

# Almost Lossless Analog Compression without Phase Information

Erwin Riegler

ETH Zurich, 8092 Zurich, Switzerland  
eriegler@nari.ee.ethz.ch

Georg Tauböck

Austrian Academy of Sciences, 1040 Vienna, Austria  
georg.tauboeck@oeaw.ac.at

**Abstract**—We propose an information-theoretic framework for phase retrieval. Specifically, we consider the problem of recovering an unknown vector  $\mathbf{x} \in \mathbb{R}^n$  up to an overall sign factor from  $m = \lfloor Rn \rfloor$  phaseless measurements with compression rate  $R$  and derive a general achievability bound for  $R$ . Surprisingly, it turns out that this bound on the compression rate is the same as the one for almost lossless analog compression obtained by Wu and Verdú (2010): Phaseless linear measurements are “as good” as linear measurements with full phase information in the sense that ignoring the sign of  $m$  measurements only leaves us with an ambiguity with respect to an overall sign factor of  $\mathbf{x}$ .

## I. INTRODUCTION

In many different areas of science, physical limitations make it impossible to measure the sign (phase in the complex case) of a signal but obtaining amplitudes is relatively easy. Well known examples are X-ray crystallography, astronomy, or diffraction imaging [1]–[3]. The problem of retrieving a signal up to a global sign (phase in the complex case) from intensity measurements is often referred to as *phase retrieval*. More formally, let  $\mathbb{R}_\pm^n$  be the set of equivalence classes  $[\mathbf{x}] = \{\mathbf{x}\} \cup \{-\mathbf{x}\}$  with  $\mathbf{x} \in \mathbb{R}^n$ . Phase retrieval is the problem of recovering  $[\mathbf{x}] \in \mathbb{R}_\pm^n$  from  $m$  phaseless measurements of the form<sup>1</sup>  $\mathbf{y} = |\mathbf{A}\mathbf{x}| \in \mathbb{R}^m$  with measurement matrix  $\mathbf{A} \in \mathbb{R}^{m \times n}$ .

It is by no means clear how large  $m$  has to be to allow for recovery of  $[\mathbf{x}] \in \mathbb{R}_\pm^n$  from  $m$  phaseless measurements. Thus from the very beginning, there have been a number of works regarding recovery conditions for this problem in the context of specific applications [4]. More recently, this question has been studied in more abstract terms, asking for the smallest number  $m$  of phaseless measurements that is required to make the mapping  $[\mathbf{x}] \mapsto |\mathbf{A}\mathbf{x}|$  injective without imposing structural assumptions on  $\mathbf{A}$ . In [5], the authors showed that at least  $2n - 1$  such measurements are necessary and generically sufficient to guarantee injectivity. Furthermore, it was shown that semidefinite programming can be used to recover  $[\mathbf{x}]$  if  $\mathbf{A}$  is random with i.i.d. Gaussian entries or with i.i.d. rows that are uniformly distributed on a sphere, as long as  $m \geq c_0 n$  for a sufficiently large constant  $c_0$  [6]. Other phase retrieval methods for which theoretical performance guarantees are available can be found, e.g., in [7]–[10].

This work was supported in part by the WWTF under grant VRG 12-009 and by the FWF under grant Y 551-N13.

<sup>1</sup>For a vector  $\mathbf{u} \in \mathbb{R}^k$ , we define the element-wise absolute value operation as  $|\mathbf{u}| = (|u_1|, \dots, |u_k|)^T$ .

Recently, there has been also interest in *sparse phase retrieval*, where the number  $s$  of nonzero coefficients of the vector  $\mathbf{x}$  is much smaller than  $n$ . This a-priori knowledge about  $\mathbf{x}$  can be used to reduce the number of measurements significantly. For instance,  $\mathcal{O}(s \log(n/s))$  measurements were shown to be sufficient for stable sparse phase retrieval [11]. If the rows of the measurement matrix  $\mathbf{A}$  are a generic choice of vectors in  $\mathbb{R}^n$ , injectivity of the mapping  $[\mathbf{x}] \mapsto |\mathbf{A}\mathbf{x}|$  is guaranteed provided that  $m \geq 2s$  [12].

