

4-2011

# Phase Retrieval for Characteristic Functions of Convex Bodies and Reconstruction from Covariograms

Gabriele Bianchi  
*Università di Firenze*

Richard J. Gardner  
*Western Washington University, Richard.Gardner@wwu.edu*

Markus Kiederlen  
*University of Aarhus*

Follow this and additional works at: [https://cedar.wwu.edu/math\\_facpubs](https://cedar.wwu.edu/math_facpubs)

 Part of the [Mathematics Commons](#)

---

## Recommended Citation

Bianchi, Gabriele; Gardner, Richard J.; and Kiederlen, Markus, "Phase Retrieval for Characteristic Functions of Convex Bodies and Reconstruction from Covariograms" (2011). *Mathematics*. 22.  
[https://cedar.wwu.edu/math\\_facpubs/22](https://cedar.wwu.edu/math_facpubs/22)

This Article is brought to you for free and open access by the College of Science and Engineering at Western CEDAR. It has been accepted for inclusion in Mathematics by an authorized administrator of Western CEDAR. For more information, please contact [westerncedar@wwu.edu](mailto:westerncedar@wwu.edu).

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

GABRIELE BIANCHI, RICHARD J. GARDNER, AND MARKUS KIDERLEN

### 1. Introduction

The *Phase Retrieval Problem* of Fourier analysis involves determining a function  $f$  on  $\mathbb{R}^n$  from the modulus  $|f|$  of its Fourier transform  $\hat{f}$ . 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  $|f|^2$  that is directly measured.) In 1984, Rosenblatt [42] wrote that the Phase Retrieval Problem “arises in all experimental uses of diffracted electromagnetic radiation for determining the intrinsic detailed structure of a diffracting object.” Today, the word “all” is perhaps too strong in view of recent advances in coherent diffraction imaging. In any case, the literature is vast; see the surveys [32], [34], [36], and [42], as well as the articles [9] and [18] and the references given there.

Phase retrieval is fundamentally underdetermined 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 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

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

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,

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

---

Received by the editors July 7, 2009 and, in revised form, June 30, 2010, and July 23, 2010.

2010 *Mathematics Subject Classification*. Primary 42–04, 42B10, 52–04, 52A20; Secondary 52B11, 62H35.

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

The second author was supported in part by U.S. National Science Foundation grant DMS-0603307.

©2010 American Mathematical Society  
Reverts to public domain 28 years from publication

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

$$(1) \quad g_K = 1_K 1_{-K} = 1_K 1_K \quad \text{---} = 1_K^2.$$

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 [38] 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 [45]. 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 [46, Theorem 7.3.1]), by Gardner and Zhang [26] in the theory of radial mean bodies, and by Tsolomitis [47] in his study of convolution bodies, which via the work of Schmuckenschläger [44] and Werner [50] 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  $|1_K|^2$ .*

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

In order to discuss our results, we must first address 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. Matheron [40] 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?*

The focus on covariograms of convex bodies is natural. One reason is that Mallows and Clark [37] constructed noncongruent 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 noncongruent nonconvex 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.

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.

A detailed historical account of the covariogram problem may be found in [4]. The current status is as follows, in which “determined” always means determined by the covariogram among all convex bodies, up to translation and reflection in the origin. Averkov and Bianchi [4] showed that planar convex bodies are determined, thereby confirming Matheron’s conjecture. Bianchi [8] proved, by a long and intricate argument, that three-dimensional convex polyhedra are determined. It is easy to see that centrally symmetric convex bodies are determined. (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  $\mathbb{R}^n$  are determined. Nevertheless, the Covariogram Problem in general has a negative answer, as Bianchi [7] demonstrated by constructing convex polytopes in  $\mathbb{R}^n$ ,  $n \geq 4$ , that are not determined. It is still unknown whether convex bodies in  $\mathbb{R}^3$  are determined.

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 [43] 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 zero mean random variables with uniformly bounded  $p$ th moments, where  $p$  is at most six and usually four. 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  $\nabla K_0$ , the so-called Blaschke body of  $K_0$ . (See Section 3 for definitions and notation.) The crucial property of  $\nabla K_0$  is that when  $K_0$  is a convex polytope, each of its facets is parallel to some facet of  $\nabla K_0$ . 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, Algorithm NoisyBrightLSQ, designed earlier by Gardner and Milanfar (see [24]) for reconstructing an  $o$ -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( $\phi$ ) 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  $\nabla K_0$ , that when  $K_0$  is a convex polytope, each of its facets is parallel to some facet of  $DK_0$ . Furthermore,  $DK_0$  is just the support of  $g_{K_0}$ . The known property that  $g_{K_0}$  is concave (a consequence of the Brunn-Minkowski inequality [21, Section 11]) can therefore be combined with techniques from multiple regression. Algorithm NoisyCovDiff( $\phi$ ) employs a Gasser-Müller type kernel estimator for  $g_{K_0}$ , with suitable kernel function  $\phi$ , 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  $2C_k^n = [-1, 1]^n$  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  $K_0$  is determined among convex bodies, up to translation and reflection in the origin, by its covariogram, we show that, almost surely,

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

as  $k \rightarrow \infty$ , where  $\delta$  denotes Hausdorff distance. (If  $K_0$  is not so determined, 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, as well as a suitable version of the Strong Law of Large Numbers. Some effort has been made to make the proof fairly self-contained, but some arguments from the proof from [24] that Algorithm NoisyBrightLSQ is strongly consistent are used in proving that Algorithm NoisyCovBlaschke is strongly consistent. One such argument rests on the Bourgain-Campi-Lindenstrauss stability result for projection bodies.

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  $|1_{K_0}|$  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  $|1_{K_0}|^2$  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  $\gamma$ . The three resulting algorithms, Algorithm NoisyMod<sup>2</sup>LSQ, Algorithm NoisyMod<sup>2</sup>Blaschke, and Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ), are stated in detail and, with suitable restrictions on  $\gamma$ , proved to be strongly consistent under the same hypotheses as for Problem 1.

Our final three algorithms, Algorithm NoisyModLSQ, Algorithm NoisyModBlaschke, and Algorithm NoisyModDiff( $\phi$ ) cater to 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, *first* use *either* Algorithm NoisyCovBlaschke *or* Algorithm NoisyCovDiff( $\phi$ ) and *then* use Algorithm NoisyCovLSQ.
- For Problem 2, *first* use *either* Algorithm NoisyMod<sup>2</sup>Blaschke *or* Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) and *then* use Algorithm NoisyMod<sup>2</sup>LSQ.
- For Problem 3, *first* use *either* Algorithm NoisyModBlaschke *or* Algorithm NoisyModDiff( $\phi$ ) and *then* use Algorithm NoisyModLSQ.

These results can also be viewed as a contribution to the literature on the associated uniqueness problems. They show that if a convex body is determined, up to translation and reflection in the origin, by its covariogram, then it is also so determined by its values at certain countable sets of points, even, almost surely, when these values are contaminated with noise. Similarly, the characteristic function of such a convex body is also determined, almost surely, by certain countable sets of noisy values of the modulus of its Fourier transform.

Our noise model is sufficiently general to apply to all the main cases of practical interest: zero mean Gaussian noise, Poisson noise (unbiased measurements following a Poisson distribution, sometimes called shot noise), or Poisson noise plus zero mean Gaussian noise. However, the main text of this paper deals solely with theory. With the exception of Corollary 6.5 and Remark 6.6, where the method of proof leads naturally to rates of convergence for Algorithm NoisyCovDiff( $\phi$ ) and hence for the two related algorithms for phase retrieval, the focus is entirely on strong consistency. Further remarks about convergence rates, sampling designs, and implementation issues have been relegated to the Appendix. Much remains to be done. We believe, however, that 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.

We are grateful to Jim Fienup, David Mason, and Sara van de Geer for helpful correspondence and to the referees for some insightful suggestions that led to significant improvements.



## 2. Guide to the paper

### §3. *Definitions, notation, and preliminary results.*

We recommend that the reader skip this section and refer back to it when necessary.

### §4. *The main algorithm for reconstruction from covariograms.*

This presents the main (*second* stage) Algorithm NoisyCovLSQ for Problem 1 and its strong consistency, established in Theorem 4.10.

### §5. *Approximating the Blaschke body via the covariogram.*

The first of the two first-stage algorithms for Problem 1, Algorithm NoisyCovBlaschke, is stated with proof of strong consistency in Theorem 5.4. 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 is a weak restriction.

### §6. *Approximating the difference body via the covariogram.*

In this section, the second of the two first-stage algorithms for Problem 1, Algorithm NoisyCovDiff( $\phi$ ), is set out and proved to be strongly consistent in Theorem 6.4.

### §7. *Phase retrieval: Framework and technical lemmas.*

Necessary material from Fourier analysis is gathered, and the scene is set for results on phase retrieval. This does not depend on the previous three sections.

### §8. *Phase retrieval from the squared modulus.*

The algorithms for Problem 2, Algorithm NoisyMod<sup>2</sup>LSQ, Algorithm NoisyMod<sup>2</sup>Blaschke, and Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) are presented and strong consistency theorems for them are proved.

### §9. *Phase retrieval from the modulus.*

The corresponding algorithms for Problem 3, Algorithm NoisyModLSQ, Algorithm NoisyModBlaschke, and Algorithm NoisyModDiff( $\phi$ ), are presented and shown to be strongly consistent.

### §10. *Appendix.*

Rates of convergence and implementation issues are discussed.

## 3. Definitions, notation, and preliminary results

**3.1. Basic 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  $\mathbb{R}^n$ . It is assumed throughout that  $n \geq 2$ . 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  $\partial A$ ,  $\text{int} A$ ,  $\text{relint} A$ ,  $\text{diam} A$ , and  $1_A$  the *boundary*, *interior*, *relative interior*, *diameter*, and *characteristic function* 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  $\varepsilon$ -*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  $\varepsilon$  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

$$(2) \quad E \mathcal{S} F = \{x \in \mathbb{R}^n : F + x \subset E\}$$

their *Minkowski difference*.

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

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

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  $|f(k)| \leq c|g(k)|$  for sufficiently large  $k$ . The notation  $f \sim g$  will mean that  $f = O(g)$  and  $g = O(f)$ .

**3.2. Convex geometry.** Let  $K^n$  be the class of compact convex sets in  $\mathbb{R}^n$ , and let  $K^n(A)$  be the subclass of members of  $K^n$  contained in the subset  $A$  of  $\mathbb{R}^n$ . A *convex body* in  $\mathbb{R}^n$  is a compact convex set with nonempty interior. The notation  $K^n(r, R)$  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 [46] is an excellent general reference for convex geometry.

Figures illustrating many of the following definitions can be found in [20].

If  $K \in K^n$ , then

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

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  $K \in K^n$  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  $x \neq 0$ . The *Hausdorff distance*  $\delta(K, L)$  between two sets  $K, L \in K^n$  can then be conveniently defined by

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

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

$$\delta(K, L) = \min\{\varepsilon \geq 0 : K \subset L + \varepsilon B^n, L \subset K + \varepsilon B^n\}.$$

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

$$S(K, E) = V_{n-1}(g^{-1}(K, E)),$$

where  $g^{-1}(K, E)$  is the set of points in  $\partial K$  at which there is an outer unit normal vector in  $E$ . Let  $S(K) = S(K, S^{n-1})$ . Then  $S(K)$  is the *surface area* of  $K$ . The



*Blaschke body*  $\nabla K$  of a convex body  $K$  is the unique  $o$ -symmetric convex body satisfying

$$(3) \quad S(\nabla K, \cdot) = \frac{1}{2}S(K, \cdot) + \frac{1}{2}S(-K, \cdot).$$

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

$$(4) \quad h_{\Pi K} = b_K.$$

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

$$(5) \quad h_{\Pi K}(u) = b_K(u) = \frac{1}{2} \int_{S^{n-1}} |u \cdot v| \, dS(K, v),$$

and Cauchy's surface area formula is

$$(6) \quad S(K) = \frac{1}{\kappa_{n-1}} \int_{S^{n-1}} b_K(u) \, du;$$

see [20, (A.45) and (A.49), p. 408]. By (3) and (5), we have

$$(7) \quad b_{\nabla K} = b_K,$$

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

The *difference body* of  $K$  is the  $o$ -symmetric convex body  $DK = K + (-K)$ .

**3.3. The covariogram.** 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  $x \notin \text{int } DK$ , 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  $K$  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  $X_u K$  defined by

$$X_u K(x) = \int_{u+x}^x 1_K(y) \, dy,$$

for  $x \in u^\perp$ . Now define

$$(8) \quad E_K(t, u) = \{y \in u^\perp : X_u K(y) > t\}$$

and

$$(9) \quad a_K(t, u) = V(E_K(t, u)),$$

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

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

$$(10) \quad g_K(t, u) = \int_t^\infty a_K(s, u) \, ds$$

was noticed by Matheron [38, p. 86] in the form

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

which holds for all  $t \geq 0$  with  $tu \in \partial(DK)$ . This also yields

$$\frac{\partial g_K(t, u)}{\partial t} \Big|_{t=0} = -b_K(u).$$

(Note that the partial derivative here is one-sided;  $g_K$  is not differentiable at the origin.)

**Lemma 3.1.** *Let  $r > 0$  and let  $K$  be a convex body with  $rB^n \subset K$ . If  $0 < t \leq 2r$ , then*

$$(11) \quad 1 - \frac{t}{2r} b_K(u) \leq \frac{g_K(o) - g_K(tu)}{t} \leq b_K(u),$$

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

*Proof.* Let  $u \in S^{n-1}$ . By (10), 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

$$(12) \quad a_K(t, u) \leq \frac{g_K(o) - g_K(tu)}{t} \leq a_K(0, u) = b_K(u).$$

The set

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

is generally not a subset of  $K$ , but elementary geometry using  $[-ru, ru] \subset K$  and (8) gives

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

Taking the  $(n - 1)$ -dimensional volumes of these sets and using (9) yields

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

The lemma follows from the previous inequality and (12). D

An inequality similar to (11) was derived in [33, Theorem 1] for  $n = 2$ .

Matheron [40, p. 2] showed that the covariogram of a convex body is a Lipschitz function. For the convenience of the reader, we provide a proof of this fact based on [19], which yields the optimal Lipschitz constant.

**Proposition 3.2.** *If  $K$  is a convex body in  $\mathbb{R}^n$  and  $x, y \in \mathbb{R}^n$ , then*

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

*Proof.* We have

$$(K \cap (K + x)) \# (K \cap (K + y)) \subset (K + x) \# (K + y).$$

This implies

$$\begin{aligned} V(K \cap (K + x)) - V(K \cap (K + y)) &\leq V(K \# (K + y - x)) \\ &= V(K) - V(K \cap (K + y - x)). \end{aligned}$$

Equivalently,  $g_K(x) - g_K(y) \leq g_K(o) - g_K(y - x) = g_K(o) - g_K(x - y)$ , and interchanging  $x$  and  $y$  yields

$$|g_K(x) - g_K(y)| \leq g_K(o) - g_K(x - y).$$

Using this and the right-hand inequality in (11), we get

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

and the proposition follows immediately. D

**Corollary 3.3.** *If  $K_0 \subset C^n_0$  is a convex body, then for all  $x, y \in \mathbb{R}^n$ ,*

$$|g_{K_0}(x) - g_{K_0}(y)| \leq \sqrt[n]{n} |x - y|.$$

*Proof.* Since  $K_0 \subset C^n_0$  Proposition 3.2 yields

$$|g_K(x) - g_K(y)| \leq \max_{u \in S^{n-1}} b_{C^n_0}(u) |x - y|.$$

By Cauchy’s projection formula (5), for  $u = (u_1, u_2, \dots, u_n) \in S^{n-1}$  we have

$$b_{C^n_0}(u) = V \left( C^n_0 |u^\perp \right) = \prod_{i=1}^n |u_i|,$$

from which it is easy to see that  $b_{C^n_0}(u) \leq \sqrt[n]{n}$ . D

**3.4. Miscellaneous definitions.** Let  $\mu$  and  $\nu$  be finite nonnegative Borel measures in  $S^{n-1}$ . Define

$$(13) \quad d_P(\mu, \nu) = \inf \{ \varepsilon > 0 : \mu(E) \leq \nu(E_\varepsilon) + \varepsilon, \nu(E) \leq \mu(E_\varepsilon) + \varepsilon, E \text{ Borel in } S^{n-1} \},$$

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 (13) over the class of *closed* sets. In addition, if  $\mu(S^{n-1}) = \nu(S^{n-1})$ , then

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

see [17].

