K_0 \subset tB^n$ with $s = \kappa_{n-1} r^{n-1}$ and $t = \sqrt{n}$. Moreover, (6) and (9) give $\Pi(\nabla K_0) = \Pi K_0$. Hence (64) implies that

$$\frac{s}{2} B^n \subset \Pi(\nabla K_0), \Pi Q_k \subset \frac{3t}{2} B^n,$$

for sufficiently large k, where s and t depend only on n and r. Exactly as in the proof from (48) to (49) of [24, Theorem 7.2] (which in turn follows the proof of [25, Lemma 4.2]), this leads to

$$r_0 B^n \subset \nabla K_0, Q_k \subset R_0 B^n,$$

for sufficiently large k, where $r_0 > 0$ and R_0 depend only on n and r. Then (62) follows from (64) and the Bourgain-Campi-Lindenstrauss stability result for projection bodies (see [12] and [16], or [20, Remark 4.3.13]). □

5. APPROXIMATING THE DIFFERENCE BODY VIA THE COVARIOGRAM

Throughout this section, φ will be a nonnegative bounded measurable function on $\mathbb{R}^n$ with support in C_0^n, such that $\int_{\mathbb{R}^n} \varphi(x)\,dx = 1$.

Algorithm NoisyCovDiff(φ)

Input: Natural numbers $n \ge 2$ and k; positive reals δ_k and ε_k; noisy covariogram measurements

$$M_{ik} = g_{K_0}(x_{ik}) + N_{ik}, \tag{65}$$

of an unknown convex body $K_0 \subset C_0^n$ at the points x_{ik}, $i = 1, \dots, I_k$ in the cubic array $2C_0^n \cap (1/k)\mathbb{Z}^n$, where the N_{ik}'s are independent normal $N(0, \sigma^2)$ random variables.

Task: Construct an o-symmetric convex polytope Q_k in $\mathbb{R}^n$ that approximates the difference body DK_0.

Action:

1. Let $\varphi_{\varepsilon_k}(x) = \varepsilon_k^{-n}\varphi(x/\varepsilon_k)$ for $x \in \mathbb{R}^n$, and let

$$g_k(x) = \sum_{i=1}^{I_k} M_{ik} \int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\,dz = \left(\sum_{i=1}^{I_k} M_{ik}\, 1_{(1/k)C_0^n + x_{ik}}\right) * \varphi_{\varepsilon_k}\,(x). \tag{66}$$

2. Define the finite set

$$S_k = \{x \in 2C_0^n \cap (1/k)\mathbb{Z}^n : g_k(x) \geq \delta_k\}. \tag{67}$$

The output is the convex polytope $Q_k = (1/2)(\mathrm{conv}\, S_k + (-\mathrm{conv}\, S_k))$.

The input δ_k in the algorithm is a threshold parameter. The function $g_k(x)$ is a Gasser-Müller type kernel estimator for g_{K_0} with kernel function φ and bandwidth ε_k. As the design points x_{ik} are deterministic, g_k is a multivariate fixed design kernel estimator. Such estimators are common in multivariate regression and are discussed in detail by Ahmad and Lin [3]. Among other things, strong pointwise consistency and a bound for the rate of weak pointwise convergence are given there. We shall need uniform bounds and establish them in the next two lemmas. By [3, Theorem 1], for any $x \in \mathbb{R}^n$, $g_k(x)$ is an asymptotically unbiased estimator for $g_{K_0}(x)$, if $\varepsilon_k \to 0$ as $k \to \infty$. We shall show that this holds uniformly in x.

For the convenience of the reader, we provide a proof of the following result of Matheron [38, p.2] that the covariogram of a convex body is a Lipschitz function.

Proposition 5.1. *If K is a convex body in $\mathbb{R}^n$ and $x, y \in \mathbb{R}^n$, then*

$$|g_K(x) - g_K(y)| \leq 2 \max_{u \in S^{n-1}} b_K(u)|x-y|.$$

Proof. Using the formula

$$g_K(x) = \int_{\mathbb{R}^n} 1_K(z) 1_K(z-x)\,dz,$$

we obtain

$$\begin{aligned}
|g_K(x) - g_K(y)| &\leq \int_{\mathbb{R}^n} 1_K(z)|1_K(z-x) - 1_K(z-y)|\,dz \\
&\leq \int_{\mathbb{R}^n} |1_K(z-x) - 1_K(z-y)|\,dz \\
&= \int_{\mathbb{R}^n} \left(1_K(z-x) - 1_K(z-y)\right)^2\,dz = 2\left(g_K(o) - g_K(x-y)\right),
\end{aligned}$$

the first equality holding since the integrand can only take values 0 or 1 and the second by a simple evaluation. Using this and the right-hand inequality in (46), we get

$$|g_K(x) - g_K(y)| \leq 2b_K\left(\frac{x-y}{|x-y|}\right)|x-y|,$$

and the proposition follows immediately. $\square$

Corollary 5.2. *If $K_0 \subset C_0^n$ is a convex body, then for all $x, y \in \mathbb{R}^n$,*

$$|g_{K_0}(x) - g_{K_0}(y)| \le 2\sqrt{n}|x-y|.$$

Proof. Since $K_0 \subset C_0^n$, Proposition 5.1 yields

$$|g_K(x) - g_K(y)| \le 2 \max_{u \in S^{n-1}} b_{C_0^n}(u)|x-y|.$$

By Cauchy's projection formula (7), for $u = (u_1, u_2, \dots, u_n) \in S^{n-1}$ we have

$$b_{C_0^n}(u) = V\left(C_0^n | u^\perp\right) = \sum_{i=1}^n |u_i|,$$

from which it is easy to see that $b_{C_0^n}(u) \le \sqrt{n}$. □

Lemma 5.3. *Suppose that K_0, ε_k, and g_k are as in Algorithm NoisyCovDiff(φ). For each $k \in \mathbb{N}$ and $x \in \mathbb{R}^n$,*

$$|E\left(g_k(x)\right) - g_{K_0}(x)| \le 2n(\varepsilon_k + 1/k).$$

Consequently, g_k is uniformly asymptotically unbiased whenever $\lim_{k\to\infty} \varepsilon_k = 0$.

Proof. Using (65), (66), and the definition of φ_{ε_k}, we obtain

$$|E\left(g_k(x)\right) - g_{K_0}(x)| \le \sum_{i=1}^{I_k} |g_{K_0}(x_{ik}) - g_{K_0}(x)| \int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\, dz, \tag{68}$$

for all $x \in \mathbb{R}^n$. The support of φ_{ε_k} is contained in $\varepsilon_k C_0^n$, so for fixed x, the support of the integrand $\varphi_{\varepsilon_k}(x-z)$ is contained in $\varepsilon_k C_0^n + x$. Now if $x_{ik} \notin (\varepsilon_k + 1/k)C_0^n + x$, then $\varepsilon_k C_0^n + x$ and $(1/k)C_0^n + x_{ik}$ are disjoint, so the corresponding summand in (68) vanishes. Moreover, for $x_{ik} \in (\varepsilon_k + 1/k)C_0^n + x$, Corollary 5.2 and the fact that the diameter of C_0^n is $\sqrt{n}$ imply that

$$|g_{K_0}(x_{ik}) - g_{K_0}(x)| \le 2n(\varepsilon_k + 1/k).$$

Consequently,

$$\begin{aligned} |E\left(g_k(x)\right) - g_{K_0}(x)| &\le 2n(\varepsilon_k + 1/k) \sum_{i=1}^{I_k} \int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\, dz \\ &\le 2n(\varepsilon_k + 1/k) \int_{\mathbb{R}^n} \varphi_{\varepsilon_k}(x-z)\, dz = 2n(\varepsilon_k + 1/k), \end{aligned}$$

as required. □

In [3, Lemma 1], a polynomial rate of convergence result in the weak sense is established. In contrast, we assume Gaussian measurement errors, which allows us to obtain an exponential convergence rate.

Lemma 5.4. *Suppose that K_0, ε_k, and g_k are as in Algorithm NoisyCovDiff(φ) and let $\delta > 0$ and $\lim_{k\to\infty}\varepsilon_k = 0$. Then there is a constant $N_2 = N_2((\varepsilon_k), n) \in \mathbb{N}$ such that*

$$\Pr\left(|g_k(x) - g_{K_0}(x)| > \delta\right) \le c_{12}(\delta(k\varepsilon_k)^{n/2})^{-1}\exp\left(-c_{13}\delta^2(k\varepsilon_k)^n\right) \tag{69}$$

for all $k \ge N_2$ and all $x \in \mathbb{R}^n$, where $c_{12} = (4\pi c_{13})^{-1/2}$ and $c_{13} = (8\sigma^2\|\varphi\|_\infty)^{-1}$.

Proof. Let

$$R_k(x) = g_k(x) - E\left(g_k(x)\right) = \sum_{i=1}^{I_k} N_{ik}\int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\,dz.$$

(Compare (66).) For fixed x, $R_k(x)$ is a weighted sum of independent normal $N(0,\sigma^2)$ random variables, so $R_k(x)$ is $N(0,\tau^2(x))$, where

$$\begin{aligned}
\tau^2(x) &= \sigma^2\sum_{i=1}^{I_k}\left(\int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\,dz\right)^2\\
&\le \sigma^2\|\varphi_{\varepsilon_k}\|_\infty V\left((1/k)C_0^n\right)\sum_{i=1}^{I_k}\int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\,dz\\
&\le \sigma^2(\varepsilon_k)^{-n}\|\varphi\|_\infty\, k^{-n}\int_{\mathbb{R}^n}\varphi_{\varepsilon_k}(x-z)\,dz = \sigma^2\|\varphi\|_\infty(k\varepsilon_k)^{-n}.
\end{aligned}$$

A well-known estimate (see [18, p. 175]) for the one-sided tail probability of a normal $N(0,1)$ random variable N states that

$$\Pr\left(N \ge t\right) \le \frac{1}{\sqrt{2\pi}t}\exp\left(-\frac{t^2}{2}\right),$$

for all $t > 0$. Hence

$$\Pr\left(|R_k(x)| \ge \delta/2\right) \le c_{12}(\delta(k\varepsilon_k)^{n/2})^{-1}\exp(-c_{13}\delta^2(k\varepsilon_k)^n), \tag{70}$$

where c_{12} and c_{13} are as in the statement of the lemma. By Lemma 5.3, there is a constant $N_2 = N_2((\varepsilon_k), n) \in \mathbb{N}$ such that for all $k \ge N_2$ and $x \in \mathbb{R}^n$, we have $|E\left(g_k(x)\right) - g_{K_0}(x)| \le \delta/2$ and therefore

$$\begin{aligned}
\Pr\left(|g_k(x) - g_{K_0}(x)| > \delta\right) &\le \Pr\left(|g_k(x) - E\left(g_k(x)\right)| + |E\left(g_k(x)\right) - g_{K_0}(x)| > \delta\right)\\
&\le \Pr\left(|R(x)| > \delta/2\right).
\end{aligned}$$

Now (69) follows from this and (70). □

For a convex body K in $\mathbb{R}^n$ and $\delta > 0$, let $K(\delta) = \{x \in \mathbb{R}^n : g_K(x) \ge \delta\}$. Since $g_K^{1/n}$ is concave on its support, $K(\delta)$ is a compact convex set, sometimes called a convolution body of K. References to results on convolution bodies can be found in [20, p. 378].