**Contributions:** Following the approach introduced for compressed sensing [13] and signal separation [14] problems, we formulate phase retrieval as an analog source coding problem. Assuming that the unknown vector  $\mathbf{x}$  is random with a certain distribution, we derive asymptotic recovery results for  $[\mathbf{x}]$ . Our results hold for Lebesgue almost all (a.a.) measurement matrices  $\mathbf{A}$ . However, our results are in terms of probability of error (with respect to the distribution of  $\mathbf{x}$ ) and hence do not provide worst-case guarantees. Specifically, we study the asymptotic setting  $n \rightarrow \infty$  where the vector  $\mathbf{x}$  is a realization of a random process; for each  $n$ , we let  $m = \lfloor Rn \rfloor$  for a parameter  $R$ , which we denote *compression rate*. In Theorem 1 we show that we can recover  $[\mathbf{x}]$  from  $m$  phaseless measurements with arbitrarily small probability of error for a.a. measurement matrices  $\mathbf{A}$ , provided that  $n$  is sufficiently large and the compression rate  $R$  is larger than the (lower) Minkowski dimension compression rate (see Definition 4) of  $\mathbf{x}$ . It is remarkable that the obtained result is identical to the corresponding result in compressive sensing [13] where  $\mathbf{y} = \mathbf{A}\mathbf{x}$ , so that we can conclude that *in terms of achievability results, phaseless linear measurements are “as good” as linear measurements with full phase information*: Ignoring the sign of  $m$  measurements only leaves us with an ambiguity with respect to an overall sign factor of  $\mathbf{x}$ .

**Notation:** Roman letters  $\mathbf{A}, \mathbf{B}, \dots$  and  $\mathbf{a}, \mathbf{b}, \dots$  designate deterministic matrices and vectors, respectively. Boldface letters  $\mathbf{A}, \mathbf{B}, \dots$  and  $\mathbf{a}, \mathbf{b}, \dots$  denote random matrices and random vectors, respectively. For the distribution of a random matrix  $\mathbf{A}$  and a random vector  $\mathbf{a}$ , we write  $\mu_{\mathbf{A}}$  and  $\mu_{\mathbf{a}}$ , respectively. The  $i$ th component of the vector  $\mathbf{u}$  (random vector  $\mathbf{u}$ ) is  $u_i$  ( $u_i$ ). The superscript  $\top$  stands for transposition. For a matrix  $\mathbf{A}$ ,  $\text{tr}(\mathbf{A})$  denotes its trace. The identity matrix of suitable size is denoted by  $\mathbf{I}$ . For a vector  $\mathbf{u}$ , we write  $\|\mathbf{u}\| = \sqrt{\mathbf{u}^\top \mathbf{u}}$  for its Euclidean norm. For the Euclidean space  $(\mathbb{R}^k, \|\cdot\|)$ , we denote the open ball of radius  $r$  centered at  $\mathbf{u} \in \mathbb{R}^k$  by  $\mathcal{B}_k(\mathbf{u}, r)$ ,

$V(k, r)$  stands for its volume. The Borel sigma algebra on  $\mathbb{R}$  is denoted by  $\mathcal{B}_{\mathbb{R}}$ . We write  $\mathbb{R}_{\geq}$  for the set of nonnegative real numbers with Borel sigma algebra  $\mathcal{B}_{\mathbb{R}_{\geq}}$ . For  $u, v \in \mathbb{R}^k$ ,  $u \sim v$  means that either  $u = v$  or  $u = -v$  and we write for the corresponding equivalence classes  $[u] = \{u\} \cup \{-u\}$ . For a set  $\mathcal{S} \subseteq \mathbb{R}^k$ ,  $\mathcal{S}_{\sim} = \{[u] \mid u \in \mathcal{S}\}$ . The indicator function on a set  $\mathcal{U}$  is denoted by  $\chi_{\mathcal{U}}$ .