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  $0 < t \leq 2$ , let

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

be the closed 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

$$|\{ u_1, \dots, u_k \} \cap C_t(u)| \geq ck,$$

for all  $u \in S^{n-1}$  and  $k \geq N$ . 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  $(u_i)$ .

Let  $p \geq 1$ . A family  $\{X_\alpha : \alpha \in A\}$  of random variables has *uniformly bounded  $p$ th absolute moments* if there is a constant  $C$  such that

$$(15) \quad E(|X_\alpha|^p) \leq C,$$

for all  $\alpha \in A$ . Of course, if  $p$  is an even integer, we can and will omit the word “absolute”. If  $1 \leq q \leq p$  and (15) holds, then it also holds with  $p$  replaced by  $q$  and  $C$  replaced by  $C^{q/p}$ .

Triangular arrays of random variables of the form  $\{X_{ik} : i = 1, \dots, m_k; k \in \mathbb{N}\}$  (or, more generally,  $\{X_{\alpha k} : \alpha \in A_k; k \in \mathbb{N}\}$ ) are called *row-wise independent* if for each  $k$ , the family  $\{X_{ik} : i = 1, \dots, m_k\}$  (or  $\{X_{\alpha k} : \alpha \in A_k\}$ , respectively) is independent.

4. The main algorithm for reconstruction from covariograms

We shall assume throughout that the unknown convex body  $K_0$  is contained in the cube  $C_0^n = [-1/2, 1/2]^n$ , 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.

We now state the main, second-stage algorithm. Note that it requires, as part of the input, an  $o$ -symmetric convex polytope that approximates either the Blaschke body  $\nabla K_0$  or the difference body  $DK_0$  of  $K_0$ . These are provided by the first-stage algorithms, Algorithm NoisyCovBlaschke and Algorithm NoisyCovDiff( $\phi$ ), described in Sections 5 and 6, respectively.

The reader should be aware that here, and throughout the paper, double subscripts in expressions such as  $x_{ik}$ ,  $M_{ik}$ ,  $N_{ik}$ , etc., represent triangular arrays. Thus, for a fixed  $k$ , the index  $i$  varies over a finite set of integers that depends on  $k$ , and similarly when the first index is labeled by another letter in expressions such as  $z_{jk}$ ,  $X_{pk}$ , and so on, or is itself represented by a double index, as in  $N_{ijk}$ . Phrases such as “the  $N_{ik}$ ’s are row-wise independent” mean that the corresponding triangular array is row-wise independent, i.e., independent for fixed  $k$ .

**Algorithm NoisyCovLSQ**

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

$$(16) \quad M_{ik} = g_{K_0}(x_{ik}) + N_{ik},$$

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  $2C_0^n \cap (1/k)Z^n$ , where the  $N_{ik}$ ’s are row-wise independent zero mean random variables with uniformly bounded third absolute moments; an  $o$ -symmetric convex polytope  $Q_k$  in  $\mathbb{R}^n$ , stochastically independent of the measurements  $M_{ik}$ , that approximates either  $\nabla K_0$  or  $DK_0$ , in the sense that, almost surely,

$$(17) \quad \lim_{k \rightarrow \infty} \delta(\nabla K_0, Q_k) = 0, \quad \text{or} \quad \lim_{k \rightarrow \infty} \delta(DK_0, Q_k) = 0.$$

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

*Action:*

1. Compute the outer unit normals  $\{\pm u_j : j = 1, \dots, s\}$  to the facets 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  $P(a) = \hat{P}(a_1^+, a_1^-, a_2^+, a_2^-, \dots, a_s^+, a_s^-)$  be the convex polytope with centroid at the origin, facet outer unit normals in

$\{\pm u_j : j = 1, \dots, s\}$  and such that the facet with normal  $u_j$  (or  $-u_j$ ) has  $(n - 1)$ -dimensional measure  $q_j^+$  (or  $q_j^-$ , respectively),  $j = 1, \dots, s$ .

Solve the following least squares problem:

$$(18) \quad \min_{i=1}^{I_k} \left( M_{ik} - g_{P(a)} \cap C_0^n(x_{ik}) \right)^2$$

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

$$\sum_{j=1}^s (a_j^+ - a_j^-) u_j = 0$$

and

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

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  $q_j^+$  and  $q_j^-$ ,  $j = 1, \dots, s$ .

**Lemma 4.1.** *Let  $0 < r < R$  and let  $Q \in K^n(r, R)$  be an  $o$ -symmetric convex polytope. Then there are facets of  $Q$  with outer unit normals  $u_1, \dots, u_n$  such that*

$$(19) \quad |\det(u_1, \dots, u_n)| > (r/R)^{n(n-1)/2}.$$

*Proof.* The polar body  $Q^*$  of  $Q$  is contained in  $K^n(1/R, 1/r)$  and has its vertices in the directions of the outer unit 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  $u_i = v_i/|v_i|$ , (19) 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  $Q^* \in K^2(1/R, 1/r)$ , 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  $v_2 \cdot e_2 \geq 0$ . If  $\alpha$  is the angle between  $v_1$  and  $v_2$ , we must then have  $\theta \leq \alpha \leq \pi/2$ , where  $\theta$  is the angle between the vectors  $(0, 1/r)$  and  $(1/R, (1/r^2) - (1/R^2))$ . Then, if  $u_i = v_i/|v_i|$  for  $i = 1, 2$ , we have

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

which proves (19) for  $n = 2$ .

Suppose that (19) holds with  $n$  replaced by  $n - 1$  and let  $Q^* \in K^n(1/R, 1/r)$ . 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  $Q^*|_{e_n^\perp} \in K^{n-1}(1/R, 1/r)$  (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

$$(20) \quad |\det(z_2, \dots, z_n)| \geq (r/R)^{(n-1)(n-2)/2}.$$

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  $v_i \cdot e_n \geq 0$  for  $i = 2, \dots, n$ . Let  $\alpha_i$  be the angle between  $v_i$  and  $w_i$  for  $i = 2, \dots, n$ . Using the fact that  $Q^*|_{e_n^\perp} \in K^{n-1}(1/R, 1/r)$ , we see that each  $v_i$ ,  $i = 2, \dots, n$ , has distance at least  $1/R$  from the  $x_n$ -axis. Therefore  $\cos \alpha_i \geq \sin \theta = r/R$  for  $i = 2, \dots, n$ . Then,

using (20) 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

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

**Lemma 4.2.** *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*

$$(21) \quad d_P(S(K, \cdot), S(L, \cdot)) < \varepsilon.$$

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

*Proof.* Using (4) and (5), we obtain

$$(22) \quad |h_{\Pi K}(u) - h_{\Pi L}(u)| = |b_K(u) - b_L(u)| \leq d_D(S(K, \cdot), S(L, \cdot)).$$

Here  $d_D$  is the Dudley metric, defined by

$$d_D(\mu, \nu) = \sup_{S^{n-1}} \int f d(\mu - \nu) : f_{BL} \leq 1,$$

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

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

(Note that for any  $u \in S^{n-1}$ , the function  $f(v) = |u \cdot v|/2, v \in S^{n-1}$  satisfies  $f_{BL} = 1$ .) By [17, Corollary 2], we have the relation

$$(23) \quad d_D(\mu, \nu) \leq 2d_P(\mu, \nu),$$

for finite nonnegative Borel measures  $\mu$  and  $\nu$  in  $S^{n-1}$ . Now (22), (23), and (21) yield

$$|h_{\Pi K}(u) - h_{\Pi L}(u)| \leq 2d_P(S(K, \cdot), S(L, \cdot)) < 2\varepsilon,$$

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

Since  $K \in \mathcal{K}^n(r, R)$ , we have  $\Pi K \in \mathcal{K}^n(\kappa_{n-1} r^{n-1}, \kappa_{n-1} R^{n-1})$ , 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  $\varepsilon, r$ , and  $R$ , but we do not need them here.) D

**Lemma 4.3.** *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*

$$(24) \quad d_P(S(\nabla K, \cdot), S(Q, \cdot)) < \varepsilon$$

*or*

$$(25) \quad d_P(S(DK, \cdot), S(Q, \cdot)) < \varepsilon,$$



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

$$(26) \quad d_P(S(K, \cdot), S(J, \cdot)) < c_1 \varepsilon.$$

*Proof.* We choose  $\varepsilon_0 > 0$  so that Lemma 4.2 holds when  $\varepsilon$  is replaced by  $\varepsilon_0$  and  $K$  is replaced by either  $\nabla K$  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 (24) holds. By (13),  $S(\nabla K, E) < S(Q, E_\varepsilon) + \varepsilon$  for each Borel subset  $E$  of  $S^{n-1}$ . If  $E_\varepsilon \cap \bigcup_{i \in I} \{u_i\} = \emptyset$ , we have  $S(Q, E_\varepsilon) = 0$ . This implies that  $S(\nabla K, E) < \varepsilon$  and so by (3),

$$(27) \quad S(K, E) < 2\varepsilon.$$

If instead (25) holds, then (13) implies that  $S(DK, E) < S(Q, E_\varepsilon) + \varepsilon$  for each Borel subset  $E$  of  $S^{n-1}$ . Then, if  $E_\varepsilon \cap \bigcup_{i \in I} \{u_i\} = \emptyset$ , we have  $S(DK, E) < \varepsilon$ . By [46, (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 (27) holds again.

For  $i \in I$ , let

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

be the Voronoi cell in  $S^{n-1}$  containing  $u_i$ . Choose Borel sets  $W_i$  such that  $\text{relint } V_i \subset W_i \subset V_i$  for each  $i$  and  $W_i \cap W_j = \emptyset$  for  $i \neq j$ , 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, i.e.,

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

we have

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

For each  $u \in S^{n-1}$  and  $t > 0$ , let  $C_t(u) = \{v \in S^{n-1} : |u - v| \leq t\}$ . Let  $W = \bigcup_{i \in I} (W_i \setminus C_\varepsilon(u_i))$ . Then  $u_i \notin W_\varepsilon$  for  $i \in I$ , so (27) implies that  $S(K, W) < 2\varepsilon$ . Using this, we obtain

$$\begin{aligned} |w| &= \sum_{i \in I} \int_{W_i \cap C_\varepsilon(u_i)} (u_i - u) \, dS(K, u) + \sum_{i \in I} \int_{W_i \setminus C_\varepsilon(u_i)} (u_i - u) \, dS(K, u) \\ &\leq \sum_{i \in I} \int_{W_i \cap C_\varepsilon(u_i)} |u_i - u| \, dS(K, u) + 2 \int_W dS(K, u) \\ (28) \quad &< \varepsilon S(K, S^{n-1}) + 4\varepsilon = (S(K) + 4)\varepsilon. \end{aligned}$$

Since  $Q$  is  $o$ -symmetric, we can apply Lemma 4.2 (with  $K$  and  $L$  replaced by  $\nabla K$  (or  $DK$ ) and  $Q$ , respectively) and Lemma 4.1 to conclude that there exist outer unit normals  $u_{i_1}, \dots, u_{i_n}$  to facets of  $Q$  such that  $|\det(u_{i_1}, \dots, u_{i_n})|_n > c_2$ , where  $c_2$  depends only on  $K$ . In particular,  $u_{i_1}, \dots, u_{i_n}$  form a basis for  $\mathbb{R}^n$ , so there exist real numbers  $b_{i_1}, \dots, b_{i_n}$  such that

$$-w = \sum_{j=1}^n b_j u_j.$$

Replacing  $u_j$  by  $-u_j$ , if necessary, we may assume that  $b_j > 0$  for  $j = 1, \dots, n$ . By Cramer's rule, we obtain  $b_j \leq |w|/|\det(u_{i_1}, \dots, u_{i_n})| < |w|/c_2$ , 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 (28),

$$(29) \quad b_i \leq n|w|/c_2 < c_3\varepsilon, \quad i \in I$$

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  $\mu$  is not contained in a great sphere, and since

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

$\mu$  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 (26). Using (29), we obtain

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

where 0 is the zero measure in  $S^{n-1}$ . In view of  $\mu_0(S^{n-1}) = S(K, S^{n-1})$  and (14), it is therefore enough to find a constant  $c_4$ , depending only on  $K$ , such that

$$(30) \quad \mu_0(E) < S(K, E_{c_4\varepsilon}) + c_4\varepsilon,$$

for any Borel set  $E$  in  $S^{n-1}$ . Let  $X = \bigcup \{W_i : u_i \in E\} \not\equiv E_\varepsilon$ . We have

$$\begin{aligned} S(K, E_\varepsilon) &\geq S(K, E_\varepsilon \cap \bigcup \{W_i : u_i \in E\}) \\ (31) \quad &= \{S(K, W_i) : u_i \in E\} - S(K, X) = \mu_0(E) - S(K, X). \end{aligned}$$

If  $x \in X$ , then for some  $i$  with  $u_i \in E$  we have  $x \in W_i$ , and so  $|x - u_i| \geq \varepsilon$  since  $x \notin E_\varepsilon$ . Moreover, if  $j \neq i$ , then  $|u_j - x| \geq |u_i - x| \geq \varepsilon$ . Hence  $\bigcap_{i \in I} \{u_i\} \cap X_\varepsilon = \emptyset$ , and by (27), we have  $S(K, X) < 2\varepsilon$ . Now (31) implies that (30) holds with  $c_4 = 2$ . D

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

$$(32) \quad |f|_q = \left( \frac{1}{q} \sum_{i=1}^q f(z_i)^2 \right)^{1/2},$$

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

$$(33) \quad \Psi(K, \mathbf{z}_q, \mathbf{X}_q) = \sum_{i=1}^{q_1} g_K(z_i) X_i$$

**Lemma 4.4.** *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 (18). Then*

$$(34) \quad |g_{K_0} - g_{P_k}|_{I_k}^2 \leq 2\Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) - 2\Psi(P(a) \cap C_0^n, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) + |g_{K_0} - g_{P(a) \cap C_0^n}|_{I_k}^2,$$

where for each  $k \in \mathbb{N}$ ,  $|\cdot|_{I_k}$  and  $\Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k})$  are defined by (32) and (33), 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  $P(a) \cap C_0^n$  is a solution of (18), then since  $g_{P_k} = g_{P(a) \cap C_0^n}$ , we obtain

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

Substituting for  $M_{ik}$  from (16) and rearranging, we obtain

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

In view of (32) and (33), this is the required inequality. D

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

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

so the inner parallel body is convex. (It may be empty.) For further properties, see [46, 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

$$(35) \quad V(K) - V(K \mathcal{S} \varepsilon B^n) < S(K)\varepsilon.$$

This follows directly from either an inequality of Sangwine-Yager or one of Brannen; see Theorem 1 or Corollary 2 of [13], respectively. The estimate (35) 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 [39].