Lemma 5.5. *Let K be a convex body in $\mathbb{R}^n$. If $0 < \delta < V(K)$, then*

$$\left(1 - \frac{\delta^{1/n}}{V(K)^{1/n}}\right)DK \subset K(\delta).$$

Proof. Let $t = (\delta/V(K))^{1/n}$ and let $x \in (1-t)DK$. Since DK is the support of g_K, there is a y in the support of g_K such that $x = (1-t)y + to$. As $g_K^{1/n}$ is concave on its support, we have

$$g_K(x)^{1/n} \geq (1-t)g_K(y)^{1/n} + tg_K(o)^{1/n} \geq tV(K)^{1/n} = \delta^{1/n}.$$

It follows that $x \in K(\delta)$. □

Theorem 5.6. *Suppose that K_0, δ_k, ε_k, and g_k are as in Algorithm NoisyCovDiff(φ). Assume that $\lim_{k\to\infty} \varepsilon_k = \lim_{k\to\infty} \delta_k = 0$ and that*

$$\liminf_{k\to\infty} \frac{\delta_k^2 (k\varepsilon_k)^n}{\log k} \geq \frac{n+2}{c_{13}}, \tag{71}$$

where c_{13} is as in Lemma 5.4. Let $c_{14} > \sqrt{n}(2/V(K_0))^{1/n}$. If Q_k is an output from Algorithm NoisyCovDiff(φ) as stated above, then, almost surely,

$$\delta(DK_0, Q_k) \leq c_{14}\delta_k^{1/n}, \tag{72}$$

for sufficiently large k. In particular, almost surely, Q_k converges to DK_0, as $k \to \infty$.

Proof. Due to (71), there is an integer $N_3 = N_3(\varphi, \sigma^2, (\varepsilon_k), (\delta_k))$ such that

$$c_{12}(\delta_k (k\varepsilon_k)^{n/2})^{-1} \leq 1 \tag{73}$$

for all $k \geq N_3$. Let

$$a_k = \max_{x \in 2C_0^n \cap (1/k)\mathbb{Z}^n} |g_k(x) - g_{K_0}(x)|.$$

By Lemma 5.4, (73), and (71), we have

$$\begin{aligned} \Pr(a_k \geq \delta_k) &\leq \sum_{x \in 2C_0^n \cap (1/k)\mathbb{Z}^n} \Pr(|g_k(x) - g_{K_0}(x)| \geq \delta_k) \\ &\leq (2k+1)^n \exp(-c_{13}\delta_k^2 (k\varepsilon_k)^n) < \frac{3}{k^2}, \end{aligned}$$

for all $k \geq \max\{N_2, N_3\}$. Therefore, by the Borel-Cantelli lemma, we see that, almost surely, $a_k < \delta_k$ for sufficiently large k. Fix a realization and a $k \in \mathbb{N}$ such that $a_k < \delta_k$ and

$$\left(\frac{2\delta_k}{V(K_0)}\right)^{1/n} + \frac{3}{s(K_0)k} \leq 1, \tag{74}$$

where $s(K_0) = \max\{\rho \geq 0 : \rho C_0^n \subset DK_0\}$. As $a_k < \delta_k$, the definition (67) of S_k implies

$$K_0(2\delta_k) \cap \frac{1}{k}\mathbb{Z}^n \subset S_k \subset DK_0.$$

The set on the left is o-symmetric, and DK_0 is convex and o-symmetric, so

$$\mathrm{conv}\left(K_0(2\delta_k) \cap \frac{1}{k}\mathbb{Z}^n\right) \subset Q_k \subset DK_0. \tag{75}$$

We claim that

$$K_0(2\delta_k) \ominus \frac{3}{k} C_0^n \subset \operatorname{conv}\left(K_0(2\delta_k) \cap \frac{1}{k}\mathbb{Z}^n\right), \tag{76}$$

where Minkowski difference $\ominus$ is defined by (2). Indeed, let $x \in K_0(2\delta_k) \ominus (3/k)C_0^n$. As $\{y + (1/k)C_0^n : y \in (1/k)\mathbb{Z}^n\}$ is a covering of $\mathbb{R}^n$, there is a $y \in (1/k)\mathbb{Z}^n$ with $x \in (1/k)C_0^n + y$ and hence $y \in (1/k)C_0^n + x$. It follows that

$$x \in \frac{1}{k}(2C_0^n) + y \subset \frac{3}{k} C_0^n + x \subset K_0(2\delta_k).$$

As the vertices of $(1/k)(2C_0^n) + y$ are in $(1/k)\mathbb{Z}^n$, we have $x \in \operatorname{conv}(K_0(2\delta_k) \cap (1/k)\mathbb{Z}^n)$, proving the claim.

Let $t_k = (2\delta_k / V(K_0))^{1/n}$. The fact that DK_0 is convex and contains the origin, (74), Lemma 5.5 (with $\delta = 2\delta_k$), and the definition of $s(K_0)$ imply that

$$\left(1 - \left(t_k + \frac{3}{s(K_0)k}\right)\right) DK_0 = (1 - t_k)\, DK_0 \ominus \left(\frac{3}{s(K_0)k} DK_0\right) \subset K_0(2\delta_k) \ominus \frac{3}{k} C_0^n.$$

From this, (76), and (75), we obtain

$$\left(1 - \left(t_k + \frac{3}{s(K_0)k}\right)\right) DK_0 \subset Q_k \subset DK_0.$$

As $DK_0 \subset \sqrt{n} B^n$, this yields

$$\delta(DK_0, Q_k) \le \sqrt{n}\left(t_k + \frac{3}{s(K_0)k}\right) = \left(\sqrt{n}\left(\frac{2}{V(K_0)}\right)^{1/n} + \frac{3\sqrt{n}}{s(K_0)k\delta_k^{1/n}}\right)\delta_k^{1/n}.$$

By (71), $k\delta_k^{1/n} \to \infty$ as $k \to \infty$, and (72) follows. □

The estimate (72) reveals that the rate of convergence of Q_k to DK_0 depends on the asymptotic behavior of the threshold parameter δ_k, which is linked to the bandwidth ε_k by (71). If we assume that $V(K_0)$ is bounded from below by a known constant, then c_{14} in the statement of Theorem 5.6 can be chosen independent of K_0. We note the resulting rate of convergence as a corollary, where we choose ε_k and $\delta_k / \log k$ as appropriate powers of k. In particular, it shows that a convergence rate of k^{-p} can be attained, where p is arbitrarily close to 1/2.

Corollary 5.7. *Suppose that K_0, δ_k, ε_k, and g_k are as in Algorithm NoisyCovDiff(φ). Let $0 < b < V(K_0)$, let $\delta_k = k^{-n(1-\alpha)/2}\log k$, and let $\varepsilon_k = k^{-\alpha}$, for some $0 < \alpha < 1$. If Q_k is an output from Algorithm NoisyCovDiff(φ) as stated above, then, almost surely,*

$$\delta(Q_k, DK_0) \le \sqrt{n}\left(\frac{2}{b}\right)^{1/n} k^{-(1-\alpha)/2}(\log k)^{1/n},$$

for sufficiently large k.

6. PHASE RETRIEVAL: FRAMEWORK AND TECHNICAL LEMMAS

In this section we set the scene for our results on phase retrieval, beginning with the necessary material from Fourier analysis.

Let g be a continuous function on $\mathbb{R}^n$ whose support is contained in $[-1,1]^n$ and let $L \geq 1$. By the classical theory, the Fourier series of g is

$$\sum_{z\in\mathbb{Z}^n} c_z e^{i\pi z\cdot x/L},$$

for $x \in [-L,L]^n$, where

$$c_z = \frac{1}{(2L)^n}\int_{[-L,L]^n} g(t)e^{-i\pi z\cdot t/L}\,dt = \frac{1}{(2L)^n}\int_{\mathbb{R}^n} g(t)e^{-i\pi z\cdot t/L}\,dt = \frac{1}{(2L)^n}\widehat{g}(\pi z/L).$$

Let

$$\mathbb{Z}^n_k = \{z \in \mathbb{Z}^n : z = (z_1,\dots,z_n), |z_j| \leq k, j = 1,\dots,k\}.$$

If g is also Lipschitz, then by [33, Theorem 3], the square partial sums $\sum_{z\in\mathbb{Z}^n_k} c_z e^{i\pi z\cdot x/L}$ of the Fourier series of g converge uniformly to g. Therefore, if g is also an even function, we can write

$$g(x) = \frac{1}{(2L)^n}\sum_{z\in\mathbb{Z}^n}\widehat{g}(\pi z/L)e^{i\pi z\cdot x/L} = \frac{1}{(2L)^n}\sum_{z\in\mathbb{Z}^n}\widehat{g}(\pi z/L)\cos\frac{\pi z\cdot x}{L}, \tag{77}$$

for all $x \in [-L,L]^n$, where equality is in the sense of uniform convergence of square partial sums.

Let $\mathbb{Z}^n_k(+)$ be a subset of $\mathbb{Z}^n_k$ such that

$$\mathbb{Z}^n_k(+) \cap (-\mathbb{Z}^n_k(+)) = \emptyset \quad\text{and}\quad \mathbb{Z}^n_k = \{o\} \cup \mathbb{Z}^n_k(+) \cup (-\mathbb{Z}^n_k(+)). \tag{78}$$

Suppose that g is even and for some fixed $0 < \gamma < 1$ and each $k \in \mathbb{N}$, we can obtain noisy measurements

$$\widetilde{g}_{z,k} = \widehat{g}(z/k^\gamma) + X_{z,k}, \tag{79}$$

of $\widehat{g}$, for $z \in \{o\}\cup\mathbb{Z}^n_k(+)$, where the $X_{z,k}$'s are independent $N(0,\sigma^2)$ random variables. Define $X_{z,k} = X_{-z,k}$, for $z \in (-\mathbb{Z}^n_k(+))$ and note that then $X_{z,k} = X_{-z,k}$ for all $z \in \mathbb{Z}^n_k$. Since g is even, $\widehat{g}$ is also even, and we have $\widetilde{g}_{z,k} = \widetilde{g}_{-z,k}$ for $z \in \mathbb{Z}^n_k$. Using these facts, (77) with $L = \pi k^\gamma$, and (79), we obtain

$$g(x) = \frac{1}{(2\pi k^\gamma)^n}\left(\sum_{z\in\mathbb{Z}^n_k}\widetilde{g}_{z,k}\cos\frac{z\cdot x}{k^\gamma} - \sum_{z\in\mathbb{Z}^n_k} X_{z,k}\cos\frac{z\cdot x}{k^\gamma} + \sum_{z\in\mathbb{Z}^n\setminus\mathbb{Z}^n_k}\widehat{g}(z/k^\gamma)\cos\frac{z\cdot x}{k^\gamma}\right), \tag{80}$$

for all $x \in [-\pi k^\gamma, \pi k^\gamma]^n$. Here the first term is an estimate of $g(x)$, the second term a random error, and the third term a deterministic error.

Since it has all the required properties, we can apply the previous equation to the covariogram $g = g_{K_0}$ of a convex body K_0 contained in C^n_0, in which case $\widehat{g_{K_0}} = |\widehat{1_{K_0}}|^2$. In order to move closer to the notation used earlier, we now use i as an index and again list the points in $[-1,1]^n \cap (1/k)\mathbb{Z}^n = (1/k)\mathbb{Z}_k^n$, but this time a little differently. We let $x_{0k} = o$, list the points in $(1/k)\mathbb{Z}_k^n(+)$ as x_{ik}, $i = 1, \dots, I'_k = ((2k+1)^n - 1)/2$, and then let $x_{ik} = -x_{(-i)k}$ for $i = -I'_k, \dots, -1$. Now let $z_{ik} = k^{1-\gamma} x_{ik}$, so that

$$(1/k^\gamma)\mathbb{Z}_k^n = \{z_{ik} : i = -I'_k, \dots, I'_k\}.$$

Setting $\widetilde{g}_{jk} = \widetilde{g_{K_0}}_{z_{jk},k}$ and $X_{jk} = X_{z_{jk},k}$, we use (79) to rewrite (80) as

$$M_k(x) = g_{K_0}(x) + N_k(x) - d_k(x), \tag{81}$$

where

$$M_k(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x)\widetilde{g}_{jk} \tag{82}$$

is an estimate of g_{K_0},

$$N_k(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x) X_{jk} \tag{83}$$

is a random variable, and

$$d_k(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{z \in \mathbb{Z}^n \setminus \mathbb{Z}_k^n} \cos\left(\frac{z \cdot x}{k^\gamma}\right) \widehat{g_{K_0}}(z/k^\gamma) \tag{84}$$

is a deterministic error.

We shall need three technical lemmas. The first of these provides a control on the deterministic error.

Lemma 6.1. *Let* $d_k = \sup\{|d_k(x)| : x \in \mathbb{R}^n\}$. *Then* $d_k = O(k^{\gamma-1}(\log k)^n)$ *as* $k \to \infty$.

Proof. From (84), the fact that $\widehat{g_{K_0}} = |\widehat{1_{K_0}}|^2$ is nonnegative, and (77) with $g = g_{K_0}$ and $L = \pi k^\gamma$, we have

$$d_k \le \frac{1}{(2\pi k^\gamma)^n} \sum_{z \in \mathbb{Z}^n \setminus \mathbb{Z}_k^n} \widehat{g_{K_0}}(z/k^\gamma) = g_{K_0}(0) - \frac{1}{(2\pi k^\gamma)^n} \sum_{z \in \mathbb{Z}_k^n} \widehat{g_{K_0}}(z/k^\gamma). \tag{85}$$

For $t \in \mathbb{R}$, let

$$D_k(t) = \sum_{l=-k}^{k} e^{ilt} = \frac{\sin((k+1/2)t)}{\sin(t/2)}$$

be the Dirichlet kernel. Note that for $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, we have

$$\sum_{z \in \mathbb{Z}_k^n} e^{iz \cdot x} = \prod_{l=1}^{n} \left(\sum_{l=-k}^{k} e^{ilx_l}\right) = \prod_{l=1}^{n} D_k(x_l).$$

Using this and the fact that g_{K_0} is even, with support in $[-1,1]^n$, we obtain

$$\begin{aligned}\frac{1}{(2\pi k^\gamma)^n}\sum_{z\in\mathbb{Z}_k^n}\widehat{g_{K_0}}(z/k^\gamma) &= \frac{1}{(2\pi k^\gamma)^n}\sum_{z\in\mathbb{Z}_k^n}\int_{[-\pi k^\gamma,\pi k^\gamma]^n} g_{K_0}(x)e^{-iz\cdot x/k^\gamma}\,dx\\ &= \frac{1}{(2\pi k^\gamma)^n}\int_{[-\pi k^\gamma,\pi k^\gamma]^n} g_{K_0}(x)\prod_{l=1}^n D_k(-x_l/k^\gamma)\,dx\\ &= \frac{1}{(2\pi)^n}\int_{[-1,1]^n} g_{K_0}(yk^\gamma)\prod_{l=1}^n D_k(y_l)\,dy. \end{aligned}\tag{86}$$

Since $\int_{-\pi}^{\pi} D_k(t)\,dt = 2\pi$, we have

$$g_{K_0}(0) = \frac{1}{(2\pi)^n}\int_{[-\pi,\pi]^n} g_{K_0}(0)\prod_{l=1}^n D_k(y_l)\,dy.\tag{87}$$

Thus, by (85), (86), and (87),

$$\begin{aligned} d_k &\le \left|\frac{1}{(2\pi)^n}\int_{[-1,1]^n}(g_{K_0}(0)-g_{K_0}(yk^\gamma))\prod_{l=1}^n D_k(y_l)\,dy\right| +\\ &+ g_{K_0}(0)\left|\frac{1}{(2\pi)^n}\int_{[-\pi,\pi]^n\setminus[-1,1]^n}\prod_{l=1}^n D_k(y_l)\,dy\right|. \end{aligned}\tag{88}$$

By Proposition 5.1, g_{K_0} is Lipschitz and hence the Lipschitz norm of $g_{K_0}(yk^\gamma)$ is $O(k^\gamma)$. Now [33, Theorem 1] implies that

$$\left|\frac{1}{(2\pi)^n}\int_{[-1,1]^n}(g_{K_0}(0)-g_{K_0}(yk^\gamma))\prod_{l=1}^n D_k(y_l)\,dy\right| \le c_{15}k^{\gamma-1}\sum_{l=0}^{n-1}(\log k)^{n-l},\tag{89}$$

for some constant c_{15} independent of k. (In the statement of [33, Theorem 1], $D_j(Y)$ should be $D_J(Y)$. In that theorem we are taking $\alpha = 1$ and $J = (k,k,\dots,k)\in\mathbb{Z}^n$.)

In view of (88) and (89), the proof will be complete if we show that

$$\int_{[-\pi,\pi]^n\setminus[-1,1]^n}\prod_{l=1}^n D_k(x_l)dx = O(1/k),\tag{90}$$

as $k\to\infty$. To this end, observe that, by trigonometric addition formulas and integration by parts,

$$\begin{aligned}\int_{-\pi}^{-1} D_k(t)\,dt = \int_1^\pi D_k(t)\,dt &= \int_1^\pi \frac{\sin(kt)\cos(t/2)}{\sin(t/2)}\,dt + \int_1^\pi \cos(kt)\,dt\\ &= \frac{\cos k\cot(1/2)}{k} + \int_1^\pi \frac{\cos(kt)}{k}\frac{d}{dt}\left(\cot(t/2)\right)\,dt - \frac{\sin k}{k}\\ &= O(1/k). \end{aligned}\tag{91}$$

Now

$$[-\pi,\pi]^n \setminus [-1,1]^n = \cup_{i=1}^n (A_i \cup B_i),$$

where

$$A_i = \{(x_1,\dots,x_n)\ : -1 \le x_j \le 1 \text{ for } j<i\ , 1 \le x_i \le \pi, -\pi \le x_j \le \pi \text{ for } j>i\}$$

and $B_i = -A_i$. By (91), we have, for each i,

$$\begin{aligned}\int_{A_i} \prod_{l=1}^n D_k(x_l)dx &= \left(\int_{-1}^1 D_k(t)dt\right)^{i-1} \int_1^\pi D_k(t)dt \left(\int_{-\pi}^{\pi} D_k(t)dt\right)^{n-i}\\ &= (2\pi - O(1/k))^{i-1}\ O(1/k)\ (2\pi)^{n-i}.\end{aligned}$$

Since $\operatorname{int}(A_i) \cap \operatorname{int}(A_j) = \emptyset$, for each i,j with $i \ne j$, $\operatorname{int}(A_i) \cap \operatorname{int}(B_j) = \emptyset$, for each i,j, and $\prod_{l=1}^n D_k(x_l)$ is even, the previous estimate proves (90). □

It is possible that the previous lemma could also be obtained via some estimates proved in [13] for the rate of decay of $\int_{S^{n-1}} |\widehat{1_{K_0}}(ru)|^2\, du$ as $r \to \infty$.