**Proposition 4.5.** *If  $K \subset C_0^n$  is a convex body and  $\varepsilon > 0$ , then*

$$V(K) - V(K \mathcal{S} \varepsilon B^n) < 2n\varepsilon.$$

Let  $G$  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  $g \in G$  and  $x \in \mathbb{R}^n$ ,  $g(x) \leq g_{C_0^n}(x) \leq V(C_0^n) = 1$ .

**Lemma 4.6.** *Let  $0 < \varepsilon < 1$  be given. Then there is a finite set  $\{(g_j^L, g_j^U) : j =$*

- (i) of pairs of functions in  $G$  such that  $g_j^U - g_j^L \leq \varepsilon$  for  $j = 1, \dots, m$  and*
- (ii) for each  $g \in G$ , there is a  $j \in \{1, \dots, m\}$  such that  $g_j^L \leq g \leq g_j^U$ .*

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

We first prove (ii). Let  $g \in G$ . There is a  $K \in K^n(C_0^n)$  such that  $g = g_K$ . Choose  $j \in \{1, \dots, m\}$  such that  $\delta(K, K_j) \leq \varepsilon/c_5$ . 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  $g_{K_j^L} = g_{K_j \ominus (\varepsilon/c_5)B^n} \subset g_K$ . These facts imply that  $g_j^L \leq g \leq g_j^U$ , as required.

It remains to prove (i). It is easy to prove (see, for example, [46, 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  $c_5 \geq 1$ , and Proposition 4.5 with  $\varepsilon$  replaced by  $\varepsilon/c_5$ , we obtain

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

provided that  $c_5$  is chosen sufficiently large. D

By analogy with [48, Definition 2.2], we refer to a finite set  $\{(g_j^L, g_j^U) : j = 1, \dots, m\}$  of pairs of functions in  $G$  satisfying (i) and (ii) of Lemma 4.6 as an  $\varepsilon$ -net with bracketing for the class  $G$ .

The following proposition is a version of the strong law of large numbers that applies to a triangular family, rather than a sequence, of random variables. A version with the assumptions of full independence and uniformly bounded fourth moments is proved in detail in [23, Lemma 4.4], with  $m_k = k$ . The stronger statement below follows directly from [30, Corollary 1] (with  $p = 1$  and  $n = m_k$

there); in fact, it is enough to assume the uniform boundedness of  $p$ th absolute moments where  $p = 2 + \varepsilon$  for some  $\varepsilon > 0$ , but we prefer to avoid this extra parameter in the sequel.

**Proposition 4.7.** *Let  $X_{ik}$ ,  $k \in \mathbb{N}$ ,  $i = 1, \dots, m_k$ , where  $m_k \geq k$ , be a triangular array of row-wise independent zero mean random variables. If the array has uniformly bounded third absolute moments, then, almost surely,*

$$(36) \quad \frac{1}{m^k} \sum_{i=1}^{m_k} X_{ik} \rightarrow 0$$

as  $k \rightarrow \infty$ .

**Lemma 4.8.** *For every  $k \in \mathbb{N}$ , let  $x_{ik}$ ,  $i = 1, \dots, I_k$ , be the points in the cubic array  $2C_0^n \cap (1/k)Z^n$ . Let  $N_{ik}$ ,  $k \in \mathbb{N}$ ,  $i = 1, \dots, I_k$ , be row-wise independent zero mean random variables with uniformly bounded third absolute moments. Then, almost surely,*

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

as  $k \rightarrow \infty$ , where for each  $k \in \mathbb{N}$ ,  $\Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k})$  is defined by (33) 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  $\varepsilon$ -net with bracketing, as provided by Lemma 4.6. Let  $K \in K^n(C_0^n)$  and let  $g = g_K \in G$ . Choose  $j \in \{1, \dots, m\}$  such that  $g_j^L \leq g \leq g_j^U$ . 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

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

where

$$(37) \quad W_k(\varepsilon) = \max_{j=1, \dots, m} \left( \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^U(x_{ik}) N_{ik}^+ - \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^L(x_{ik}) N_{ik}^- \right)$$

is independent of  $K$ . Consequently,

$$(38) \quad \sup_{K \in K^n(C_0^n)} \Psi(K, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) \leq W_k(\varepsilon),$$

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  $g_j^U(x_{ik}) \leq 1$ , it is easy to check that the random variables  $X_{ik}$  satisfy the hypotheses of Proposition 4.7. By (36) with  $m_k = I_k$ , we obtain, almost surely,

$$\limsup_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^U(x_{ik}) N_{ik}^+ = \limsup_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^U(x_{ik}) E(N_{ik}^+).$$

The same argument, with limits superior replaced by limits inferior, applies when  $X_{ik}$  is defined by  $X_{ik} = g_j^L(x_{ik})N_{ik}^- - g_j^L(x_{ik})E(N_{ik}^-)$ . Our moment assumption on the random variables  $N_{ik}$  implies that there is a constant  $C$  such that

$$E(N^+) = E(N^-) = \frac{1}{|N|} E(|N|) \leq C.$$

Also, by Lemma 4.6(i) we have  $g_j^U - g_j^L \leq \frac{\varepsilon}{2}$  and by Lemma 4.6(ii) we may assume that  $g_j^U - g_j^L \geq 0$ , for  $i = 1, \dots, m$ . Therefore, almost surely,

$$\begin{aligned} & \limsup_{k \rightarrow \infty} W_k(\varepsilon) \\ & \leq \max_{j=1, \dots, m} \left( \limsup_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^U(x_{ik}) E(N_{ik}^+) - \liminf_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^L(x_{ik}) E(N_{ik}^-) \right) \\ & \leq \max_{j=1, \dots, m} \left( C \limsup_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^U(x_{ik}) - \liminf_{k \rightarrow \infty} \frac{1}{I_k} \sum_{i=1}^{I_k} g_j^L(x_{ik}) \right) \\ & \leq \max_{j=1, \dots, m} \frac{C}{2^n} \int_{C_0^n} (g_j^U(x) - g_j^L(x)) dx \leq \frac{C\varepsilon}{2^n}. \end{aligned}$$

This and (38) complete the proof. D

**Lemma 4.9.** *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,*

$$(39) \quad \lim_{k \rightarrow \infty} |g_{K_0} - g_{P_k}|_{I_k} = 0.$$

*Proof.* Let  $Q_k$  be the  $o$ -symmetric polytope from the input of Algorithm NoisyCovLSQ that satisfies, almost surely, (17). Fix a realization for which (17) holds. We may assume that

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

as the other case is completely analogous. By [46, Theorem 4.2.1],  $S(Q_k, \cdot)$  converges weakly to  $S(\nabla K_0, \cdot)$  as  $k \rightarrow \infty$ . By [10, 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  $k \rightarrow \infty$ . Now Lemma 4.3 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  $k \rightarrow \infty$ . We may assume that the centroid of  $J_k$  is at the origin for each  $k$ . By Lemma 4.2 (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  $k \geq k_0$ . 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

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

(This consequence of the fact that  $d_P(S(K_0, \cdot), S(J_k, \cdot)) \rightarrow 0$  as  $k \rightarrow \infty$  can also be derived from a stability estimate of Hug and Schneider [31, Theorem 3.1], but



we do not need the full force of that result here.) It follows from the continuity of volume that  $g_{K_0} - g_{J_k \cap C_0^n} \rightarrow 0$  as  $k \rightarrow \infty$  and hence that

$$(40) \quad \lim_{k \rightarrow \infty} \int_{J_k \cap C_0^n} g_{K_0} - g_{J_k \cap C_0^n} = 0.$$

Next, we observe that  $J_k$  can serve as the  $P(a)$  in Lemma 4.4. 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 4.8 we obtain

$$(41) \quad \lim_{k \rightarrow \infty} \Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) = 0 \quad \text{and} \quad \lim_{k \rightarrow \infty} \Psi(J_k \cap C_0^n, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) = 0.$$

Now (39) follows directly from (34) (with  $P(a)$  replaced by  $J_k$ ), (40), and (41). D

**Theorem 4.10.** *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,*

$$(42) \quad \min\{\delta(K_0, P_k), \delta(-K_0, P_k)\} \rightarrow 0$$

as  $k \rightarrow \infty$ .

*Proof.* By Lemma 4.9, almost surely,

$$(43) \quad |g_{K_0} - g_{P_k}|_{I_k} \rightarrow 0,$$

as  $k \rightarrow \infty$ . 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 and be a translate of a subset of  $C_0^n$ .

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

$$g_{K_0} - g_{P_{k^l}}|_{I_{k^l}} \rightarrow \frac{1}{2^n} \int_{2C_0^n} (g_{K_0}(x) - g_L(x))^2 dx,$$

as  $k^l \rightarrow \infty$ . From this and (43), we obtain  $\|g_{K_0} - g_L\|_{L^2(2C_0^n)} = 0$ , and hence, since covariograms are clearly continuous,  $g_{K_0} = g_L$  on  $2C_0^n$ . As the supports of  $g_{K_0}$  and  $g_L$  are contained in  $2C_0^n$ , 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 (42). D

### 5. 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

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

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  $N_{ijk}^{(m)}$ ’s are row-wise independent (i.e., independent for fixed  $k$ ) zero mean random variables with uniformly bounded sixth moments.

*Task:* Construct an  $o$ -symmetric convex polytope  $Q_k$  that approximates the Blaschke body  $\nabla K_0$ .

*Action:*

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

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

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  $Q_k$ .

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

$$(44) \quad |f|_q = \left( \frac{1}{q} \sum_{i=1}^q f(u_i)^2 \right)^{1/2},$$

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

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

The same set of notation was used for a technically different pseudonorm and function  $\Psi$  in the previous section, but this should cause no confusion.

**Lemma 5.1.** *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*

$$(45) \quad |b_{K_0} - b_{Q_k}|_k \leq 2\Psi(Q_k, (u_i), \mathbf{X}_k) - 2\Psi(K_0, (u_i), \mathbf{X}_k) + \frac{c_6}{k} |b_{K_0} - b_{Q_k}|_k,$$

for all  $k \in \mathbb{N}$ . Here  $\mathbf{X}_k = (X_{1k}, \dots, X_{kk})$ , with

$$X_{ik} = \frac{1}{k^2} \sum_{j=1}^{k^2} (N_{ijk}^{(1)} - N_{ijk}^{(2)}),$$

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

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

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

say, where the  $X_{ik}$ 's are row-wise independent zero mean random variables. Note that the  $y_{ik}$ 's are also row-wise independent. Furthermore, by Khinchine's inequality (see, for example, [29, (4.32.1), p. 307] with  $\alpha = 6$ ), there is a constant  $C$  such that

$$E(|X_{ik}|^6) \leq \frac{C}{k^2} \sum_{j=1}^{k^2} E|N_{ijk}^{(1)} - N_{ijk}^{(2)}|^6,$$

from which we see that the  $X_{ik}$ 's also have uniformly bounded sixth moments. By Lemma 3.1,

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

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

$$b_{K_0}(u) \leq b_{\mathbb{G}^n}(u) \leq b_{(n/2)B^n}(u) = (n/4)^{(n-1)/2} \kappa_{n-1}$$

and

$$(46) \quad 0 \leq b_{K_0}(u) - \mu_{ik} \leq \frac{1}{1 - \frac{1}{2rk}^{n-1}} b_{K_0}(u) \leq \frac{n-1}{2rk} b_{K_0}(u), \quad k \geq 1/(2r),$$

by Lemma 3.1, so there is a constant  $c_7 = c_7(n, r)$  such that

$$(47) \quad 0 \leq b_{K_0}(u_i) - \mu_{ik} \leq \frac{c_7}{k},$$

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

By the formulation of Algorithms NoisyCovBlaschke and NoisyBrightLSQ (see [24, p. 1352] and take [24, Proposition 2.1] into account),  $Q_k$  minimizes

$$(48) \quad \sum_{i=1}^k (b_K(u_i) - y_{ik})^2$$

over the class of all  $o$ -symmetric convex bodies  $K$  in  $\mathbb{R}^n$ . By (7), 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 (48), we obtain

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

Rearranging and using (44), we obtain

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

The definition of  $\Psi$  and the Cauchy-Schwarz inequality yield

$$\begin{aligned} |b_{K_0} - b_{Q_k}|_k^2 &\leq 2\Psi(Q_k, (u_i), \mathbf{X}_k) - 2\Psi(K_0, (u_i), \mathbf{X}_k) \\ &\quad + 2|b_{K_0} - b_{Q_k}|_k \frac{1}{k} \sum_{i=1}^k (b_{K_0}(u_i) - \mu_{ik})^2. \end{aligned}$$

In view of (47), this proves (45) with  $c_6 = 2c_7$ . D

**Lemma 5.2.** *Suppose that the assumptions of Lemma 5.1 are satisfied with a sequence  $(u_i)$  such that  $(u_i^*)$  is evenly spread. Let  $C$  be a uniform upper bound for the second moments of the  $X_{ik}$ 's. Then, almost surely, there are constants  $c_8 = c_8(C, n, r, (u_i))$  and  $N_1 = N_1((X_{ik}), (u_i))$  such that*

$$(49) \quad S(Q_k) \leq c_8,$$

for all  $k \geq N_1$ .

*Proof.* By the Cauchy-Schwarz inequality,

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

This and (45) imply that

$$|b_{K_0} - b_{Q_k}|_k \leq 2 \sqrt{\frac{1}{k} \sum_{i=1}^k X_{ik}^2} + \frac{c_6}{k},$$

for all  $k \in \mathbb{N}$ . Since the  $X_{ik}$ 's have uniformly bounded sixth moments, we can apply Proposition 4.7 with  $m_k$  and  $X_{ik}$  replaced by  $k$  and  $X_{ik}^2 - E(X_{ik}^2)$ , respectively, to conclude that the first term on the right-hand side is bounded, almost surely. Thus, almost surely, there are constants  $c_9 = c_9(C, n, r)$  and  $N_2 = N_2((X_{ik}), (u_i))$  such that

$$(50) \quad |b_{K_0} - b_{Q_k}|_k \leq c_9,$$

for all  $k \geq N_2$ . As  $(u^*)$  is evenly spread, we can apply [24, Lemma 7.1] with  $K$  and  $L$  replaced by  $\Pi K_0$  and  $\Pi Q_k$ , respectively. Using this, the fact that  $\Pi K_0 \subset \Pi C^n = 2C^n \subset nB^n$  (see [20, p. 145]), and (4), we find that there are constants

$$(51) \quad b_{Q_k} \leq c_{10} |b_{K_0} - b_{Q_k}|_k + 2 \sqrt{\frac{1}{n}},$$

for  $k \geq N_3$ . Finally, (49) follows directly from (50), (51), and (6). D

**Lemma 5.3.** *Suppose that the assumptions of Lemma 5.1 are satisfied with a sequence  $(u_i)$  such that  $(u^*)$  is evenly spread. Then, almost surely,*

$$(52) \quad \lim_{k \rightarrow \infty} |b_{K_0} - b_{Q_k}|_k = 0.$$

*Proof.* Choose a constant  $C_1$  such that  $E(X_{ik}^2) \leq C_1$  for all  $i$  and  $k$ . Due to (45) and (50), there is, almost surely, a constant  $c_{11} = c_{11}(C_1, n, r)$  such that

$$(53) \quad |b_{K_0} - b_{Q_k}|_k \leq 2\Psi(Q_k, (u_i), \mathbf{X}_k) - 2\Psi(K_0, (u_i), \mathbf{X}_k) + \frac{c_{11}}{k},$$

for all  $k \geq N_2$ . By Proposition 4.7 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  $k \rightarrow \infty$ .