The next two lemmas will allow us to circumvent Proposition 3.7, the version of the Strong Law of Large Numbers used earlier.

Lemma 6.2. *Let Y_{jk}, $j = 1,\dots,m_k$, $k \in \mathbb{N}$ be a triangular array of independent $N(0,\sigma^2)$ random variables, where $m_k \sim k^n$ as $k \to \infty$. Let ν and a_{pqk}, $p,q = 1,\dots,m_k$ be constants such that $|a_{pqk}| = O(k^\nu)$ as $k \to \infty$ uniformly in p and q, where $2n - 4n\gamma + 2\nu < -1$. Then, almost surely,*

$$Z_k = \frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p,q=1}^{m_k} a_{pqk} Y_{pk} Y_{qk} \to 0,$$

as $k \to \infty$.

Proof. Note that $E(Y_{pk}Y_{qk}) = E(Y_{pk})E(Y_{qk}) = 0$ unless $p = q$. Therefore

$$E(Z_k) = \frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p,q=1}^{m_k} a_{pqk} E(Y_{pk}Y_{qk}) = \frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p=1}^{m_k} a_{ppk} E(Y_{pk}^2) = \frac{E(Y_{11}^2)}{(2\pi k^\gamma)^{2n}} \sum_{p=1}^{m_k} a_{ppk},$$

so $|E(Z_k)| = O(k^{n-2n\gamma+\nu})$ and hence $E(Z_k)$ converges to zero as $k \to \infty$.

Let

$$v_{pqrs} = \operatorname{cov}(Y_{pk}Y_{qk}, Y_{rk}Y_{sk}) = E(Y_{pk}Y_{qk}Y_{rk}Y_{sk}) - E(Y_{pk}Y_{qk})E(Y_{rk}Y_{sk}).$$

If the cardinality of the set $\{p,q,r,s\}$ is 3 or 4, then at least one of the indices, say p, is different from all the others and

$$v_{pqrs} = E(Y_{pk})E(Y_{qk}Y_{rk}Y_{sk}) - E(Y_{pk})E(Y_{qk})E(Y_{rk}Y_{sk}) = 0 - 0 = 0.$$

If the cardinality of the set $\{p,q,r,s\}$ is 1, then

$$v_{pqrs} = v_{pppp} = E(Y_{pk}^4) - E(Y_{pk}^2)^2 = \operatorname{var}(Y_{11}^2).$$

If the cardinality of the set $\{p,q,r,s\}$ is 2, then either $p = q$, $r = s$ and $p \ne r$, and

$$v_{pqrs} = v_{pprr} = E(Y_{pk}^2 Y_{rk}^2) - E(Y_{pk}^2)E(Y_{rk}^2) = 0,$$

or $p=r$, $q=s$ and $p\neq q$, and

$$v_{pqrs}=v_{pqpq}=E(Y_{pk}^2Y_{qk}^2)-E(Y_{pk}Y_{qk})^2=E(Y_{11}^2)^2=\mathrm{var}\,(Y_{11})^2,$$

or $p=s$, $q=r$ and $p\neq q$, and

$$v_{pqrs}=v_{pqqp}=E(Y_{pk}^2Y_{qk}^2)-E(Y_{pk}Y_{qk})^2=E(Y_{11}^2)^2=\mathrm{var}\,(Y_{11})^2.$$

Thus

$$\begin{aligned}\mathrm{var}\,(Z_k)&=\frac{1}{(2\pi k^\gamma)^{4n}}\sum_{p,q,r,s=1}^{m_k}a_{pqk}a_{rsk}v_{pqrs}\\&=\frac{\mathrm{var}\,(Y_{11}^2)}{(2\pi k^\gamma)^{4n}}\sum_{p=1}^{m_k}a_{ppk}^2+\frac{\mathrm{var}\,(Y_{11})^2}{(2\pi k^\gamma)^{4n}}\left(\sum_{p\neq q=1}^{m_k}a_{pqk}^2+\sum_{p\neq q=1}^{m_k}a_{pqk}a_{qpk}\right)\\&=O\left(k^{2n-4n\gamma+2\nu}\right).\end{aligned}$$

Let $\varepsilon>0$. For sufficiently large k, we have $\varepsilon-E(Z_k)>0$, and for such k, by Chebyshev's inequality,

$$\Pr(Z_k>\varepsilon)=\Pr\bigl(Z_k-E(Z_k)>\varepsilon-E(Z_k)\bigr)\leq\frac{\mathrm{var}\,(Z_k)}{(\varepsilon-E(Z_k))^2}=O\left(k^{2n-4n\gamma+2\nu}\right).$$

Our hypothesis and the Borel-Cantelli Lemma imply that, almost surely, Z_k converges to zero, as $k\to\infty$. $\square$

Lemma 6.3. *Let $Y_{jk}^{(r)}$, $j=1,\dots,m_k$, $k\in\mathbb{N}$, $r=1,2$ be independent $N(0,\sigma^2)$ random variables, where $m_k\sim k^n$ as $k\to\infty$. Let ν and a_{pqk}, $p,q=1,\dots,m_k$ be constants such that $|a_{pqk}|=O(k^\nu)$ as $k\to\infty$ uniformly in p and q, where $2n-4n\gamma+2\nu<-1$. Then, almost surely,*

$$\overline{Z}_k=\frac{1}{(2\pi k^\gamma)^{2n}}\sum_{p,q=1}^{m_k}a_{pqk}Y_{pk}^{(1)}Y_{pk}^{(2)}Y_{qk}^{(1)}Y_{qk}^{(2)}\to0,$$

as $k\to\infty$.

Proof. Straightforward modifications to the proof of Lemma 6.2 show that

$$E(\overline{Z}_k)=\frac{E\left(\left(Y_{11}^{(1)}\right)^2\right)^2}{(2\pi k^\gamma)^{2n}}\sum_{p=1}^{m_k}a_{ppk},$$

so $|E(\overline{Z}_k)|=O(k^{n-2n\gamma+\nu})$ and hence $E(\overline{Z}_k)$ converges to zero as $k\to\infty$. We also obtain

$$\begin{aligned}\mathrm{var}\,(\overline{Z}_k)&=\frac{E\left(\left(Y_{11}^{(1)}\right)^4\right)^2-E\left(\left(Y_{11}^{(1)}\right)^2\right)^4}{(2\pi k^\gamma)^{4n}}\sum_{p=1}^{m_k}a_{ppk}^2+\frac{\mathrm{var}\,\left(Y_{11}^{(1)}\right)^4}{(2\pi k^\gamma)^{4n}}\left(\sum_{p\neq q=1}^{m_k}a_{pqk}^2+\sum_{p\neq q=1}^{m_k}a_{pqk}a_{qpk}\right)\\&=O\left(k^{2n-4n\gamma+2\nu}\right).\end{aligned}$$

The proof is concluded as in Lemma 6.2. □

7. Phase retrieval from the squared modulus

This section addresses Problem 2 in the introduction.

Algorithm NoisyMod^{2}LSQ

Input: Natural numbers $n \geq 2$ and k; a real number γ such that $0 < \gamma < 1$; noisy measurements

$$\widetilde{g}_{ik} = |\widehat{1_{K_0}}(z_{ik})|^2 + X_{ik}, \tag{92}$$

of the squared modulus of the Fourier transform of the characteristic function of an unknown convex body $K_0 \subset C_0^n$ whose centroid is at the origin, at the points in

$$\{z_{ik} : i = 0, 1, \dots, I'_k\} = \{o\} \cup (1/k^\gamma)\mathbb{Z}_k^n(+),$$

where $\mathbb{Z}_k^n(+)$ satisfies (78) and where the X_{ik}'s are independent normal $N(0, \sigma^2)$ random variables; an o-symmetric convex polytope Q_k in $\mathbb{R}^n$, stochastically independent of the measurements $\widetilde{g}_{ik}$, that approximates either ∇K_0 or DK, in the sense that, almost surely,

$$\lim_{k\to\infty} \delta(Q_k, \nabla K_0) = 0, \qquad \text{or} \qquad \lim_{k\to\infty} \delta(Q_k, DK_0) = 0. \tag{93}$$

Task: Construct a convex polytope P_k that approximates K_0, up to reflection in the origin.

Action:

1. Let $\widetilde{g}_{ik} = \widetilde{g}_{(-i)k}$, for $i = -I'_k, \dots, -1$, let $x_{ik} = k^{\gamma-1}z_{ik}$, $i = -I'_k, \dots, I'_k$ be the points in the cubic array $2C_0^n \cap (1/k)\mathbb{Z}^n$, and let

$$M_k(x_{ik}) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x_{ik})\widetilde{g}_{jk}, \tag{94}$$

for $i = -I'_k, \dots, I'_k$.

2. Run Algorithm NoisyCovLSQ with inputs n, k, Q_k, and with M_{ik} replaced by $M_k(x_{ik})$, for $i = -I'_k, \dots, I'_k$ and with the obvious re-indexing in i. The resulting output P_k of that algorithm is also the output of the present one.

The main result in this section corresponds to Theorem 3.10 above. We first state it, and then show that it can be proved by suitable modifications to the proof of Theorem 3.10 if in addition $\gamma > 1/2 + 1/(4n)$.

Theorem 7.1. *Suppose that $K_0 \subset C_0^n$ is a convex body with its centroid at the origin. Suppose also that K_0 is determined, up to translation and reflection in the origin, among all convex bodies in $\mathbb{R}^n$, by its covariogram. Let*

$$1/2 + 1/(4n) < \gamma < 1. \tag{95}$$

If P_k, $k \in \mathbb{N}$, *is an output from Algorithm NoisyMod*^{2}*LSQ as stated above, then, almost surely,*

$$\min\{\delta(K_0, P_k), \delta(-K_0, P_k)\} \to 0 \tag{96}$$

as $k \to \infty$.