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

$$(54) \quad \lim_{k \rightarrow \infty} \sup_{K \in H_m} |\Psi(K, (u_i), \mathbf{X}_k)| = 0,$$

then by (49), almost surely,

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

This and (53) will yield (52), completing the proof.

To prove (54), note first that by (5), we have

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

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

$$(55) \quad \lim_{k \rightarrow \infty} \sup_{v \in S^{n-1}} \frac{1}{k} \sum_{i=1}^k |u_i \cdot v| X_{ik} = 0.$$

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. Indeed, suppose that (55) does not hold almost surely. Choose a constant  $C_2$  such that  $E(|X_{ik}|) \leq C_2$  for all  $i$  and  $k$ . Then there is a  $\delta > 0$  such that

$$(56) \quad \limsup_{k \rightarrow \infty} \sup_{v \in S^{n-1}} \frac{1}{k} \sum_{i=1}^k |u_i \cdot v| X_{ik} > \delta C_2$$

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

$$(57) \quad \frac{1}{k} \sum_{i=1}^k |u_i \cdot v_k| X_{ik} = \sup_{v \in S^{n-1}} \frac{1}{k} \sum_{i=1}^k |u_i \cdot v| X_{ik}.$$

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  $(k^l)$  of  $(k)$  such that  $|v_{k^l} - w_j| \leq \delta$  holds for sufficiently large  $k$ , we have, almost surely,

$$\limsup_{k^l \rightarrow \infty} \frac{1}{k^l} \sum_{i=1}^{k^l} |u_i \cdot v_{k^l}| X_{ik^l} - \frac{1}{k^l} \sum_{i=1}^{k^l} |u_i \cdot w_j| X_{ik^l} \leq \delta \limsup_{k^l \rightarrow \infty} \frac{1}{k^l} \sum_{i=1}^{k^l} |X_{ik^l}| \leq \delta C_2,$$

by Proposition 4.7 with  $m_k$  and  $X_{ik}$  replaced by  $k^l$  and  $|X_{ik^l}| - E(|X_{ik^l}|)$ , respectively. But Proposition 4.7, with  $m_k$  and  $X_{ik}$  replaced by  $k^l$  and  $|u_i \cdot w_j| X_{ik^l}$ , respectively, also implies that, almost surely, the second term on the left-hand side converges to zero, as  $k^l \rightarrow \infty$ . In view of (57), this yields

$$\limsup_{k^l \rightarrow \infty} \sup_{v \in S^{n-1}} \frac{1}{k^l} \sum_{i=1}^{k^l} |u_i \cdot v| X_{ik^l} \leq \delta C_2,$$

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 (56). D

**Theorem 5.4.** *Let  $K_0 \subset C^n$  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,*

$$(58) \quad \lim_{k \rightarrow \infty} \delta(\nabla K_0, Q_k) = 0.$$

*Proof.* We have  $o \in \text{int} K_0$ , so there is an  $r > 0$  such that  $rB^n \subset K_0$ . By Lemmas 5.2 and 5.3, we can fix a realization for which both (49) and (52) are true. Using (4), we observe that (52) is equivalent to

$$(59) \quad \lim_{k \rightarrow \infty} |h_{\Pi K_0} - h_{\Pi Q_k}|_k = 0.$$

We also have  $h_{\Pi Q_k} = b_{Q_k} \leq S(Q_k)$ , so by (49), the sets  $\Pi Q_k$  are uniformly bounded. With these observations and the fact that  $(u_1, -u_1, u_2, -u_2, \dots)$  is evenly spread,

we can follow the proof of [24, Theorem 6.1]), from the fourth line, with  $K$  and  $\hat{P}_k$  replaced by  $\Pi K_0$  and  $\Pi Q_k$ , respectively, to conclude that

$$(60) \quad \lim_{k \rightarrow \infty} \delta(\Pi K_0, \Pi Q_k) = 0.$$

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  $t = \sqrt[n]{nr}$ .

Moreover, (4) and (7) give  $\Pi(\nabla K_0) = \Pi K_0$ . Hence (60) 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 (58) follows from (60) and the Bourgain-Campi-Lindenstrauss stability result for projection bodies (see [11] and [16], or [20, Remark 4.3.13]). D

### 6. Approximating the difference body via the covariogram

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

#### Algorithm NoisyCovDiff( $\phi$ )

*Input:* Natural numbers  $n \geq 2$  and  $k$ ; positive reals  $\delta_k$  and  $\varepsilon_k$ ; noisy covariogram measurements

$$(61) \quad M_{ik} = g_{K_0}(x_{ik}) + N_{ik},$$

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  $2C_0^n \cap (1/k)Z^n$ , where the  $N_{ik}$ 's are row-wise independent zero mean random variables with uniformly bounded fourth moments.

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

*Action:*

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

$$(62) \quad g_k(x) = \frac{1}{I_k} \sum_{i=1}^{I_k} M_{ik} \int_{(1/k)C_0^n + x_{ik}} \phi_{\varepsilon_k}(x - z) dz = \frac{1}{I_k} \sum_{i=1}^{I_k} M_{ik} 1_{(1/k)C_0^n + x_{ik}} \cdot \phi_{\varepsilon_k}(x).$$

2. Define the finite set

$$(63) \quad S_k = \{x \in 2C_0^n \cap (1/k)Z^n : g_k(x) \geq \delta_k\}.$$

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

The input  $\delta_k$  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  $\phi$  and bandwidth  $\varepsilon_k$ . 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  $\varepsilon_k \rightarrow 0$  as  $k \rightarrow \infty$ . We shall show that this holds uniformly in  $x$ .

**Lemma 6.1.** *Suppose that  $K_0$ ,  $\varepsilon_k$ , and  $g_k$  are as in Algorithm NoisyCovDiff( $\phi$ ). For each  $k \in \mathbb{N}$  and  $x \in \mathbb{R}^n$ ,*

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

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

*Proof.* Using (61), (62), and the definition of  $\phi_{\varepsilon_k}$ , we obtain

$$(64) \quad |E(g_k(x)) - g_{K_0}(x)| \leq \sum_{i=1}^{I_k} \int_{(1/k)C_0^n + x_{ik}} \phi_{\varepsilon_k}(x - z) dz,$$

for all  $x \in \mathbb{R}^n$ . The support of  $\phi_{\varepsilon_k}$  is contained in  $\varepsilon_k C_0^n$ , so for fixed  $x$ , the support then  $\varepsilon_k C_0^n + x$  and  $(1/k)C_0^n + x_{ik}$  are disjoint, so the corresponding summand in (64) vanishes. Moreover, for  $x_{ik} \in (\varepsilon_k + 1/k)C_0^n + x$ , Corollary 3.3 and the fact that the diameter of  $C_0^n$  is  $\sqrt{n}$  imply that

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

Consequently,

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

as required. D

In [3, Lemma 1], a polynomial rate of convergence result in the weak sense is established for independent identically distributed measurement errors with polynomial tails. In contrast, we assume only uniformly bounded fourth moments and obtain a convergence rate that holds uniformly, using the Lipschitz continuity of the covariogram.

**Lemma 6.2.** *Suppose that  $K_0$ ,  $\varepsilon_k$ , and  $g_k$  are as in Algorithm NoisyCovDiff( $\phi$ ) and let  $\delta > 0$  and  $\lim_{k \rightarrow \infty} \varepsilon_k = 0$ . Then there are constants  $c_{12} = c_{12}(\phi)$  and  $N_4 = N_4((\varepsilon_k), n) \in \mathbb{N}$  such that*

$$(65) \quad \Pr(|g_k(x) - g_{K_0}(x)| > \delta) \leq c_{12}(2k + 1)^n \delta^{-4} (k\varepsilon_k)^{-3n},$$

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

*Proof.* Let  $x \in \mathbb{R}^n$  and  $k \in \mathbb{N}$  be fixed and define

$$(66) \quad \beta_{ik} = \beta_{ik}(x) = \int_{(1/k)C_0^n + x_{ik}} \phi_{\varepsilon_k}(x - z) dz,$$

for  $i = 1, \dots, I_k$ . Then

$$(67) \quad \beta_{ik} \leq \phi_{\varepsilon_k} \otimes V((1/k)C_0^n) = \phi_{\infty}(k\varepsilon_k)^{-n}$$

and

$$(68) \quad \sum_{i=1}^{I_k} \int_{\mathbb{R}^n} \phi_{\varepsilon_k}(x - z) dz = 1.$$

In view of (61), (62), and (66),

$$g_k(x) - E(g_k(x)) = \sum_{i=1}^{I_k} \beta_{ik} N_{ik}$$

is a sum of zero mean independent random variables. The assumption that the  $N_{ik}$ 's have uniformly bounded fourth moments implies that  $E(|N_{ik}|^4) \leq C$  for some constant  $C$  and all  $i$  and  $k$ . Now, using Markov's inequality, Khinchine's inequality (see, for example, [29, (4.32.1), p. 307] with  $\alpha = 4$ ), (67), and (68), we obtain

$$\begin{aligned} \Pr(|g_k(x) - E(g_k(x))| \geq \delta/2) &\leq (\delta/2)^{-4} E \left( \sum_{i=1}^{I_k} \beta_{ik} N_{ik} \right)^4 \\ &\leq c \delta^{-4} E \sum_{i=1}^{I_k} |\beta_{ik} N_{ik}|^4 \\ &\leq c C \delta^{-4} \sum_{i=1}^{I_k} \beta_{ik}^4 \\ &\leq c C \delta^{-4} \sum_{i=1}^{I_k} \left( \phi_{\infty}(k\varepsilon_k) \right)^{-3} \beta_{ik} \\ (69) \qquad \qquad \qquad &\leq c_{12} (2k+1)^n \delta^{-4} (k\varepsilon_k)^{-3n}, \end{aligned}$$

for all  $\delta > 0$ , where  $c$  is a constant and  $c_{12} = cC \phi_{\infty}^{-3}$ . By Lemma 6.1, there is a constant  $N_4 = N_4((\varepsilon_k), n) \in \mathbb{N}$  such that for all  $k \geq N_4$  and  $x \in \mathbb{R}^n$ , we have  $|E(g_k(x)) - g_{K_0}(x)| \leq \delta/2$  and therefore

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

Now (65) follows from this and (69). D

For a convex body  $K$  in  $\mathbb{R}^n$  and  $\delta > 0$ , let  $K(\delta) = \{x \in \mathbb{R}^n : g_K(x) \geq \delta\}$ . Since  $g_K$  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 6.3.** *Let  $K$  be a convex body in  $\mathbb{R}^n$ . If  $0 < \delta < V(K)$ , then*

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

*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  $x \in K(\delta)$ . D

**Theorem 6.4.** *Suppose that  $K_0, \delta_k, \varepsilon_k$ , and  $g_k$  are as in Algorithm NoisyCovDiff( $\phi$ ).*

*Assume that  $\lim_{k \rightarrow \infty} \varepsilon_k = \lim_{k \rightarrow \infty} \delta_k = 0$  and that*

$$(70) \quad \liminf_{k \rightarrow \infty} \delta_k^4 \varepsilon_k^{3n} k^{n-3/2} > 0.$$

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

$$(71) \quad \delta(DK_0, Q_k) \leq c_{13} \delta_k^{1/n},$$

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

*Proof.* Let

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

By Lemma 6.2 and (70), we have

$$\begin{aligned} \Pr(a_k \geq \delta_k) &\leq \Pr(|g_k(x) - g_{K_0}(x)| \geq \delta_k) \\ &\leq c_{12} (2k+1)^{2n} \delta^{-4} (k\varepsilon_k)^{-3n} = O\left(\frac{1}{k^{3/2}}\right). \end{aligned}$$

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

$$(72) \quad \frac{2\delta_k}{V(K_0)}^{1/n} + \frac{3}{s(K_0)k} \leq 1,$$

where  $s(K_0) = \max\{\rho \geq 0 : \rho C_0^n \subset DK_0\}$ . As  $a_k < \delta_k$ , the definition (63) of  $S_k$  implies

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

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

$$(73) \quad \text{conv} \left( K_0(2\delta_k) \cap \frac{1}{k}Z^n \right) \subset Q_k \subset DK_0.$$

We claim that

$$(74) \quad K_0(2\delta_k) \mathcal{S} \frac{3}{k}C_0 \subset \text{conv} \left( K_0(2\delta_k) \cap \frac{1}{k}Z^n \right),$$

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

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

As the vertices of  $(1/k)(2C_0^n) + y$  are in  $(1/k)Z^n$ , we have  $x \in \text{conv}(K_0(2\delta_k) \cap (1/k)Z^n)$ , 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, (72), Lemma 6.3 (with  $\delta = 2\delta_k$ ), and the definition of  $s(K_0)$  imply that

$$1 - t_k + \frac{3}{s(K_0)k} DK_0 = (1 - t_k) DK_0 \mathcal{S} \frac{3}{s(K_0)k} DK_0 \subset K_0(2\delta_k) \mathcal{S} \frac{3}{k}C_0.$$

From this, (74), and (73), we obtain

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

As  $DK_0 \subset \sqrt[n]{nB^n}$ , this yields

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

By (70),  $k\delta_k^{1/n} \rightarrow \infty$  as  $k \rightarrow \infty$ , and (71) follows. D

The estimate (71) reveals that the rate of convergence of  $Q_k$  to  $DK_0$  depends on the asymptotic behavior of the threshold parameter  $\delta_k$ , which is linked to the bandwidth  $\varepsilon_k$  by (70). If we assume that  $V(K_0)$  is bounded from below by a known constant, then  $c_{13}$  in the statement of Theorem 6.4 can be chosen independent of  $K_0$ . We note the resulting rate of convergence as a corollary, where we choose  $\varepsilon_k$  and  $\delta_k$  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  $1/4 - 3/(8n)$ .

**Corollary 6.5.** *Suppose  $K_0$ ,  $\delta_k$ ,  $\varepsilon_k$ , and  $g_k$  are as in Algorithm NoisyCovDiff( $\phi$ ). Let  $0 < b < V(K_0)$ , let  $\delta_k = k^{-(n-3an-3/2)/4}$ , and let  $\varepsilon_k = k^{-a}$ , for some  $0 < a < 1/3 - 1/(2n)$ . If  $Q_k$  is an output from Algorithm NoisyCovDiff( $\phi$ ) as stated above, then, almost surely,*

$$\delta(DK_0, Q_k) \leq \sqrt[n]{\frac{2}{b}} \frac{1}{k^{(1-3a-3/(2n))/4}},$$

for sufficiently large  $k$ .

*Remark 6.6.* Here we outline how a stronger assumption, but one that still applies to all the noise models of practical interest, on the random variables in Algorithm NoisyCovDiff( $\phi$ ) leads to a better convergence rate in Corollary 6.5.

Consider a family  $\{X_\alpha : \alpha \in A\}$  of zero mean random variables with variances  $\sigma_\alpha^2$  that satisfy the hypothesis of Bernstein’s inequality (see [14, Theorem 5.2, p. 27] or [49, Lemma 2.2.11]), that is,

$$(75) \quad |E(X^m)| \leq \frac{m!}{2^a} \sigma^2 H^{m-2},$$

for some  $H > 0$  and all  $\alpha \in A$  and  $m = 2, 3, \dots$ , and also have uniformly bounded variances, that is,

$$(76) \quad \sigma_\alpha^2 \leq \sigma^2,$$

say, for all  $\alpha \in A$ . If the family  $\{X_1, \dots, X_r\}$  of independent zero mean random variables satisfies (75) with  $A = \{1, \dots, r\}$ , then Bernstein’s inequality states that

$$\Pr \left( \sum_{i=1}^r X_i \geq \delta \right) \leq 2 \exp \left( - \frac{\delta^2}{2(\delta H + \sum_{i=1}^r \sigma_i^2)} \right),$$

for all  $\delta > 0$ .

Suppose that the random variables  $N_{ik}$  in Algorithm NoisyCovDiff( $\phi$ ) are row-wise independent, zero mean, and satisfy (75) and (76). Then Bernstein’s inequality

can be applied in the proof of Lemma 6.2, together with (67) and (68), to show that

$$(77) \quad \Pr(|g_k(x) - E(g_k(x))| \geq \delta/2) \leq 2 \exp \left[ -\frac{\delta^2(k\varepsilon_k)^n}{4 \phi_\infty (\delta H + 2\sigma^2)} \right],$$

for all  $\delta > 0$ . (Compare the weaker upper bound in (69).) As at the end of the proof of Lemma 6.2, this results in the same upper bound for  $\Pr(|g_k(x) - g_{K_0}(x)| > \delta)$ .

The improved bound (77), combined with the argument of Theorem 6.4, leads to the assumption

$$(78) \quad \liminf_{k \rightarrow \infty} \frac{\delta_k^2(k\varepsilon_k)^n}{\log k} > c_{14}(n+2),$$

where  $c_{14} = 12 \phi_\infty \sigma^2$ , instead of (70). In Corollary 6.5 we take instead  $\delta_k = k^{-n(1-\alpha)/2} \log k$  and  $\varepsilon_k = k^{-\alpha}$ , for some  $0 < \alpha < 1$ . The final conclusion is that if  $Q_k$  is an output from Algorithm NoisyCovDiff( $\phi$ ), then, almost surely,

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

for sufficiently large  $k$ . In particular, a convergence rate of  $k^{-p}$  can be attained, where  $p$  is arbitrarily close to  $1/2$ .

Note that families of zero mean Gaussian and centered Poisson random variables satisfy (75) and (76). Also, if two independent families with the same index set satisfy (75) and (76), the same is true for their sums (with possibly different constants  $H$  and  $\sigma^2$ ).

### 7. 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

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

Let

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

If  $g$  is also Lipschitz, then by [35, Theorem 3], the square partial sums

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

of the Fourier series of  $g$  converge uniformly to  $g$ . Therefore, if  $g$  is also an even function, we can write

$$(79) \quad g(x) = \frac{1}{(2L)^n} \sum_{z \in \mathbb{Z}^n} \hat{g}(\pi z/L) e^{i\pi z \cdot x/L} = \frac{1}{(2L)^n} \sum_{z \in \mathbb{Z}^n} \hat{g}(\pi z/L) \cos \frac{\pi z \cdot x}{L},$$

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

Let  $Z^n(+)$  be a subset of  $Z^n$  such that

$$(80) \quad Z^n_k(+) \cap (-Z^n_k(+)) = \emptyset \quad \text{and} \quad Z^n_k = \{o\} \cup Z^n_k(+) \cup (-Z^n_k(+)).$$

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

$$(81) \quad g_{z,k} = g(z/k^Y) + X_{z,k},$$

for  $z \in \{o\} \cup Z^n_k(+)$ , where the  $X_{z,k}$  s are row-wise independent (i.e., independent for fixed  $k$ ) zero mean random variables. Define  $X_{z,k} = X_{-z,k}$ , for  $z \in (-Z^n_k(+))$  and note that then  $X_{z,k} = X_{-z,k}$  for all  $z \in Z^n_k$ . Since  $g$  is even,  $g_{z,k} = g_{-z,k}$  for  $z \in Z^n_k$ . Using these facts, (79) with  $L = \pi k^Y$ , and (81), we obtain

$$(82) \quad \frac{1}{(2\pi k^Y)^n} \sum_{z \in Z^n_k} g_{z,k} \cos \frac{z \cdot x}{k^Y} = g(x) + \frac{1}{(2\pi k^Y)^n} \left( \sum_{z \in Z^n_k} X_{z,k} \cos \frac{z \cdot x}{k^Y} - \sum_{z \in Z^n \setminus Z^n_k} g_{z,k} \cos \frac{z \cdot x}{k^Y} \right),$$

for all  $x \in [-\pi k^Y, \pi k^Y]^n$ . Here the left-hand side is an estimate of  $g(x)$  and the second and third terms on the right-hand side are a random error and a deterministic error, respectively.

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  $C^n_\theta$  in which case  $g_{K_0} = |1_{K_0}|^2$ . In order to move closer to the notation used earlier, we now use  $i$  as an index and again list the points in  $[-1, 1]^n \cap (1/k)Z^n = (1/k)Z^n_k$  but this time a little differently. We let  $x_{0k} = o$ , list the points in  $(1/k)Z^n_k(+)$  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  $z_{ik} = k^{1-Y}x_{ik}$ , so that

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

Setting  $g_{jk} = g_{K_0, z_{jk}, k}$  and  $X_{jk} = X_{z_{jk}, k}$ , we use (81) to rewrite (82) as

$$(83) \quad M_k(x) = g_{K_0}(x) + N_k(x) - d_k(x),$$

where

$$(84) \quad M_k(x) = \frac{1}{(2\pi k^Y)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x) g_{jk}$$

is an estimate of  $g_{K_0}$ ,

$$(85) \quad N_k(x) = \frac{1}{(2\pi k^Y)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x) X_{jk}$$

is a random variable, and

$$(86) \quad d_k(x) = \frac{1}{(2\pi k^Y)^n} \sum_{z \in Z^n \setminus Z^n_k} \cos \frac{z \cdot x}{k^Y} g_{K_0}(z/k^Y)$$

is a deterministic error.

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

**Lemma 7.1.** *Let  $d_k = \sup\{|d_k(x)| : x \in \mathbb{R}^n\}$ . Then  $d_k = O(k^{Y-1}(\log k)^n)$  as  $k \rightarrow \infty$ .*

*Proof.* From (86), the fact that  $g_{K_0} = |1_{K_0}|^2$  is nonnegative, and (79) with  $g = g_{K_0}$  and  $L = \pi k^Y$ , we have

$$(87) \quad d_k \leq \frac{1}{(2\pi k^Y)^n} \int_{z \in \mathbb{Z}_k^n \setminus \mathbb{Z}_k^n} g_{K_0}(z/k^Y) = g_{K_0}(o) - \frac{1}{(2\pi k^Y)^n} \int_{z \in \mathbb{Z}_k^n} g_{K_0}(z/k^Y).$$

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

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

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

$$e^{iz \cdot x} = \prod_{l=1}^n e^{im_l x_l} = \prod_{l=1}^n D_k(x_l).$$

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

$$(88) \quad \begin{aligned} \frac{1}{(2\pi k^Y)^n} \int_{z \in \mathbb{Z}_k^n} g_{K_0}(z/k^Y) &= \frac{1}{(2\pi k^Y)^n} \int_{z \in \mathbb{Z}_k^n} \int_{[-\pi k^Y, \pi k^Y]^n} g_{K_0}(x) e^{-iz \cdot x/k^Y} dx \\ &= \frac{1}{(2\pi k^Y)^n} \int_{[-\pi k^Y, \pi k^Y]^n} g_{K_0}(x) \prod_{l=1}^n D_k(-x_l/k^Y) dx \\ &= \frac{1}{(2\pi)^n} \int_{[-1, 1]^n} g_{K_0}(y k^Y) \prod_{l=1}^n D_k(y_l) dy. \end{aligned}$$

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

$$(89) \quad g_{K_0}(o) = \frac{1}{(2\pi)^n} \int_{[-\pi, \pi]^n} g_{K_0}(o) \prod_{l=1}^n D_k(y_l) dy.$$

Thus, by (87), (88), and (89),

$$(90) \quad \begin{aligned} d_k &\leq \frac{1}{(2\pi)^n} \int_{[-1, 1]^n} (g_{K_0}(o) - g_{K_0}(y k^Y)) \prod_{l=1}^n D_k(y_l) dy \\ &+ \frac{g_{K_0}(o)}{(2\pi)^n} \int_{[-\pi, \pi]^n \setminus [-1, 1]^n} \prod_{l=1}^n D_k(y_l) dy. \end{aligned}$$

By Proposition 3.2,  $g_{K_0}$  is Lipschitz and hence the Lipschitz norm of  $g_{K_0}(y k^Y)$  is  $O(k^Y)$ . Now [35, Theorem 1] implies that

$$(91) \quad \frac{1}{(2\pi)^n} \int_{[-1, 1]^n} (g_{K_0}(o) - g_{K_0}(y k^Y)) \prod_{l=1}^n D_k(y_l) dy \leq c k^{Y-1} (\log k)^{n-1}$$

for some constant  $c_{15}$  independent of  $k$ . (In the statement of [35, 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 (90) and (91), the proof will be complete if we show that

$$(92) \quad \int_{[-\pi, \pi]^n \setminus [-1, 1]^n} \prod_{l=1}^n D_k(x_l) dx = O(1/k),$$



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

$$\begin{aligned} \int_{-\pi}^{-1} D_k(t) dt &= \int_1^\pi D_k(t) dt = \int_1^\pi \frac{\sin(kt) \cos(t/2)}{\cos k \cot(1/2)} dt + \int_1^\pi \cos(kt) dt \\ &= \frac{\sin(t/2)}{k} \Big|_1^\pi + \int_1^\pi \frac{\cos(kt)}{k} d(\cot(t/2)) dt - \frac{\sin k}{k} \\ (93) \qquad &= O(1/k). \end{aligned}$$

Now

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

where

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

and  $B_i = -A_i$ . By (93), we have, for each  $i$ ,

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

Since  $\text{int}(A_i) \cap \text{int}(A_j) = \emptyset$ , for each  $i, j$  with  $i \neq j$ ,  $\text{int}(A_i) \cap \text{int}(B_j) = \emptyset$ , for each  $i, j$ , and  $\int_{\prod_{l=1}^n D_k(x_l)}$  is even, the previous estimate proves (92). D

It is possible that the previous lemma could also be obtained via some estimates proved in [12] for the rate of decay of  $\int_{S^{n-1}} |1_{K_0}(ru)|^2 du$  as  $r \rightarrow \infty$ .

The next two lemmas will allow us to circumvent Proposition 4.7, the version of the Strong Law of Large Numbers used earlier.

**Lemma 7.2.** *Let  $Y_{jk}$ ,  $j = 1, \dots, m_k$ ,  $k \in \mathbb{N}$ , be a triangular array of row-wise independent zero mean random variables with uniformly bounded fourth moments, where  $m_k \sim k^n$  as  $k \rightarrow \infty$ . Let  $v$  and  $a_{pqk}$ ,  $p, q = 1, \dots, m_k$ , be constants such that  $|a_{pqk}| = O(k^v)$  as  $k \rightarrow \infty$  uniformly in  $p$  and  $q$ , where  $2n - 4n\gamma + 2v < -1$ . Then, almost surely,*

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

as  $k \rightarrow \infty$ .

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

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

Since the  $Y_{pk}$ 's have uniformly bounded second moments,  $|E(Z_k)| = O(k^{n-2n\gamma+v})$  and hence  $E(Z_k)$  converges to zero as  $k \rightarrow \infty$ .

Let

$$v_{\{p,q,r,s\}} = \text{cov}(Y_{pk} Y_{qk}, Y_{rk} Y_{sk}) = E(Y_{pk} Y_{qk} Y_{rk} Y_{sk}) - E(Y_{pk} Y_{qk}) E(Y_{rk} Y_{sk}).$$

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

$$v_{\{p,q,r,s\}} = E(Y_{pk}) E(Y_{qk} Y_{rk} Y_{sk}) - E(Y_{pk}) E(Y_{qk}) E(Y_{rk} Y_{sk}) = 0 - 0 = 0.$$

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

$$v_{pqrs}^{(k)} = v_{pppp}^{(k)} = E(Y_{pk}^4) - E(Y_{pk}^2)^2.$$

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

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

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

$$v_{pqrs}^{(k)} = v_{ppqq}^{(k)} = E(Y_{pk}^2 Y_{qk}^2) - E(Y_{pk} Y_{qk})^2 = E(Y_{pk}^2) E(Y_{qk}^2) - E(Y_{pk})^2 E(Y_{qk})^2,$$

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

$$v_{pqrs}^{(k)} = v_{ppqq}^{(k)} = E(Y_{pk}^2 Y_{qk}^2) - E(Y_{pk} Y_{qk})^2 = E(Y_{pk}^2) E(Y_{qk}^2) - E(Y_{pk})^2 E(Y_{qk})^2.$$

In view of the fact that the  $Y_{jk}$ 's have uniformly bounded fourth moments, the covariances  $v_{pqrs}^{(k)}$  are also uniformly bounded, and hence

$$\begin{aligned} \text{var}(Z_k) &= \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{p,q,r,s=1}^{m_k} a_{pqk} a_{rsk} v_{pqrs}^{(k)} \\ &= \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{p=1}^{m_k} a_{ppk}^2 v_{pppp}^{(k)} + \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{\substack{p=q=1 \\ p \neq q}}^{m_k} a_{pqk}^2 v_{ppqq}^{(k)} + \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{\substack{p=q=1 \\ p \neq q}}^{m_k} a_{pqk} a_{qp k} v_{ppqq}^{(k)} \\ &= O(k^{2n-4n\gamma+2\nu}). \end{aligned}$$

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

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

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

**Lemma 7.3.** *Let  $Y_{jk}^{(r)}$ ,  $j = 1, \dots, m_k$ ,  $r = 1, 2$ ,  $k \in \mathbb{N}$ , be a triangular array of row-wise independent (i.e., independent for fixed  $k$ ) zero mean random variables with uniformly bounded fourth moments, where  $m_k \sim k^n$  as  $k \rightarrow \infty$ . Let  $\nu$  and  $a_{pqk}$ ,  $p, q = 1, \dots, m_k$ , be constants such that  $|a_{pqk}| = O(k^\nu)$  as  $k \rightarrow \infty$  uniformly in  $p$  and  $q$ , where  $2n - 4n\gamma + 2\nu < -1$ . Then, almost surely,*

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

as  $k \rightarrow \infty$ .

*Proof.* As in the proof of Lemma 7.2, we have

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

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

Let

$$w_{pqrs}^{(k)} = \text{COV} \left( Y_{pk}^{(1)}, Y_{pk}^{(2)}, Y_{qk}^{(1)}, Y_{qk}^{(2)}, Y_{rk}^{(1)}, Y_{rk}^{(2)}, Y_{sk}^{(1)}, Y_{sk}^{(2)} \right).$$

Straightforward modifications to the proof of Lemma 7.2 and the assumption of uniformly bounded fourth moments yield

$$\begin{aligned} \text{var}(\bar{Z}_k) &= \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{p,q,r,s=1}^{m_k} a_{pqk} a_{rsk} w_{pqrs}^{(k)} \\ &= \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{p=1}^{m_k} a_{ppk}^2 w_{pppp}^{(k)} + \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{\substack{p/q= \\ 1}}^{m_k} a_{pqk}^2 w_{ppqq}^{(k)} + \frac{1}{(2\pi k^\gamma)^{4n}} \sum_{\substack{p/q= \\ 1}}^{m_k} a_{pqk} a_{qpq} w_{ppqq}^{(k)} \\ &= O(k^{2n-4n\gamma+2\nu}). \end{aligned}$$

The proof is concluded as in Lemma 7.2. D

### 8. Phase retrieval from the squared modulus

This section addresses Problem 2 in the Introduction.