As we shall now show, the proof of this theorem basically follows the analysis given in Section 3. Of course, alterations must be made, since the measurements M_{ik} in Algorithm NoisyCovLSQ have been replaced by the new measurements $M_k(x_{ik})$ defined by (94) or equivalently by (82) with $x = x_{ik}$. In view of (81), we have

$$M_k(x_{ik}) = g_{K_0}(x_{ik}) + N_k(x_{ik}) - d_k(x_{ik}),$$

$i = -I'_k, \dots, I'_k$, where $N_k(x_{ik})$ and $d_k(x_{ik})$ are given by (83) and (84), respectively, with $x = x_{ik}$.

We begin with a lemma. Note that $I_k = 2I'_k + 1$, so the expression in the lemma is the sample mean. Also, recall that by their definition, the random variables X_{pk} and X_{ql} are $N(0, \sigma^2)$ and independent unless $k = l$ and $p = \pm q$, in which case they are equal.

Lemma 7.2. *Let* $N_k(x_{ik})^+ = \max\{N_k(x_{ik}), 0\}$ *for all* i *and* k. *If (95) holds, then, almost surely,*

$$\frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} N_k(x_{ik})^+ \to 0,$$

as $k \to \infty$.

Proof. Note firstly that

$$\frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} N_k(x_{ik})^+ \le \frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} |N_k(x_{ik})| \le \left(\frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} N_k(x_{ik})^2 \right)^{1/2}.$$

Thus it suffices to prove that, almost surely,

$$S_k = \frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} N_k(x_{ik})^2 \to 0,$$

as $k \to \infty$.

We have

$$\begin{aligned} S_k &= \frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\left(\frac{1}{(2\pi k^{\gamma})^n}\sum_{p=-I'_k}^{I'_k}\cos(z_{pk}\cdot x_{ik})X_{pk}\right)^2 \\ &= \frac{1}{(2\pi k^{\gamma})^{2n}}\sum_{p,q=-I'_k}^{I'_k}\left(\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\cos(z_{pk}\cdot x_{ik})\cos(z_{qk}\cdot x_{ik})\right)X_{pk}X_{qk} \\ &= \frac{1}{(2\pi k^{\gamma})^{2n}}\sum_{p,q=-I'_k}^{I'_k}c_{pqk}X_{pk}X_{qk}, \end{aligned}$$

say. Since $c_{(-p)qk} = c_{p(-q)k} = c_{pqk}$, it is clearly enough to show that, almost surely,

$$\frac{1}{(2\pi k^{\gamma})^{2n}}\sum_{p,q=1}^{I'_k}c_{pqk}X_{pk}X_{qk} \to 0,$$

as $k\to\infty$. In view of (95) and the fact that $|c_{pqk}| = O(1)$, this follows from Lemma 6.2 with $Y_{jk} = X_{jk}$, $m_k = I'_k$, $a_{pqk} = c_{pqk}$ for all p, q, and k, and $\nu = 0$. □

Proof of Theorem 7.1. We shall indicate the modifications needed in Section 3. No changes are required in the lemmas before Lemma 3.4. For the latter, we shall use the same notation as before, with the understanding that the indexing has changed and the new random variables $N_k(x_{ik})$ replace the random variables N_{ik} of Section 3. Thus we write

$$|f|_{I_k} = \left(\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}f(z_i)^2\right)^{1/2},$$

with corresponding changes in indexing in the definitions of $\mathbf{x}_{I_k}$, $\mathbf{N}_{I_k}$, and Ψ. With the same proof as Lemma 3.4, we now have the inequality

$$\begin{aligned} |g_{K_0}-g_{P_k}|^2_{I_k} \;&\le\; 2\Psi(P_k,\mathbf{x}_{I_k},\mathbf{N}_{I_k}) - 2\Psi(P(a)\cap C_0^n,\mathbf{x}_{I_k},\mathbf{N}_{I_k}) + \left|g_{K_0}-g_{P(a)\cap C_0^n}\right|^2_{I_k} + \\ &\quad + \frac{2}{I_k}\sum_{i=-I'_k}^{I'_k}\left(g_{P(a)\cap C_0^n}(x_{ik}) - g_{P_k}(x_{ik})\right)d_k(x_{ik}), \end{aligned} \tag{97}$$

instead of (35).

Proposition 3.5 and Lemma 3.6 are unchanged. We do not require Proposition 3.7 in order to conclude as in Lemma 3.8 that, almost surely,

$$\sup_{K\in\mathcal{K}^n(C_0^n)}\Psi(K,\mathbf{x}_{I_k},\mathbf{N}_{I_k}) \to 0, \tag{98}$$

as $k \to \infty$. Indeed, it is enough to show that, almost surely, the new expression corresponding to (39), namely,

$$W_k(\varepsilon) = \max_{j=1,\dots,m} \left\{ \frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} g_j^U(x_{ik}) N_k(x_{ik})^+ - \frac{1}{I_k} \sum_{i=-I'_k}^{I'_k} g_j^L(x_{ik}) N_k(x_{ik})^- \right\},$$

converges to zero, as $k \to \infty$. This follows from Lemma 7.2, because the coefficients $g_j^U(x_{ik})$ and $g_j^U(x_{ik})$ are uniformly bounded by 1 and Lemma 7.2 holds both when such coefficients are inserted and when $N_k(x_{ik})^+$ is replaced by $N_k(x_{ik})^- = N_k(x_{ik}) - N_k(x_{ik})^+ = \max\{-N_k(x_{ik}), 0\}$.

All this is enough to ensure that Lemma 3.9 still holds. Indeed, since a translate of P_k is contained in C_0^n, and $\Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k})$ is unchanged by such a translation, we know from (98) that, almost surely, the first and second terms on the right-hand side of (97) converge to zero, as $k \to \infty$. We have $g_{P(a)\cap C_0^n}(x_{ik}) \le 1$ and $g_{P_k}(x_{ik}) \le V(2C_0^n)$, since $P_k \subset 2C_0^n$, and then Lemma 6.1 implies that the new fourth term on the right-hand side of (97) converges to zero as $k \to \infty$. The rest of the proof of Lemma 3.9 proceeds as before.

The proof of the main Theorem 3.10 now applies without change. □

The user of Algorithm NoisyMod²LSQ must supply as input an o-symmetric convex polytope Q_k in $\mathbb{R}^n$ that approximates either ∇K_0 or DK. For this purpose we provide two algorithms that do the work of Algorithm NoisyCovBlaschke and Algorithm NoisyCovDiff(φ).

Algorithm NoisyMod²Blaschke

Input: Natural numbers $n \ge 2$ and k; a positive real number h_k; mutually nonparallel vectors $u_i \in S^{n-1}$, $i = 1, \dots, k$ that span $\mathbb{R}^n$; noisy measurements

$$\widetilde{g}_{ik} = |\widehat{1_{K_0}}(z_{ik})|^2 + X_{ik}, \tag{99}$$

of the squared modulus of the Fourier transform of the characteristic function of an unknown convex body $K_0 \subset C_0^n$ whose centroid is at the origin, at the points in

$$\{z_{ik} : i = 0, 1, \dots, I'_k\} = \{o\} \cup (1/k^\gamma)\mathbb{Z}_k^n(+),$$

where $\mathbb{Z}_k^n(+)$ satisfies (78) and where the X_{ik}'s are independent normal $N(0, \sigma^2)$ random variables.

Task: Construct an o-symmetric convex polytope Q_k that approximates the Blaschke body ∇K_0.

Action:

1. Let $\widetilde{g}_{ik} = \widetilde{g}_{(-i)k}$, for $i = -I'_k, \dots, -1$, and let

$$M_k(o) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \widetilde{g}_{jk} \quad \text{and} \quad M_k(h_k u_i) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot h_k u_i) \widetilde{g}_{jk}, \tag{100}$$

for $i = 1, \dots, k$. Then for $i = 1, \dots, k$, let

$$y_{ik} = \frac{M_k(o) - M_k(h_k u_i)}{h_k}. \tag{101}$$

2. With the natural numbers $n \geq 2$ and k, and vectors $u_i \in S^{n-1}$, $i = 1, \dots, k$ use the quantities y_{ik} instead of noisy measurements of the brightness function $b_K(u_i)$ as input to Algorithm NoisyBrightLSQ (see [24, p. 1352]). The output of the latter algorithm is Q_k.

We shall show that the argument of Section 4 can be modified to yield a convergence result corresponding to Theorem 4.5. It is clear that any such result must require the input h_k to satisfy $h_k \to 0$ as $k \to \infty$, but we need a stronger condition phrased in terms of parameters ε and γ that satisfy (102). Since the second inequality in (102) is equivalent to $\gamma > (2n + 5 - 4\varepsilon)/(4n + 4)$, which decreases as n increases and equals $(9 - 4\varepsilon)/12$ when $n = 2$, it is possible to choose γ and ε so that (102) is satisfied. Specifically, one can choose $3/4 \leq \gamma < 1$ and $0 < \varepsilon < 1 - \gamma$. Note also that (102) implies (95).

There is considerable flexibility in the choice of the parameter h_k, and it would be possible to introduce a further parameter q_k by working with input vectors $u_i \in S^{n-1}$, $i = 1, \dots, q_k$, where $q_k \to \infty$ as $k \to \infty$. To avoid overcomplicating the exposition, however, we shall not discuss this any further.

Theorem 7.3. *Let $K_0 \subset C_0^n$ be a convex body with its centroid at the origin. Let (u_i) be a sequence in S^{n-1} such that (u_i^*) is evenly spread. Suppose that $h_k \sim k^{\gamma-1+\varepsilon}$, $k \in \mathbb{N}$, where ε and γ satisfy*

$$0 < \varepsilon < 1 - \gamma \quad \text{and} \quad 2n - 4n\gamma + 4(1 - \gamma - \varepsilon) < -1. \tag{102}$$

If Q_k is an output from Algorithm NoisyMod^{2}Blaschke as stated above, then, almost surely,

$$\lim_{k\to\infty} \delta(\nabla K_0, Q_k) = 0. \tag{103}$$

Proof. We shall indicate the changes needed in Section 4. Note that by (101), and (81) with $x = o$ and $x = h_k u_i$, we have

$$y_{ik} = \frac{M_k(o) - M_k(h_k u_i)}{h_k} = \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} + \frac{N_k(o) - N_k(h_k u_i)}{h_k} - \frac{d_k(o) - d_k(h_k u_i)}{h_k}, \tag{104}$$

for $i = 1, \dots, k$, where $N_k(o)$, $d_k(o)$, $N_k(h_k u_i)$, and $d_k(h_k u_i)$ are given by (83) and (84) with $x = o$ or $x = h_k u_i$, as appropriate.