#### Algorithm NoisyMod<sup>2</sup>LSQ

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

$$(94) \quad g_{ik} = |1^{K_0}(z^{ik})|^2 + X_{ik},$$

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

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

where  $Z_k^n(+)$  satisfies (80) and where the  $X_{ik}$ 's are row-wise independent zero mean random variables with uniformly bounded fourth moments; an  $o$ -symmetric convex polytope  $Q_k$  in  $R^n$ , stochastically independent of the measurements  $g_{ik}$  that approximates either  $\nabla K_0$  or  $DK$ , in the sense that, almost surely,

$$\lim_{k \rightarrow \infty} \delta(\nabla K_0, Q_k) = 0, \quad \text{or} \quad \lim_{k \rightarrow \infty} \delta(DK_0, Q_k) = 0.$$

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

*Action:* Let  $g_{ik} = g_{(-i)k}$ , 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  $2C_0^n \cap (1/k)Z_k^n$ , and let

$$(95) \quad M_k(x_{ik}) = \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x_{ik}) g_{jk},$$

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 4.10 above. We first state it and then show that it can be proved by suitable modifications to the proof of Theorem 4.10 if in addition  $\gamma > 1/2 + 1/(4n)$ .

**Theorem 8.1.** *Suppose that  $K_0 \subset C^n_0$  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  $R^n$ , by its covariogram. Let*

$$(96) \quad 1/2 + 1/(4n) < \gamma < 1.$$

*If  $P_k, k \in N$ , is an output from Algorithm NoisyMod<sup>2</sup>LSQ as stated above, then, almost surely,*

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

*as  $k \rightarrow \infty$ .*

As we shall now show, the proof of this theorem basically follows the analysis given in Section 4. 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 (95) or equivalently by (84) with  $x = x_{ik}$ . In view of (83), 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 (85) and (86), 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  $X_{ik}$  have uniformly bounded fourth moments, and  $X_{pk}$  and  $X_{qk}$  are independent unless  $p = \pm q$ , in which case they are equal.

**Lemma 8.2.** *Let  $N_k(x_{ik})^+ = \max\{N_k(x_{ik}), 0\}$  for all  $i$  and  $k$ . If (96) holds, then, almost surely,*

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

*as  $k \rightarrow \infty$ .*

*Proof.* Note firstly that

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

Thus it suffices to prove that, almost surely,

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

*as  $k \rightarrow \infty$ .*

We have

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

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

$$\frac{1}{(2\pi k^V)^{2n}} \sum_{p,q=1}^{I_k^t} c_{pqk} X_{pk} X_{qk} \rightarrow 0,$$

as  $k \rightarrow \infty$ . In view of (96) and the fact that  $|c_{pqk}| = O(1)$ , this follows from Lemma 7.2 with  $Y_{jk} = X_{jk}$ ,  $m_k = I_k^t a_{pqk} = c_{pqk}$  for all  $p, q$ , and  $k$ , and  $v = 0$ .  $\square$

*Proof of Theorem 8.1.* We shall indicate the modifications needed in Section 4. No changes are required in the lemmas before Lemma 4.4. 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 4. Thus we write

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

with corresponding changes in indexing in the definitions of  $\mathbf{x}_{I_k}$ ,  $\mathbf{N}_{I_k}$  and  $\Psi$ . With the same proof as Lemma 4.4, we now have the inequality

$$\begin{aligned}
 |g_{K_0} - g_{P_k}|_{I_k}^2 &\leq 2\Psi(P_k, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) - 2\Psi(P(a) \cap C_0^n, \mathbf{x}_{I_k}, \mathbf{N}_{I_k}) + |g_{K_0} - g_{P(a) \cap C_0^n}|_{I_k}^2 \\
 (97) \quad &\frac{1}{I_k} \sum_{i=-I_k^t}^{I_k^t} \left( g_{P(a) \cap C_0^n}(x_{ik}) - g_{P_k}(x_{ik}) \right) d_k(x_{ik}),
 \end{aligned}$$

instead of (34).

Proposition 4.5 and Lemma 4.6 are unchanged. We do not require Proposition 4.7 in order to conclude as in Lemma 4.8 that, almost surely,

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

as  $k \rightarrow \infty$ . Indeed, it is enough to show that, almost surely, the new expression corresponding to (37), namely,

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

converges to zero, as  $k \rightarrow \infty$ . This follows from Lemma 8.2, because the coefficients  $g_j^U(x_{ik})$  and  $g_j^L(x_{ik})$  are uniformly bounded by 1 and Lemma 8.2 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 4.9 still holds. Indeed, since a translate of  $P_k$  is contained in  $C_0^n$  and  $\Psi(P_k, \mathbf{x}_I, \mathbf{N}_I)$  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  $k \rightarrow \infty$ . We have  $g_{P(a) \cap C^n}(x_{ik}) \leq 1$  and  $g_{P_k}(x_{ik}) \leq V(2C_0)^n$ , since  $P_k \subset 2C_0$ , and then Lemma 7.1 implies that the new fourth term on the right-hand side of (97) converges to zero as  $k \rightarrow \infty$ . The rest of the proof of Lemma 4.9 proceeds as before.

The proof of the main theorem, Theorem 4.10, now applies without change. D

The user of Algorithm NoisyMod<sup>2</sup>LSQ must supply as input an  $o$ -symmetric convex polytope  $Q_k$  in  $\mathbb{R}^n$  that approximates either  $\nabla K_0$  or  $DK$ . For this purpose we provide two algorithms that do the work of Algorithm NoisyCovBlaschke and Algorithm NoisyCovDiff( $\phi$ ).

**Algorithm NoisyMod<sup>2</sup>Blaschke**

*Input:* Natural numbers  $n \geq 2$  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

$$(99) \quad \mathfrak{G}_k = |1^{K_0}(z^{ik})|^2 + X^{ik},$$

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

$$\{z_{ik} : i = 0, 1, \dots, I^i\} = \{o\} \cup (1/k^Y)Z_k^n(+),$$

where  $Z_k^n(+)$  satisfies (80) and where the  $X_{ik}$ 's are row-wise independent zero mean random variables with uniformly bounded fourth moments.

*Task:* Construct an  $o$ -symmetric convex polytope  $Q_k$  that approximates the Blaschke body  $\nabla K_0$ .

*Action:*

1. Let  $\mathfrak{g}_k = \mathfrak{g}_{-i}k$ , for  $i = -I^i, \dots, -1$ , and let

$$M_k(o) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I^i_k}^{I^i_k} \mathfrak{g}_{jk} \diamond \quad \text{and} \quad M_k(h_k u) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I^i_k}^{I^i_k} \cos(z \cdot h_k u) \mathfrak{g}_{jk} \diamond,$$

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

$$(100) \quad y_{ik} = \frac{M_k(o) - M_k(h_k u_i)}{h_k}.$$

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 5 can be modified to yield a convergence result corresponding to Theorem 5.4. It is clear that any such result must require the input  $h_k$  to satisfy  $h_k \rightarrow 0$  as  $k \rightarrow \infty$ , but we need a stronger condition phrased in terms of parameters  $\varepsilon$  and  $\gamma$  that satisfy (101). Since the second inequality in (101) 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  $\gamma$  and  $\varepsilon$  so

that (101) is satisfied. Specifically, one can choose  $3/4 \leq \gamma < 1$  and  $0 < \varepsilon < 1 - \gamma$ . Note also that (101) implies (96).

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  $q_k \rightarrow \infty$  as  $k \rightarrow \infty$ . To avoid overcomplicating the exposition, however, we shall not discuss this any further.

**Theorem 8.3.** *Let  $K_0 \subset C^n_0$  be a convex body with its centroid at the origin. Let  $(u_i)$  be a sequence in  $S^{n-1}$  such that  $(u^*)$  is evenly spread. Suppose that  $h_k \sim k^{\gamma-1+\varepsilon}$ ,  $k \in \mathbb{N}$ , where  $\varepsilon$  and  $\gamma$  satisfy*

$$(101) \quad 0 < \varepsilon < 1 - \gamma \quad \text{and} \quad 2n - 4n\gamma + 4(1 - \gamma - \varepsilon) < -1.$$

*If  $Q_k$  is an output from Algorithm NoisyMod<sup>2</sup>Blaschke as stated above, then, almost surely,*

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

*Proof.* We shall indicate the changes needed in Section 5. Note that by (100), and (83) with  $x = o$  and  $x = h_k u_i$ , we have

$$\begin{aligned} y_{ik} &= \frac{M_k(o) - M_k(h_k u_i)}{h_k} \\ &= \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} + \frac{N_k(o) - N_k(h_k u_i)}{h_k} - \frac{d_k(o) - d_k(h_k u_i)}{h_k}, \end{aligned}$$

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 (85) and (86) with  $x = o$  or  $x = h_k u_i$ , as appropriate.

In the proof of Lemma 5.1, we now have

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

where

$$(102) \quad \zeta_{ik} = \frac{g_{K_0}(o) - g_{K_0}(h_k u_i)}{h_k} - \frac{d_k(o) - d_k(h_k u_i)}{h_k} \quad \text{and} \quad T_{ik} = \frac{N_k(o) - N_k(h_k u_i)}{h_k},$$

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  $\zeta_{ik}$  converges to zero as  $k \rightarrow \infty$ , by Lemma 7.1, and hence  $\zeta_{ik} \rightarrow b_{K_0}(u_i)$  as  $k \rightarrow \infty$ , as before, for  $i = 1, \dots, k$ . Moreover,

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

so arguing as in the proof of Lemma 5.1, we use Lemma 3.1 with  $t = h_k$  to obtain (46) with  $t = h_k$ , that is,

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

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

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

by Lemma 7.1, so there is a constant  $c_{16} = c_{16}(n, r)$  such that

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



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 5.1 can be followed, yielding that, almost surely, there is a constant  $c_{17} = c_{17}(n, r)$  such that

$$(103) \quad |b_{K_0} - b_{Q_k}|_k \leq 2\Psi(Q_k, (u_i), \mathbf{T}_k) - 2\Psi(K_0, (u_i), \mathbf{T}_k) + \frac{c_{17}}{k^\beta} |b_{K_0} - b_{Q_k}|_k,$$

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 5.2 still holds. With (103) in hand, this rests on proving that, almost surely,

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

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

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

where

$$(104) \quad a_{pqk} = \frac{1}{k h_k^2} \prod_{i=1}^k (1 - \cos(z_{pk} \cdot h_k u_i)) (1 - \cos(z_{qk} \cdot h_k u_i))$$

and hence  $|a_{pqk}| \leq 4/h_k^2$ . As in the proof of Lemma 8.2, we may take the indices  $p, q$  from 1 to  $I_k$  and then, by (101), the claim follows from Lemma 7.2 with  $m_k = I_k$  and  $v = 2(1 - \gamma - \varepsilon)$ .

At this stage the work for Lemma 5.3 is already done. Indeed, by the Cauchy-Schwarz inequality,

$$\begin{aligned} \Psi(Q_k, (u_i), \mathbf{T}_k) - \Psi(K_0, (u_i), \mathbf{T}_k) &\leq |b_{K_0} - b_{Q_k}|_k \frac{1}{k} \prod_{i=1}^k T_{ik}^{1/2} \\ &= |b_{K_0} - b_{Q_k}|_k V_k^{1/2}. \end{aligned}$$

Using this and (103) we see that, almost surely,

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

as  $k \rightarrow \infty$ .

Finally, the proof of Theorem 5.4 can be applied without change. D

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

**Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ )**

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

$$(105) \quad g_{ik} = |1^{K_0}(z_{ik})|^2 + X_{ik},$$

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

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

where  $Z^n(+)$  satisfies (80) and where the  $X_{ik}$ 's are row-wise independent zero mean random variables with uniformly bounded fourth moments.

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

*Action:* Let  $g_{ik} = g_{(-i)k}$ , for  $i = -I'_k, \dots, -1$ , let  $x_{ik} = k^{Y-1}z_{ik}$ ,  $i = -I'_k, \dots, I'_k$ , be the points in the cubic array  $2C^n \cap (1/k)Z^n$ , and let

$$(106) \quad M_k(x_{ik}) = \frac{1}{(2\pi k^Y)^n} \sum_{j=-I'_k}^{I'_k} \cos(z_{jk} \cdot x_{ik}) g_{jk},$$

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

2. Run Algorithm NoisyCovDiff( $\phi$ ) with inputs  $n, k, \delta_k, \varepsilon_k$ , and  $M_{ik}$  replaced by  $M_k(x_{ik})$ , for  $i = -I'_k, \dots, I'_k$  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 6 used to prove Theorem 6.4 can be modified to yield the following convergence result.

**Theorem 8.4.** *Suppose  $K_0, \delta_k, \varepsilon_k$ , and  $g_k$  are as in Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ). Assume that  $\lim_{k \rightarrow \infty} \varepsilon_k = \lim_{k \rightarrow \infty} \delta_k = 0$  and that*

$$(107) \quad \liminf_{k \rightarrow \infty} \delta_k^4 k^{4\gamma n - 3n - 3/2} > 0,$$

where  $\gamma > 3(1 + 1/(2n))/4$ . If  $Q_k$  is an output from Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) as stated above, then, almost surely,

$$\delta(DK_0, Q_k) \leq c_{13} \delta_k^{1/n},$$

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

*Proof.* Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) can be regarded formally as Algorithm NoisyCovDiff( $\phi$ ) with  $M_{ik}$  and  $N_{ik}$  replaced by  $M_k(x_{ik})$  defined by (106) and  $N_k(x_{ik}) - d_k(x_{ik})$  defined by (85) and (86) with  $x = x_{ik}$ , respectively. We follow the arguments of Section 6 with this substitution in mind.

For Lemma 6.1, we note first that by (85),  $E(N_k(x_{ik})) = 0$  for all  $i$  and  $k$ . The same calculations as in the proof of Lemma 6.1 lead to

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

where  $d_k$  is as in Lemma 7.1. By that lemma,  $d_k \rightarrow 0$  as  $k \rightarrow \infty$  and hence the second statement in Lemma 6.1 still holds.

Next, for Lemma 6.2, recall the definition (66) of  $\beta_{ik}(x)$ . Then we have, by (85),

$$\begin{aligned} g_k(x) - E(g_k(x)) &= \sum_{i=-I_k^t}^{I_k^t} \beta_{ik}(x) N_k(x_{ik}) \\ &= \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I_k^t}^{I_k^t} \left( \sum_{i=-I_k^t}^{I_k^t} \beta_{ik}(x) \cos(z_{jk} \cdot x_{ik}) \right) X_{jk} \\ &= \frac{1}{(2\pi k^\gamma)^n} \sum_{j=-I_k^t}^{I_k^t} \zeta_{jk}(x) X_{jk}, \end{aligned}$$

say. This is a weighted sum of independent random variables, so we can apply Khinchine's inequality (see, for example, [29, (4.32.1), p. 307] with  $\alpha = 4$ ) to obtain

$$\left( E \left| \sum_{i=-I_k^t}^{I_k^t} \beta_{ik}(x) N_k(x_{ik}) \right|^4 \right)^{1/4} \leq \frac{c(2k+1)^n}{(2\pi k^\gamma)^{4n}} E \left| \sum_{j=-I_k^t}^{I_k^t} \zeta_{jk}(x) X_{jk} \right|^4$$

for some constant  $c > 0$ . Also,

$$\left| \sum_{i=-I_k^t}^{I_k^t} \beta_{ik}(x) \right|^4 \leq 1,$$

by (68). The same argument as in the proof of Lemma 6.2 now leads to the conclusion that there are constants  $c_{18} = c_{18}(\phi)$  and  $N_5 = N_5((\varepsilon_k), n) \in \mathbb{N}$  such that if  $\delta > 0$ , then

$$(108) \quad \Pr(|g_k(x) - g_{K_0}(x)| > \delta) \leq c_{18}(2k+1)^{2n} k^{-4\gamma n} \delta^{-4},$$

for all  $k \geq N_5$  and all  $x \in \mathbb{R}^n$ . (Compare (65).)

Lemma 6.3 is unchanged. With (107) instead of the hypothesis (70) of Theorem 6.4 and with the new estimate (108), we arrive in the proof of Theorem 6.4 at the estimate

$$\Pr(a_k \geq \delta_k) \leq c_{18}(2k+1)^{3n} k^{-4\gamma n} \delta_k^{-4} = O(k^{-3/2}),$$

so the Borel-Cantelli Lemma can be used as before. This is all that is required to allow the proof of Theorem 6.4 to go through until near the end, when we use the fact that  $k\delta_k^{1/n} \rightarrow \infty$  as  $k \rightarrow \infty$ . By (107) and the fact that  $\gamma < 1$ , this still holds. Then the conclusion is the same, namely that, almost surely,

$$\delta(DK_0, Q_k) \leq c_{13} \delta_k^{1/n},$$

for sufficiently large  $k$ . D

Concerning Corollary 6.5, by using  $\gamma > 3(1 + 1/(2n))/4$  and (107) instead of (70), we can achieve a convergence rate arbitrarily close to  $k^{-1/4+3/(8n)}$ , the same as before. If we assume instead that the random variables  $X_{ik}$  in Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) are row-wise independent, zero mean, and satisfy (75) and (76), that  $\gamma > 1/2$ , and that

$$(109) \quad \liminf_{k \rightarrow \infty} \frac{\delta_k^2 k^{n(2\gamma-1)}}{\log k} > c_{19}(n+2),$$

where  $c_{19} = c_{19}(n, \sigma) = (3^{n+2}\sigma^2)/((2\pi)^{2n})$ , then a rate arbitrarily close to  $k^{-1/2}$  can be obtained by the methods outlined in Remark 6.6.

### 9. 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  $g \cdot w$  here  $g$  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  $g$  considered earlier. Thus instead of (81) above we have, for  $r = 1, 2$ , measurements

$g_{z,k}^{(r)} = \int_{\mathbb{R}^n} g(z/k^Y) + X_{z,k}^{(r)}$  of  $g$  or  $z \in \{0\} \cup \mathbb{Z}^{n(+)}$ , where  $\mathbb{Z}^{n(+)}$  satisfies (80) and where the  $X_{z,k}^{(r)}$ 's are row-wise independent (i.e., independent for fixed  $k$ ) zero mean random variables with uniformly bounded fourth moments. Then we replace  $\tilde{g}_{z,k}$  in (81) by

$$(110) \quad g_{z,k} = g_{z,k}^{(1)} g_{z,k}^{(2)} = \int_{\mathbb{R}^n} g(z/k^Y) + X_{z,k}^{(1)} + X_{z,k}^{(2)}$$

Setting  $\bar{g}_{jk} = \overline{g_{z,k}^{(1)} g_{z,k}^{(2)}}$  and  $X_{jk} = X_{z_{jk},k}$ , the same notation and analysis that gave (83), but now using (82) and (110), leads instead to

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

where

$$(111) \quad \bar{M}_k(x) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I_k}^{I_k} \cos(z_{jk} \cdot x) g_{jk}$$

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

$$(112) \quad N_k(x) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I_k}^{I_k} g_{K_0}(z_{jk}) \cos(z_{jk} \cdot x) X_{jk}^{(1)} + X_{jk}^{(2)} + \frac{1}{(2\pi k^Y)^n} \int_{j=-I_k}^{I_k} \cos(z_{jk} \cdot x) X_{jk}^{(1)} X_{jk}^{(2)}$$

is a random variable, and the deterministic error  $d_k(x)$  is given as before by (86).

For our analysis it will be convenient to let

$$(113) \quad N_{k1}(x) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I_k}^{I_k} g_{K_0}(z_{jk}) \cos(z_{jk} \cdot x) X_{jk}^{(1)} + X_{jk}^{(2)}$$

and

$$(114) \quad N_{k2}(x) = \frac{1}{(2\pi k^Y)^n} \int_{j=-I_k}^{I_k} \cos(z_{jk} \cdot x) X_{jk}^{(1)} X_{jk}^{(2)},$$

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

To keep the exposition brief, we shall not give a formal presentation of our algorithms, called **Algorithm NoisyModLSQ**, **Algorithm NoisyModBlaschke**, and **Algorithm NoisyModDiff( $\phi$ )**, since they are very similar to Algorithm NoisyMod<sup>2</sup>LSQ, Algorithm NoisyMod<sup>2</sup>Blaschke, and Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ), respectively. In each case the input is as before, except that instead of (94), (99), and (105), we now have measurements

$$g_{ik}^{(r)} = |1_{K_0}(zik)| + X_{ik}^{(r)},$$

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 row-wise independent zero mean random variables with uniformly bounded fourth moments. The task is the same in each case. For the actions, we first let  $\bar{g}_{ik} = \bar{g}_{ik}^{(1)} \bar{g}_{ik}^{(2)}$  and then follow the actions of the appropriate algorithms in the previous section, replacing  $g$  by  $\bar{g}$ . Thus in the action of each algorithm, we replace  $M_k(x)$  by  $M_k(x)$  defined by (111), for the appropriate  $x$ .

**Theorem 9.1.** *Theorem 8.1 holds when Algorithm NoisyMod<sup>2</sup>LSQ is replaced by Algorithm NoisyModLSQ.*

*Proof.* In the action of Algorithm NoisyModLSQ, the measurements used in Algorithm NoisyCovLSQ are now  $M_k(x_{ik})$ ,  $i = -I'_k, \dots, I'_k$  where  $M_k(x_{ik})$  is given by (111) with  $x = x_{ik}$ . Thus we have

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

$i = -I'_k, \dots, I'_k$ , where  $\bar{N}_k(x_{ik})$  and  $d_k(x_{ik})$  are given by (112) and (86), respectively, with  $x = x_{ik}$ .

We claim that Lemma 8.2 holds when  $N_k(x_{ik})$  is replaced by  $\bar{N}_k(x_{ik})$ . To see this, use the triangle inequality to obtain

$$\begin{aligned} \left( \sum_{i=-I'_k}^{I'_k} N_k(x_{ik}) \right)^{1/2} &\leq \left( \sum_{i=-I'_k}^{I'_k} N_k(x_{ik})^2 \right)^{1/2} \\ &\leq \left( \sum_{i=-I'_k}^{I'_k} N_{k1}(x_{ik})^2 \right)^{1/2} + \left( \sum_{i=-I'_k}^{I'_k} N_{k2}(x_{ik})^2 \right)^{1/2}, \end{aligned}$$

where  $\bar{N}_{k1}(x_{ik})$  and  $\bar{N}_{k2}(x_{ik})$  are given by (113) and (114), respectively, with  $x = x_{ik}$ . Since  $g_{K_0}$ s are bounded, the same analysis as in the proof of Lemma 8.2, up to a constant, applies to the first of the two sums in the previous expression. So it suffices to prove that, almost surely,

$$\sum_{i=-I'_k}^{I'_k} N_{k2}(x_{ik})^2 \rightarrow 0,$$

as  $k \rightarrow \infty$ . As in the proof of Lemma 8.2, it is enough to show that, almost surely,

$$\sum_{p,q=1}^{I'_k} c_{pqk} X_{pk}^{(1)} X_{pk}^{(2)} X_{qk}^{(1)} X_{qk}^{(2)} \rightarrow 0,$$

as  $k \rightarrow \infty$ . This follows from Lemma 7.3 and proves the claim.

With this in hand, we can conclude exactly as in the proof of Theorem 8.1 that Algorithm NoisyCovLSQ works with the new measurements under the same hypotheses. D

We remark that the computation of  $E(Z_k)$  in Lemma 7.3 shows why we take two independent measurements of  $\sqrt{g_{K_0}}$  and multiply, rather than taking a single measurement and squaring it. In the latter case we would be led to

$$E(Z_k) = \frac{1}{(2\pi k^\gamma)^{2n}} \sum_{p,q=1}^m a_{pqk} E(Y_{pk}^2) E(Y_{qk}^2) = O(k^{2n-2n\gamma+v}),$$

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

**Theorem 9.2.** *Theorem 8.3 holds when Algorithm NoisyMod<sup>2</sup>Blaschke is replaced by Algorithm NoisyModBlaschke.*

*Proof.* We now have

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

where  $\zeta_{ik}$  is as in (102) and

$$(115) \quad T_{ik} = \frac{\bar{N}_k(o) - \bar{N}_k(h_k u_i)}{h_k} = \frac{\bar{N}_{k1}(o) - \bar{N}_{k1}(h_k u_i)}{h_k} + \frac{\bar{N}_{k2}(o) - \bar{N}_{k2}(h_k u_i)}{h_k},$$

for  $i = 1, \dots, k$ , where  $\bar{N}_{k1}$  and  $\bar{N}_{k2}$  are given by (113) and (114). The proof of Theorem 8.3 can be followed, except that for Lemma 5.2, one now shows that, almost surely,

$$\sum_{k=1}^{\infty} T_{ik} \rightarrow 0$$

as  $k \rightarrow \infty$ . Using the fact that the earlier analysis applies to  $\bar{N}_{k1}$ , and using also the triangle inequality, as we did in the proof of Theorem 9.1, with (115), we see that it suffices to examine

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

where  $a_{pqk}$  is given by (104). Then Lemma 7.3 shows that it is possible to choose  $\gamma$  and  $\varepsilon$  exactly as in Theorem 8.3 to ensure that Lemma 5.2 holds. No further changes are required, so Algorithm NoisyCovBlaschke works with the new measurements under the same hypotheses as in Theorem 8.3. D

**Theorem 9.3.** *Theorem 8.4 holds when Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) is replaced by Algorithm NoisyModDiff( $\phi$ ).*

*Proof.* Note that by (112), we have  $E(\bar{N}_k(x_{ik})) = 0$  for all  $i$  and  $k$ . Therefore the same calculations as in the proof of Theorem 8.4 show that the second statement in Lemma 6.1 still holds.

In Lemma 6.2, it is enough in view of the proof of Theorem 8.4 to consider the contribution to  $g_k(x) - E(g_k(x))$  from  $\bar{N}_{k2}(x_{ik})$ , namely,

$$\frac{1}{(2\pi k^\gamma)^n} \sum_{j=-\frac{r}{k}}^{\frac{r}{k}} \sum_{i=-\frac{r}{k}}^{\frac{r}{k}} \beta_{ik}(x) \cos(z_{jk} \cdot x_{ik}) X_{jk}^{(1)} X_{jk}^{(2)}.$$

This allows the same estimate as before, up to a constant. No further changes are required, so Algorithm NoisyCovDiff( $\phi$ ) works with the new measurements under the same hypotheses as in Theorem 8.4. D

The previous result provides a convergence rate for Algorithm NoisyModDiff( $\phi$ ) arbitrarily close to  $k^{-1/4+3/(8n)}$ , as was noted for Algorithm NoisyMod<sup>2</sup>Diff( $\phi$ ) after Theorem 8.4. If we assume instead that the random variables  $X_{ik}$  in Algorithm NoisyModDiff( $\phi$ ) are row-wise independent, zero mean, and satisfy (75) and (76), that  $\gamma > 1/2$ , and that (109) holds, then a rate arbitrarily close to  $k^{-1/2}$  can be obtained by the methods outlined in Remark 6.6.

## 10. Appendix

**10.1. Convergence rates.** Rates of convergence for Algorithm NoisyCovDiff( $\phi$ ), and hence for the two related algorithms for phase retrieval, are provided in Corollary 6.5 and Remark 6.6. For the other algorithms, however, rates of convergence are more difficult to obtain. To explain why, it will be necessary to describe some results from [24], where convergence rates were obtained for algorithms for reconstructing convex bodies from finitely many noisy measurements of either their support functions or their brightness functions. The algorithms are called Algorithm NoisySupportLSQ and Algorithm NoisyBrightnessLSQ, respectively.

In [24], an unknown convex body  $K$  is assumed to be contained in a known ball  $RB^n$ ,  $R > 0$ , in  $R^n$ . An infinite sequence  $(u_i)$  in  $S^{n-1}$  is selected, and one of the algorithms is run with noisy measurements from the first  $k$  directions in the sequence as input. The noise is modeled by Gaussian  $N(0, \sigma^2)$  random variables. With an assumption on  $(u_i)$  slightly stronger than the condition that it is evenly spread (but still mild and satisfied by many natural sequences) and another unimportant assumption on the relation between  $R$  and  $\sigma$ , it is proved in [24, Theorem 6.2] that if  $P_k$  is the corresponding output from Algorithm NoisySupportLSQ, then, almost surely, there are constants  $C = C(n, (u_i))$  and  $N = N(\sigma, n, R, (u_i))$  such that

$$(116) \quad \delta_2(K, P_k) \leq C \sigma^{4/(n+3)} R^{(n-1)/(n+3)} k^{-2/(n+3)},$$

for  $k \geq N$ , provided that the dimension  $n \leq 4$ . Here  $\delta_2$  is the  $L_2$  metric, so that  $\delta_2(K, P_k) = \|h_K - h_{P_k}\|_2$ , where  $\|\cdot\|_2$  denotes the  $L_2$  norm on  $S^{n-1}$ . Convergence rates for the Hausdorff metric are then obtained by using the known relations between the two metrics.

It is an artifact of the method that while convergence rates can also be obtained for  $n \geq 5$ , neither these nor those for the Hausdorff metric are expected to be optimal. In contrast, it has recently been proved by Guntuboyina [28] that the rate given in (116) for  $n \leq 4$  is the best possible in the minimax sense. With the additional assumption that  $K$  is  $o$ -symmetric, corresponding rates for Algorithm NoisyBrightLSQ are obtained in [24, Theorem 7.6] from those for Algorithm NoisySupportLSQ by exploiting (4) and the Bourgain-Campi-Lindenstrauss stability theorem for projection bodies.

There are two principal ingredients in the proof of (116). The first is [24, Corollary 4.2], a corollary of a deep result of van de Geer [48, Theorem 9.1]. This corollary provides convergence rates for least squares estimators of an unknown function in



a class  $\mathcal{G}$ , based on finitely many noisy measurements of its values, where the noise is uniformly sub-Gaussian. The result and the rates depend on having a suitable estimate for the size of  $\mathcal{G}$  in terms of its  $\varepsilon$ -entropy with respect to a suitable pseudo-metric. The second ingredient is a known estimate (see [24, Proposition 5.4]) of the  $\varepsilon$ -entropy of the class of support functions of compact convex sets contained in  $B^n$ , with respect to the  $L_\infty$  metric.