Lemma 4.1 is unchanged. Turning to the proof of Lemma 4.2, we now have

$$y_{ik} = \zeta_{ik} + T_{ik},$$

where

$$\zeta_{ik} = \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} - \frac{d_k(o) - d_k(h_k u_i)}{h_k} \quad \text{and} \quad T_{ik} = \frac{N_k(o) - N_k(h_k u_i)}{h_k}, \tag{105}$$

for $i = 1, \dots, k$. Since $h_k \sim k^{\gamma-1+\varepsilon}$ for $0 < \varepsilon < 1-\gamma$, the second term in the previous expression for ζ_{ik} converges to zero as $k \to \infty$, by Lemma 6.1, and hence $\zeta_{ik} \to b_{K_0}(u_i)$ as $k \to \infty$, as before, for $i = 1, \dots, k$. Moreover,

$$b_{K_0}(u_i) - \zeta_{ik} = \left(b_{K_0}(u_i) - \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} \right) + \frac{d_k(o) - d_k(h_k u_i)}{h_k},$$

so arguing as in the proof of Lemma 4.2, we use Lemma 4.1 with $t = h_k$ to obtain (50) with $t = h_k$, that is,

$$0 \le b_{K_0}(u_i) - \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} \le \frac{(n-1)h_k}{2r} b_{K_0}(u_i),$$

if $h_k \le 2r$. We also have

$$\frac{d_k(o) - d_k(h_k u_i)}{h_k} = O(k^{-\varepsilon}),$$

by Lemma 6.1, so there is a constant $c_{16} = c_{16}(n, r)$ such that

$$|b_{K_0}(u_i) - \zeta_{ik}| \le c_{16} k^{-\beta},$$

for $\beta = \min\{\varepsilon, 1-\gamma+\varepsilon\}$, and all $k \in \mathbb{N}$ and $i = 1, \dots, k$. The rest of the proof of Lemma 4.2 can be followed, yielding that, almost surely, there is a constant $c_{17} = c_{17}(n, r)$ such that

$$|b_{K_0} - b_{Q_k}|_k^2 \le 2\Psi(Q_k, (u_i), \mathbf{T}_k) - 2\Psi(K_0, (u_i), \mathbf{T}_k) + \frac{c_{17}}{k^\beta} |b_{K_0} - b_{Q_k}|_k, \tag{106}$$

for all $k \in \mathbb{N}$. (Again, we assume that the obvious changes are made in the notation.)

The next task is to check that Lemma 4.3 still holds. With (106) in hand, this rests on proving that, almost surely,

$$V_k = \frac{1}{k} \sum_{i=1}^{k} T_{ik}^2$$

is bounded. In fact we claim that, almost surely, $V_k \to 0$ as $k \to \infty$. To see this, note that

$$\begin{aligned} V_k &= \frac{1}{k} \sum_{i=1}^{k} \left(\frac{N_k(o) - N_k(h_k u_i)}{h_k} \right)^2 \\ &= \frac{1}{k} \sum_{i=1}^{k} \left(\frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I_k'}^{I_k'} \left(\frac{1 - \cos(z_{jk} \cdot h_k u_i)}{h_k} \right) X_{jk} \right)^2 \\ &= \frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p,q=-I_k'}^{I_k'} a_{pqk} X_{pk} X_{qk}, \end{aligned}$$

where

$$a_{pqk} = \frac{1}{k h_k^2} \sum_{i=1}^{k} \bigl(1 - \cos(z_{pk} \cdot h_k u_i)\bigr)\bigl(1 - \cos(z_{qk} \cdot h_k u_i)\bigr) \tag{107}$$

and hence $|a_{pqk}| \leq 4/h_k^2$. As in the proof of Lemma 7.2, we may take the indices p, q from 1 to I'_k, and then, by (102), the claim follows from Lemma 6.2 with $m_k = I'_k$ and $\nu = 2(1-\gamma-\varepsilon)$.

At this stage the work for Lemma 4.4 is already done. Indeed, by the Cauchy-Schwarz inequality,

$$\Psi(Q_k, (u_i), \mathbf{T}_k) - \Psi(K_0, (u_i), \mathbf{T}_k) \leq |b_{K_0} - b_{Q_k}|_k \left(\frac{1}{k} \sum_{i=1}^{k} T_{ik}^2 \right)^{1/2} = |b_{K_0} - b_{Q_k}|_k \, V_k^{1/2}.$$

Using this and (106) we see that, almost surely,

$$|b_{K_0} - b_{Q_k}|_k \leq 2V_k^{1/2} + \frac{c_{17}}{k^\beta} \to 0,$$

as $k \to \infty$.

Finally, the proof of Theorem 4.5 can be applied without change. ☐

The next algorithm corresponds to Algorithm NoisyCovDiff(φ). As for that algorithm, φ is a nonnegative bounded measurable function on $\mathbb{R}^n$ with support in C_0^n, such that $\int_{\mathbb{R}^n} \varphi(x)\,dx = 1$.

Algorithm NoisyMod^{2}Diff(φ)

Input: Natural numbers $n \geq 2$ and k; positive reals δ_k and ε_k; a real number γ satisfying $0 < \gamma < 1$; noisy measurements

$$\widetilde{g}_{ik} = |\widehat{1_{K_0}}(z_{ik})|^2 + X_{ik}, \tag{108}$$

of the squared modulus of the Fourier transform of the characteristic function of an unknown convex body $K_0 \subset C_0^n$ whose centroid is at the origin, at the points in

$$\{z_{ik} : i = 0, 1, \ldots, I'_k\} = \{o\} \cup (1/k^\gamma)\mathbb{Z}_k^n(+),$$

where $\mathbb{Z}_k^n(+)$ satisfies (78) and where the X_{ik}'s are independent normal $N(0, \sigma^2)$ random variables.

Task: Construct an o-symmetric convex polytope Q_k in $\mathbb{R}^n$ that approximates the difference body DK_0.

Action:

1. Let $\widetilde{g}_{ik} = \widetilde{g}_{(-i)k}$, for $i = -I'_k, \ldots, -1$, let $x_{ik} = k^{\gamma-1} z_{ik}$, $i = -I'_k, \ldots, I'_k$ be the points in the cubic array $2C_0^n \cap (1/k)\mathbb{Z}^n$, and let

$$M_k(x_{ik}) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x_{ik}) \widetilde{g}_{jk}, \tag{109}$$

for $i = -I'_k, \ldots, I'_k$.

2. Run Algorithm NoisyCovDiff(φ) with inputs n, k, δ_k, ε_k, and M_{ik} replaced by $M_k(x_{ik})$, for $i = -I'_k, \ldots, I'_k$ and with the obvious re-indexing in i. The output Q_k of that algorithm is also the output of the present one.

We shall show that the argument in Section 5 used to prove Theorem 5.6 can be modified to yield the following convergence result.

Theorem 7.4. *Suppose that* K_0, δ_k, ε_k, *and* g_k *are as in Algorithm NoisyMod*^{2}*Diff*(φ). *Assume that* $\lim_{k\to\infty}\varepsilon_k = 0$ *and that* $\delta_k \sim k^{-\lambda}$, *where* $0<\lambda<n(\gamma-1/2)$. *If* Q_k *is an output from Algorithm NoisyMod*^{2}*Diff*(φ) *as stated above, then, almost surely,*

$$\delta(DK_0, Q_k) \le c_{18}\delta_k^{1/n}, \tag{110}$$

for sufficiently large k. *In particular, almost surely,* Q_k *converges to* DK_0 *as* $k\to\infty$.

Proof. Algorithm NoisyMod^{2}Diff(φ) can be regarded as Algorithm NoisyCovDiff(φ) with M_{ik} and N_{ik} replaced by $M_k(x_{ik})$ defined by (109) and $N_k(x_{ik})$ defined by (83) with $x = x_{ik}$, respectively. We follow the arguments of Section 5 with this substitution in mind.

Proposition 5.1 and Corollary 5.2 are unaltered. For Lemma 5.3, we note first that by (83), $E(N_k(x_{ik})) = 0$ for all i and k. The same calculations as in the proof of Lemma 5.3 lead to

$$|E(g_k(x)) - g_{K_0}(x)| \le 2n(\varepsilon_k + 1/k) + d_k,$$

where d_k is as in Lemma 6.1. By that lemma, $d_k \to 0$ as $k\to\infty$ and hence the second statement in Lemma 5.3 still holds.

Next, for Lemma 5.4, it will be convenient to let

$$\alpha(i,k,x) = \int_{(1/k)C_0^n + x_{ik}} \varphi_{\varepsilon_k}(x-z)\,dz.$$

Then we have, by (83),

$$\begin{aligned} R_k(x) = g_k(x) - E(g_k(x)) &= \sum_{i=-I'_k}^{I'_k} \alpha(i,k,x) N_k(x_{ik}) \\ &= \sum_{j=-I'_k}^{I'_k} \left(\frac{1}{(2\pi k^\gamma)^n} \sum_{i=-I'_k}^{I'_k} \alpha(i,k,x)\cos(z_{jk}\cdot x_{ik}) \right) X_{jk}. \end{aligned}$$

This is a weighted sum of independent $N(0,\sigma^2)$ random variables, so it is $N(0,\tau^2(x))$, where

$$\tau^2(x) = \frac{\sigma^2}{(2\pi k^\gamma)^{2n}} \sum_{j=-I'_k}^{I'_k} \left(\sum_{i=-I'_k}^{I'_k} \alpha(i,k,x)\cos(z_{jk}\cdot x_{ik}) \right)^2.$$

Using the fact that $|\cos t| \le 1$ and $\sum_{i=-I'_k}^{I'_k}\alpha(i,k,x)\le 1$, we see that

$$\tau^2(x) \le \frac{\sigma^2(2k+1)^n}{(2\pi k^\gamma)^{2n}} = O(k^{n-2\gamma n}).$$

The same argument as in the proof of Lemma 5.4 now leads to the conclusion that there is an $N_4 = N_4((\varepsilon_k), n)\in\mathbb{N}$ such that

$$\Pr(|g_k(x) - g_{K_0}(x)| > \delta) \le c_{19}(\delta k^{\gamma n - n/2})^{-1}\exp(-c_{20}\delta^2 k^{2\gamma n - n}), \tag{111}$$

for all $k \geq N_4$ and all $x \in \mathbb{R}^n$. (Compare (69).)