It should be possible to apply this method to obtain convergence rates for Algorithm NoisyCovBlaschke and the two related algorithms for phase retrieval. With Gaussian noise, or more generally uniformly sub-Gaussian noise, this requires a modification to [48, Theorem 9.1] that, in our situation, allows (53) to be used instead of the same inequality without the term  $c_{11}/k$ . (Compare [48, (9.1), p. 148].) This would yield the same convergence rates given in [24, Theorem 7.6] for Algorithm NoisyBrightLSQ. To cover the case of Poisson noise, however, one can make the general assumption that the random variables are row-wise independent, zero mean, and satisfy (75) and (76), as in Remark 6.6. This creates considerable further technical difficulties. It may well be possible to overcome these, using the machinery behind another result of van de Geer [48, Theorem 9.2]. But, as van de Geer points out in [48, p. 134], there is a price to pay: One now requires a uniform bound on the class  $\mathcal{G}$  of functions, as well as estimates of  $\varepsilon$ -entropy “with bracketing”. The former condition might be dealt with by (49), which implies that the sets  $\Pi Q_k$  are uniformly bounded for any fixed realization. It should also be possible to obtain the latter, by combining suitable modifications of the bracketing argument of Lemma 4.6 and of the proof in [24, Theorem 7.3] of the  $\varepsilon$ -entropy estimate for the class of zonoids contained in  $B^n$ .

But we have not carried out a complete investigation into convergence rates for Algorithm NoisyCovBlaschke and the related algorithms for phase retrieval, despite having a strategy for doing so, described in the previous paragraph. The main reason is that there are more serious technical obstacles in achieving convergence rates for Algorithm NoisyCovLSQ, even for the case of Gaussian noise. In principal, the method outlined above could be applied by taking  $\mathcal{G}$  to be the class of covariograms of compact convex subsets of the unit ball in  $\mathbb{R}^n$ . However, an estimate would be required of the  $\varepsilon$ -entropy of this class with respect to the  $L_\infty$  metric or some other suitable pseudo-metric. Even if this were available, an application of the theory of empirical processes as described above would yield convergence rates not for  $\delta_2(K, P_k)$  but rather for  $\|g_K - g_{P_k}\|_2$ . To obtain rates for  $\delta_2(K, P_k)$ , one would then also need suitable stability versions of the uniqueness results for the Covariogram Problem described in the Introduction. In view of the difficulty of these uniqueness results, proving such stability versions will presumably be very challenging.

In summary, a full study of convergence rates for the other algorithms proposed here must remain a project for future study.

**10.2. Implementation issues.** The study undertaken in this paper is a theoretical one. Although we propose algorithms in enough detail to allow implementation, the laborious task of writing all the necessary programs, carrying out numerical experiments, and comparing with other algorithms, largely lies ahead.

At the present time we only have a rudimentary implementation of Algorithms NoisyCovBlaschke and NoisyCovLSQ. The programs were written, mainly in Matlab, by Michael Sterling-Goens while he was an undergraduate student at Western

Washington University and are confined to the planar case. Algorithm NoisyCovBlaschke seems to be very fast; this is to be expected, since it is based on Algorithm NoisyBrightnessLSQ, which is also fast even in three dimensions. Behind both of these latter two algorithms is a linear least squares problem (cf. [25, (18) and (19)]). In contrast, the least squares problem (18) in Algorithm NoisyCovLSQ is nonlinear. Preliminary experiments indicate that reasonably good reconstructions, such as those depicted in Figures 1–4 (based on Gaussian  $N(0, \sigma^2)$  noise,  $k = 60$  equally spaced directions in Algorithm NoisyCovBlaschke and  $k = 8$  in Algorithms NoisyCovLSQ), can usually be obtained in a reasonable time in the planar case. Occasionally, however, reconstructions can be considerably worse, particularly for regular  $m$ -gons for very small  $m$ . Better and faster reconstructions, also in higher dimensions, will probably require bringing to bear the usual array of techniques for nonlinear optimization, such as simulated annealing.

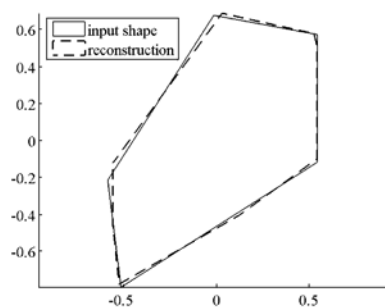


Figure 1. Pentagon, no noise

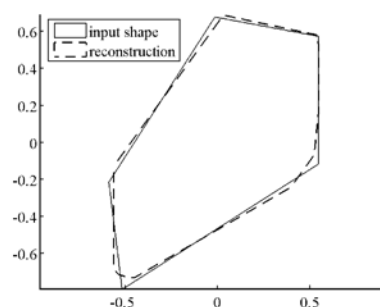
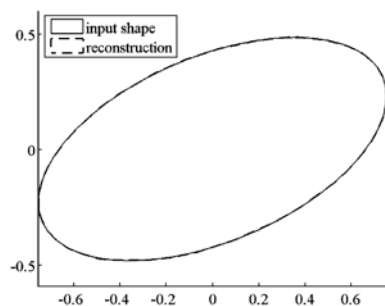
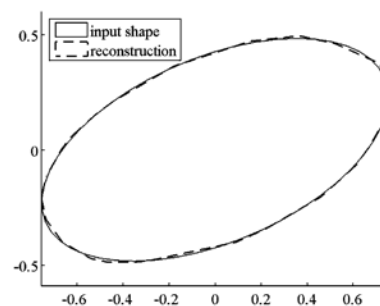
Figure 2. Pentagon,  $\sigma = 0.01$ 

Figure 3. Ellipse, no noise

Figure 4. Ellipse,  $\sigma = 0.01$ 

Since the least squares problem (18) is nonlinear, it is important to control the number of variables, that is, the number of facets of the approximation  $Q_k$  to the Blaschke body  $\nabla K_0$  of  $K_0$ . To a large extent, Algorithm NoisyCovBlaschke already does this; the potential  $O(k^{n-1})$  variables that would otherwise be required (see [24, p. 1335]) is, as experiments show, considerably reduced. In fact, if there is little or no noise, a linear programming version of the brightness function reconstruction program due to Kiderlen (see [25, p. 289], where it is stated for measurements without noise) is not only even faster, but also produces approximations  $Q_k$  to

$\nabla K_0$  with at most  $2k$  facets. Beyond this, there is the possibility of using the pruning techniques discussed in [41, Section 3.3].

There is also the possibility of changing the variables in the least squares problem (18). A convex polytope  $P$  whose facet outer unit normals are a subset of a prescribed set  $\{\pm u_j : j = 1, \dots, s\}$  of directions can be specified by the vector  $h = (h_1^+, h_1^-, \dots, h_s^+, h_s^-)$  such that

$$P = P(h) = \{x \in \mathbb{R}^n : -h_j^- \leq x \cdot u_j \leq h_j^+, j = 1, \dots, s\}.$$

The possible advantage in using these variables arises from the fact that, by the Brunn-Minkowski inequality (cf. [21, Section 11]), the covariogram  $g_{P(h)}(x)$  turns out to be  $(1/n)$ -concave (i.e.,  $g_{P(h)}(x)^{1/n}$  is concave) on its support in the combined variable  $(h, x)$ . One may therefore try solving the problem

$$(117) \quad \min_{i=1}^{I_k} (M_{ik} - g_{P(h)}(x_{ik}))^2$$

over the variables  $h_1^+, h_1^-, \dots, h_s^+, h_s^-$ . By expanding the square in (117), approximating the sums by integrals, and using the Prékopa-Leindler inequality [21, Section 7], the objective function can be seen as an approximation to the difference of two log-concave functions. These admittedly weak concavity properties may help.

Regularization is often used to improve Fourier inversion in the presence of noise. We expect this to be of benefit in implementing the phase retrieval algorithms, where preliminary investigations indicate that regularization will allow the restriction on the parameter  $\gamma$  to be considerably relaxed.

Corresponding to the two basic approaches to reconstruction—one via the Blaschke body and one via the difference body—there are two different sampling designs. For the former, measurements are made first at the origin and at points in a small sphere centered at the origin and then again at points in a cubic array. For the latter, measurements are made twice, each time at points in a cubic array. These sampling designs are a matter of convenience, at least regarding the cubic array. It should be possible to use a variety of different sets of measurement points, at least for reconstructing from covariogram measurements, with appropriate adjustments in the consistency proofs.

### 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. MR1450931 (98e:60054)
- [3] I. A. Ahmad and P.-E. Lin, Fitting a multiple regression function, *J. Statist. Plann. Inference* **9** (1984), 163–176. MR738366 (86a:62053)
- [4] G. Averkov and G. Bianchi, Confirmation of Matheron’s conjecture on the covariogram of a planar convex body, *J. Europ. Math. Soc.* **11** (2009), 1187–1202. MR2557133
- [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. MR2441634 (2009e:52004)
- [7] G. Bianchi, Matheron’s conjecture for the covariogram problem, *J. London Math. Soc.* (2) **71** (2005), 203–220. MR2108257 (2005i:60021)
- [8] G. Bianchi, The covariogram determines three-dimensional convex polytopes, *Adv. Math.* **220** (2009), 1771–1808. MR2493181 (2010i:60035)
- [9] G. Bianchi, F. Segala, and A. Volčič, The solution of the covariogram problem for plane  $C^2_+$  convex bodies, *J. Differential Geom.* **60** (2002), 177–198. MR1938112 (2003h:52001)

- [10] P. Billingsley, *Convergence of Probability Measures*, second edition, John Wiley and Sons, New York, 1999. MR1700749 (2000e:60008)
- [11] 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. MR950986 (89g:46024)
- [12] 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. MR2006553 (2004g:42015)
- [13] N. S. Brannen, The Wills conjecture, *Trans. Amer. Math. Soc.* **349** (1997), 3977–3987. MR1373630 (97m:52024)
- [14] V. V. Buldygin and Y. V. Kozachenko, *Metric Characterization of Random Variables and Random Processes*, American Mathematical Society, Providence, RI, 2000. MR1743716 (2001g:60089)
- [15] A. Cabo and A. Baddeley, Estimation of mean particle volume using the set covariance function, *Adv. in Appl. Probab.* **35** (2003), 27–46. MR1974301 (2004c:60025)
- [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. MR964515 (89m:52002)
- [17] R. M. Dudley, Distances of probability measures and random variables, *Ann. Math. Stat.* **39** (1968), 1563–1572. MR0230338 (37:5900)
- [18] J. R. Fienup, Phase retrieval algorithms: a comparison, *Appl. Opt.* **21** (1982), 2758–2769.
- [19] B. Galerne, Computation of the perimeter of measurable sets via their covariogram. Applications to random sets, *Image Anal. Stereol.*, to appear.
- [20] R. J. Gardner, *Geometric Tomography*, second edition, Cambridge University Press, New York, 2006. MR2251886 (2007i:52010)
- [21] R. J. Gardner, The Brunn-Minkowski inequality, *Bull. Amer. Math. Soc.* **39** (2002), 355–405. MR1898210 (2003f:26035)
- [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. MR2160045 (2006i:52026)
- [23] R. J. Gardner and M. Kiderlen, A solution to Hammer’s X-ray reconstruction problem, *Adv. Math.* **214** (2007), 323–343. MR2348033 (2008h:52004)
- [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. MR2278360 (2008e:68146)
- [25] R. J. Gardner and P. Milanfar, Reconstruction of convex bodies from brightness functions, *Discrete Comput. Geom.* **29** (2003), 279–303. MR1957233 (2004a:68145)
- [26] R. J. Gardner and G. Zhang, Affine inequalities and radial mean bodies, *Amer. J. Math.* **120** (1998), 493–504. MR1623396 (99e:52006)
- [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. MR1416411 (97g:52017)
- [28] A. Guntuboyina, Lower bounds for the minimax risk using  $f$ -divergences and applications, *IEEE Trans. Inform. Theory*, to appear.
- [29] J. Hoffmann-Jørgensen, *Probability With a View Toward Statistics*, Vol. I, Chapman & Hall, New York, 1994. MR1278485 (95c:60001a)
- [30] T.-C. Hu, F. Móricz, and R. L. Taylor, Strong laws of large numbers for arrays of row-wise independent random variables, *Acta Math. Hungar.* **54** (1989), 153–162. MR1015785 (91f:60061)
- [31] 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. MR1962583 (2004b:52004)
- [32] N. E. Hurt, *Phase Retrieval and Zero Crossings*, Kluwer, Dordrecht, 1989. MR1093464 (92k:94002)
- [33] 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. MR1990605 (2004k:60023)
- [34] M. V. Klivanov, P. E. Sacks, and A. V. Tikhonravov, The phase retrieval problem, *Inverse Problems* **11** (1995), 1–28. MR1313598 (95m:35203)
- [35] F. C. Liu, On the localization of rectangular partial sums for multiple Fourier series, *Proc. Amer. Math. Soc.* **34** (1972), 90–96. MR0294993 (45:4061)
- [36] D. R. Luke, J. V. Burke, and R. G. Lyon, Optical wavefront reconstruction: theory and numerical methods, *SIAM Rev.* **44** (2002), 169–224. MR1926097 (2003i:78006)

- [37] C. L. Mallows and J. M. C. Clark, Linear-intercept distributions do not characterize plane sets, *J. Appl. Probab.* **7** (1970), 240–244. MR0259976 (41:4605)
- [38] G. Matheron, *Random Sets and Integral Geometry*, Wiley, New York, 1975. MR0385969 (52:6828)
- [39] G. Matheron, La formule de Steiner pour les érosions, *J. Appl. Probab.* **15** (1978), 126–135. MR0493914 (58:12874)
- [40] G. Matheron, Le covariogramme géométrique des compacts convexes des  $R^2$ , *Technical Report N-2/86/G*, Centre de Géostatistique, Ecole Nationale Supérieure des Mines de Paris, 1986.
- [41] A. Poonawala, P. Milanfar, and R. J. Gardner, Shape estimation from support and diameter functions, *J. Math. Imaging Vision* **24** (2006), 229–244. MR2227098 (2007j:94009)
- [42] J. Rosenblatt, Phase retrieval, *Commun. Math. Phys.* **95** (1984), 317–343. MR765273 (86k:82075)
- [43] 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. MR1196706 (93j:68223)
- [44] M. Schmuckenschläger, The distribution function of the convolution square of a convex symmetric body in  $R^n$ , *Israel J. Math.* **78** (1992), 309–334. MR1194970 (93k:52008)
- [45] J. Serra, *Image Analysis and Mathematical Morphology*, Academic Press, London, 1982. MR753649 (87d:68106)
- [46] R. Schneider, *Convex Bodies: The Brunn-Minkowski Theory*, Cambridge University Press, Cambridge, 1993. MR1216521 (94d:52007)
- [47] A. Tsolomitis, Convolution bodies and their limiting behavior, *Duke Math. J.* **87** (1997), 181–203. MR1440068 (98c:52007)
- [48] S. van de Geer, *Applications of Empirical Process Theory*, Cambridge University Press, New York, 2000. MR1739079 (2001h:62002)
- [49] A. W. van der Waart and J. A. Wellner, *Weak Convergence and Empirical Processes*, Springer, New York, 1996. MR1385671 (97g:60035)
- [50] E. Werner, A general geometric construction for affine surface area, *Studia Math.* **132** (1999), 227–238. MR1669674 (99m:52008)

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, Washington 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