Lemma 5.5 is unchanged. If $\delta_k = O(k^{-\lambda})$ for some $\lambda > 0$, then

$$c_{19}(\delta_k k^{\gamma n - n/2})^{-1} = O(k^{n/2-\gamma n+\lambda}) \leq 1,$$

for sufficiently large n, provided $\lambda < n(\gamma - 1/2)$. The latter condition also ensures that the exponent of k in the exponential term in (111) (with $\delta = \delta_k$) is positive. This is all that is required to allow the proof of Theorem 5.6 to go through until near the end, when we use the fact that $k\delta_k^{1/n} \to \infty$ as $k \to \infty$. If $\delta_k \sim k^{-\lambda}$, this still holds since $\lambda/n < \gamma - 1/2 < 1$ and hence $1 - \lambda/n > 0$. In this case the conclusion is the same, namely that, almost surely,

$$\delta(DK_0, Q_k) \leq c_{18}\delta_k^{1/n},$$

for sufficiently large k. □

Concerning Corollary 5.7, if $\lim_{k\to\infty} \varepsilon_k = 0$ and $\delta_k \sim k^{-\lambda}$, we have now the convergence rate $k^{-\lambda/n}$. Since $\lambda/n < \gamma - 1/2$ and $\gamma < 1$, we can achieve a rate arbitrarily close to $k^{-1/2}$, the same as before.

8. Phase retrieval from the modulus

This section addresses Problem 3 in the introduction. A simple trick converts Problem 3 into one very closely related to Problem 2, considered in the previous section.

Suppose, more generally, that noisy measurements are taken of $\sqrt{\widehat{g}}$, where g is an even continuous real-valued function on $\mathbb{R}^n$ with support in $[-1,1]^n$. The just-mentioned trick is to take two independent measurements at each point, multiply the two, and use the resulting quantities in place of the measurements of $\widehat{g}$ considered earlier. Thus instead of (79) above we have, for $r = 1, 2$, measurements

$$\overline{g}^{(r)}_{z,k} = \sqrt{\widehat{g}(z/k^\gamma)} + X^{(r)}_{z,k}, \tag{112}$$

of $\sqrt{\widehat{g}}$, for $z \in \{o\} \cup \mathbb{Z}^n_k(+)$, where $\mathbb{Z}^n_k(+)$ satisfies (78) and where the $X^{(r)}_{z,k}$'s are independent $N(0,\sigma^2)$ random variables. Then we replace $\tilde{g}_{z,k}$ in (79) by

$$\overline{g}_{z,k} = \overline{g}^{(1)}_{z,k}\overline{g}^{(2)}_{z,k} = \widehat{g}(z/k^\gamma) + \sqrt{\widehat{g}(z/k^\gamma)}\left(X^{(1)}_{z,k} + X^{(2)}_{z,k}\right) + X^{(1)}_{z,k}X^{(2)}_{z,k}. \tag{113}$$

Setting $\overline{g}_{jk} = \overline{g_{K_0}}_{z_{jk},k}$ and $X_{jk} = X_{z_{jk},k}$, the same notation and analysis that gave (81), but now using (80) and (113), leads instead to

$$\overline{M}_k(x) = g_{K_0}(x) + \overline{N}_k(x) - d_k(x), \tag{114}$$

where

$$\overline{M}_k(x) = \frac{1}{(2\pi k^\gamma)^n}\sum_{j=-I'_k}^{I'_k}\cos(z_{jk}\cdot x)\overline{g}_{jk} \tag{115}$$

is an estimate of $g_{K_0}(x)$,

$$\overline{N}_k(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \sqrt{\widehat{g_{K_0}}(z_{jk}/k^\gamma)} \cos(z_{jk} \cdot x) \left(X_{jk}^{(1)} + X_{jk}^{(2)}\right) + \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x) X_{jk}^{(1)} X_{jk}^{(2)} \tag{116}$$

is a random variable, and the deterministic error $d_k(x)$ is given as before by (84).

For our analysis it will be convenient to let

$$\overline{N}_{k1}(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \sqrt{\widehat{g_{K_0}}(z_{jk}/k^\gamma)} \cos(z_{jk} \cdot x) \left(X_{jk}^{(1)} + X_{jk}^{(2)}\right) \tag{117}$$

and

$$\overline{N}_{k2}(x) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x) X_{jk}^{(1)} X_{jk}^{(2)}, \tag{118}$$

so that $\overline{N}_k(x) = \overline{N}_{k1}(x) + \overline{N}_{k2}(x)$.

To keep the exposition brief, we shall not give a formal presentation of our algorithms, called **Algorithm NoisyModLSQ**, **Algorithm NoisyModBlaschke**, and **Algorithm NoisyModDiff(φ)**, since they are very similar to Algorithm NoisyMod^{2}LSQ, Algorithm NoisyMod^{2}Blaschke, and Algorithm NoisyMod^{2}Diff(φ), respectively. In each case the input is as before, except that instead of (92), (99), and (108), we now have measurements

$$\overline{g}_{ik}^{(r)} = |\widehat{1_{K_0}}(z_{ik})| + X_{ik}^{(r)}, \tag{119}$$

for $r = 1, 2$, of the modulus of the Fourier transform of the characteristic function of K_0, where the $X_{ik}^{(r)}$'s are independent normal $N(0, \sigma^2)$ random variables. The task is the same in each case. For the actions, we first let $\overline{g}_{ik} = \overline{g}_{ik}^{(1)} \overline{g}_{ik}^{(2)}$ and then follow the actions of the appropriate algorithms in the previous section, replacing $\widetilde{g}$ by $\overline{g}$. Thus in the action of each algorithm, we replace $M_k(x)$ by $\overline{M}_k(x)$ defined by (115), for the appropriate x.

Theorem 8.1. *Theorem 7.1 holds when Algorithm NoisyMod^{2}LSQ is replaced by Algorithm NoisyModLSQ.*

Proof. In the action of Algorithm NoisyModLSQ, the measurements used in Algorithm NoisyCovLSQ are now $\overline{M}_k(x_{ik})$, $i = -I'_k, \dots, I'_k$, where $\overline{M}_k(x_{ik})$ is given by (115) with $x = x_{ik}$. Thus we have

$$\overline{M}_k(x_{ik}) = g_{K_0}(x_{ik}) + \overline{N}_k(x_{ik}) - d_k(x_{ik}),$$

$i = -I'_k, \dots, I'_k$, where $\overline{N}_k(x_{ik})$ and $d_k(x_{ik})$ are given by (116) and (84), respectively, with $x = x_{ik}$.

We claim that Lemma 7.2 holds when $N_k(x_{ik})$ is replaced by $\overline{N}_k(x_{ik})$. To see this, use the triangle inequality to obtain

$$\begin{aligned}\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\overline{N}_k(x_{ik})^+ &\le \left(\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\overline{N}_k(x_{ik})^2\right)^{1/2}\\ &\le \left(\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\overline{N}_{k1}(x_{ik})^2\right)^{1/2}+\left(\frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\overline{N}_{k2}(x_{ik})^2\right)^{1/2},\end{aligned}$$

where $\overline{N}_{k1}(x_{ik})$ and $\overline{N}_{k2}(x_{ik})$ are given by (117) and (118), respectively, with $x = x_{ik}$. Since $\widehat{g_{K_0}}$ is bounded, the same analysis as in the proof of Lemma 7.2, up to a constant, applies to the first of the two sums in the previous expression. So it suffices to prove that, almost surely,

$$\overline{S}_k = \frac{1}{I_k}\sum_{i=-I'_k}^{I'_k}\overline{N}_{k2}(x_{ik})^2 \to 0,$$

as $k \to \infty$. As in the proof of Lemma 7.2, it is enough to show that, almost surely,

$$\frac{1}{(2\pi k^\gamma)^{2n}}\sum_{p,q=1}^{I'_k} c_{pqk}X^{(1)}_{pk}X^{(2)}_{pk}X^{(1)}_{qk}X^{(2)}_{qk} \to 0,$$

as $k \to \infty$. This follows from Lemma 6.3 and proves the claim.

With this in hand, we can conclude exactly as in the proof of Theorem 7.1 that Algorithm NoisyCovLSQ works with the new measurements under the same hypotheses. □

We remark that the computation of $E(\overline{Z}_k)$ in Lemma 6.3 shows why we take two independent measurements of $\sqrt{\widehat{g_{K_0}}}$ and multiply, rather than taking a single measurement and squaring it. In the latter case we would be led to

$$E(\overline{Z}_k) = \frac{E(Y_{11}^2)}{(2\pi k^\gamma)^{2n}}\sum_{p,q=1}^{m_k} a_{pqk} = O(k^{2n-2n\gamma+\nu}),$$

which may be unbounded as $k \to \infty$.

Theorem 8.2. *Theorem 7.3 holds when Algorithm NoisyMod^{2}Blaschke is replaced by Algorithm NoisyModBlaschke.*

Proof. We now have

$$\overline{y}_{ik} = \zeta_{ik} + \overline{T}_{ik},$$

where ζ_{ik} is as in (105) and

$$\overline{T}_{ik} = \frac{\overline{N}_k(o)-\overline{N}_k(h_ku_i)}{h_k} = \frac{\overline{N}_{k1}(o)-\overline{N}_{k1}(h_ku_i)}{h_k} + \frac{\overline{N}_{k2}(o)-\overline{N}_{k2}(h_ku_i)}{h_k}, \tag{120}$$

for $i = 1, \dots, k$, where $\overline{N}_{k1}$ and $\overline{N}_{k2}$ are given by (117) and (118). The proof of Theorem 7.3 can be followed, except that for Lemma 4.3, one now shows that, almost surely,

$$\overline{V}_k = \frac{1}{k}\sum_{i=1}^{k} \overline{T}_{ik}^2 \to 0$$

as $k \to \infty$. Using the fact that the earlier analysis applies to $\overline{N}_{k1}$, and using also the triangle inequality, as we did in the proof of Theorem 8.1, with (120), we see that it suffices to examine

$$\frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p,q=1}^{I'_k} a_{pqk} X_{pk}^{(1)} X_{pk}^{(2)} X_{qk}^{(1)} X_{qk}^{(2)},$$

where a_{pqk} is given by (107). Then Lemma 6.3 shows that it is possible to choose γ and ε exactly as in Theorem 7.3 to ensure that Lemma 4.3 holds. No further changes are required, so Algorithm NoisyCovBlaschke works with the new measurements under the same hypotheses as in Theorem 7.3. □

Theorem 8.3. *Theorem 7.4 holds when Algorithm NoisyMod^{2}Diff(φ) is replaced by Algorithm NoisyModDiff(φ).*

Proof. Note that by (116), we have $E(\overline{N}_k(x_{ik})) = 0$ for all i and k. Therefore the same calculations as in the proof of Theorem 7.4 show that the second statement in Lemma 5.3 still holds.

In Lemma 5.4, it is enough in view of the proof of Theorem 7.4 to consider the contribution to $R_k(x)$ from $\overline{N}_{k2}(x_{ik})$, namely,

$$\sum_{j=-I'_k}^{I'_k} \left(\frac{1}{(2\pi k^\gamma)^n} \sum_{i=-I'_k}^{I'_k} \alpha(i,k,x) \cos(z_{jk}\cdot x_{ik}) \right) X_{jk}^{(1)} X_{jk}^{(2)}.$$

This is a weighted sum of independent random variables, though these variables are no longer normal. The mean is clearly zero, and the variance is

$$\overline{\tau}^2(x) = \frac{\sigma^4}{(2\pi k^\gamma)^{2n}} \sum_{j=-I'_k}^{I'_k} \left(\sum_{i=-I'_k}^{I'_k} \alpha(i,k,x) \cos(z_{jk}\cdot x_{ik}) \right)^2.$$

This allows the same estimate as before, up to a constant. No further changes are required, so Algorithm NoisyCovDiff(φ) works with the new measurements under the same hypotheses as in Theorem 7.4. □

The previous result provides a convergence rate for Algorithm NoisyCovDiff(φ) arbitrarily close to $k^{-1/2}$, as was noted for Algorithm NoisyMod^{2}Diff(φ) after Theorem 7.4.

References

[1] R. J. Adler and R. Pyke, Problem 91–3, *Inst. Math. Statist. Bull.* **20** (1991), 409.

[2] R. J. Adler and R. Pyke, Scanning Brownian processes, *Adv. in Appl. Probab.* **39** (2007), 613–629.

[3] I. A. Ahmad and P.-E. Lin, Fitting a multiple regression function, *J. Statist. Plann. Inference* **9** (1984), 163–176.

[4] G. Averkov and G. Bianchi, Confirmation of Matheron's conjecture on the covariogram of a planar convex body, *J. Europ. Math. Soc.*, to appear.

[5] M. Baake and U. Grimm, Homometric model sets and window covariograms, *Z. Krist.* **222** (2007), 54–58.

[6] C. Benassi and G. D'Ercole, An algorithm for reconstructing a convex polygon from its covariogram, *Rend. Istit. Mat. Univ. Trieste* **39** (2007), 457–476.

[7] G. Bianchi, Determining convex polygons from their covariograms, *Adv. in Appl. Probab.* **34** (2002), 261–266.

[8] G. Bianchi, Matheron's conjecture for the covariogram problem, *J. London Math. Soc.* (2) **71** (2005), 203–220.

[9] G. Bianchi, The covariogram determines three-dimensional convex polytopes, *Adv. Math.* **220** (2009), 1771–1808.

[10] G. Bianchi, F. Segala, and A. Volčič, The solution of the covariogram problem for plane $\mathcal{C}^2_+$ convex bodies, *J. Differential Geom.* **60** (2002), 177–198.

[11] P. Billingsley, *Convergence of Probability Measures*, second edition, John Wiley and Sons, New York, 1999.

[12] J. Bourgain and J. Lindenstrauss, *Projection bodies*, in: Geometric Aspects of Functional Analysis (1986/7), Lecture Notes in Math. 1317, Springer, Berlin, 1988, pp. 250–270.

[13] L. Brandolini, S. Hoffman, and A. Iosevich, Sharp rate of average decay of the Fourier transform of a bounded set, *Geom. Funct. Anal.* **13** (2003), 671–680.

[14] N. S. Brannen, The Wills conjecture, *Trans. Amer. Math. Soc.* **349** (1997), 3977–3987.

[15] A. Cabo and A. Baddeley, Estimation of mean particle volume using the set covariance function, *Adv. in Appl. Probab.* **35** (2003), 27–46.

[16] S. Campi, Recovering a centred convex body from the areas of its shadows: a stability estimate, *Ann. Mat. Pura Appl.* (4) **151** (1988), 289–302.

[17] R. M. Dudley, Distances of probability measures and random variables, *Ann. Math. Stat.* **39** (1968), 1563–1572.

[18] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1, third edition, John Wiley and Sons, New York, 1968.

[19] J. R. Fienup, Phase retrieval algorithms: a comparison, *Appl. Opt.* **21** (1982), 2758–2769.

[20] R. J. Gardner, *Geometric Tomography*, second edition, Cambridge University Press, New York, 2006.

[21] R. J. Gardner, The Brunn-Minkowski inequality, *Bull. Amer. Math. Soc.* **39** (2002), 355–405.

[22] R. J. Gardner, P. Gronchi, and C. Zong, Sums, projections, and sections of lattice sets, and the discrete covariogram, *Discrete Comput. Geom.* **34** (2005), 391–409.

[23] R. J. Gardner and M. Kiderlen, A solution to Hammer's X-ray reconstruction problem, *Adv. Math.* **214** (2007), 323–343.

[24] R. J. Gardner, M. Kiderlen, and P. Milanfar, Convergence of algorithms for reconstructing convex bodies and directional measures, *Ann. Statist.* **34** (2006), 1331–1374.

[25] R. J. Gardner and P. Milanfar, Reconstruction of convex bodies from brightness functions, *Discrete Comput. Geom.* **29** (2003), 279–303.

[26] R. J. Gardner and G. Zhang, Affine inequalities and radial mean bodies, *Amer. J. Math.* **120** (1998), 493–504.

[27] P. Goodey, R. Schneider, and W. Weil, On the determination of convex bodies by projection functions, *Bull. London Math. Soc.* **29** (1997), 82-88.

[28] E. K. Haviland and A. Wintner, On the Fourier transform of distributions on convex curves, *Duke Math. J.* **2** (1936), 712–721.

[29] D. Hug and R. Schneider, Stability results involving surface area measures of convex bodies, *Rend. Circ. Mat. Palermo* (2) Suppl. No. 70, part II (2002), 21–51.

[30] N. E. Hurt, *Phase Retrieval and Zero Crossings*, Kluwer, Dordrecht, 1989.

[31] M. Kiderlen and E. B. V. Jensen, Estimation of the directional measure of planar random sets by digitization, *Adv. Appl. Probab.* **35** (2003), 583–602.

[32] M. V. Klibanov, P. E. Sacks, and A. V. Tikhonravov, The phase retrieval problem, *Inverse Problems* **11** (1995), 1–28.

[33] F. C. Liu, On the localization of rectangular partial sums for multiple Fourier series, *Proc. Amer. Math. Soc.* **34** (1972), 90–96.

[34] D. R. Luke, J. V. Burke, and R. G. Lyon, Optical wavefront reconstruction: theory and numerical methods, *SIAM Rev.* **44** (2002), 169–224.

[35] C. L. Mallows and J. M. C. Clark, Linear-intercept distributions do not characterize plane sets, *J. Appl. Probab.* **7** (1970), 240–244.

[36] G. Matheron, *Random Sets and Integral Geometry*, Wiley, New York, 1975.

[37] G. Matheron, La formule de Steiner pour les érosions, *J. Appl. Probab.* **15** (1978), 126–135.

[38] G. Matheron, Le covariogramme géometrique des compacts convexes des R^2, *Technical Report N-2/86/G, Centre de Géostatistique, Ecole Nationale Supérieure des Mines de Paris*, 1986.

[39] W. Nagel, Orientation-dependent chord length distributions characterize convex polygons, *J. Appl. Probab.* **30** (1993), 730–736.

[40] J. Rosenblatt, Phase retrieval, *Commun. Math. Phys.* **95** (1984), 317–343.

[41] M. Schmitt, On two inverse problems in mathematical morphology, in: *Mathematical Morphology in Image Processing*, ed. by E. R. Dougherty, Marcel Dekker, New York, pp. 151–169.

[42] M. Schmuckenschläger, The distribution function of the convolution square of a convex symmetric body in $\mathbb{R}^n$, *Israel J. Math.* **78** (1992), 309–334.

[43] J. Serra, *Image Analysis and Mathematical Morphology*, Academic Press, London, 1982.

[44] R. Schneider, *Convex Bodies: The Brunn-Minkowski Theory*, Cambridge University Press, Cambridge, 1993.

[45] A. Tsolomitis, Convolution bodies and their limiting behavior, *Duke Math. J.* **87** (1997), 181–203.

[46] S. van de Geer, *Applications of Empirical Process Theory*, Cambridge University Press, New York, 2000.

[47] E. Werner, A general geometric construction for affine surface area, *Studia Math.* **132** (1999), 227–238.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI FIRENZE, VIALE MORGAGNI 67/A, FIRENZE, ITALY I-50134

E-mail address: `gabriele.bianchi@unifi.it`

DEPARTMENT OF MATHEMATICS, WESTERN WASHINGTON UNIVERSITY, BELLINGHAM, WA 98225-9063

E-mail address: `Richard.Gardner@wwu.edu`

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF AARHUS, NY MUNKEGADE, DK–8000 AARHUS C, DENMARK

E-mail address: `kiderlen@imf.au.dk`