## II. MAIN RESULTS

We start by formulating phase retrieval as a source coding problem.

**Definition 1.** (Source vector) Let  $(x_i)_{i \in \mathbb{N}}$  be a stochastic process on  $(\mathbb{R}^{\mathbb{N}}, \mathcal{B}_{\mathbb{R}^{\mathbb{N}}})$ . Then, for  $n \in \mathbb{N}$ , the source vector  $\mathbf{x}$  of length  $n$  is given by  $\mathbf{x} = (x_1, \dots, x_n)^{\top} \in \mathbb{R}^n$ .

**Definition 2.** (Code, achievable rate) For  $\mathbf{x}$  as in Definition 1 and  $\varepsilon > 0$ , an  $(n, m)$  code consists of

- (i) measurements  $|A \cdot | : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq}^m$ ;
- (ii) a decoder  $g : \mathbb{R}_{\geq}^m \rightarrow \mathbb{R}^n$  that is measurable with respect to  $\mathcal{B}_{\mathbb{R}_{\geq}}^m$  and  $\mathcal{B}_{\mathbb{R}^n}$ .

We call  $R$  with  $0 < R \leq 1$  an  $\varepsilon$ -achievable rate if there exists an  $N(\varepsilon) \in \mathbb{N}$  and a sequence of  $(n, \lfloor Rn \rfloor)$  codes with decoders  $g$  such that

$$\mathbb{P}[g(|A\mathbf{x}|) \not\sim \mathbf{x}] \leq \varepsilon$$

for all  $n \geq N(\varepsilon)$ .

Next, we introduce the Minkowski dimension compression rate for source vectors.

**Definition 3.** (Minkowski dimension) Let  $\mathcal{U}$  be a nonempty bounded set in  $\mathbb{R}^n$ . The lower Minkowski dimension of  $\mathcal{U}$  is defined as

$$\underline{\dim}_{\mathbb{B}}(\mathcal{U}) = \liminf_{\rho \rightarrow 0} \frac{\log N_{\mathcal{U}}(\rho)}{\log \frac{1}{\rho}}$$

and the upper Minkowski dimension of  $\mathcal{U}$  is defined as

$$\overline{\dim}_{\mathbb{B}}(\mathcal{U}) = \limsup_{\rho \rightarrow 0} \frac{\log N_{\mathcal{U}}(\rho)}{\log \frac{1}{\rho}}$$

where  $N_{\mathcal{U}}(\rho)$  is the covering number of  $\mathcal{U}$  given by

$$N_{\mathcal{U}}(\rho) = \min \left\{ k \in \mathbb{N} \mid \mathcal{U} \subseteq \bigcup_{i \in \{1, \dots, k\}} \mathcal{B}_n(u_i, \rho), u_i \in \mathbb{R}^n \right\}.$$

If  $\underline{\dim}_{\mathbb{B}}(\mathcal{U}) = \overline{\dim}_{\mathbb{B}}(\mathcal{U})$ , we write  $\dim_{\mathbb{B}}(\mathcal{U})$ .

**Definition 4.** (Minkowski dimension compression rate) For  $\mathbf{x}$  from Definition 1 and  $\varepsilon > 0$ , we define the lower Minkowski dimension compression rate as

$$\begin{aligned} \underline{R}_{\mathbb{B}}(\varepsilon) &= \limsup_{n \rightarrow \infty} \underline{a}_n(\varepsilon), \quad \text{where} \\ \underline{a}_n(\varepsilon) &= \inf \left\{ \frac{\underline{\dim}_{\mathbb{B}}(\mathcal{U})}{n} \mid \mathcal{U} \subset \mathbb{R}^n, \mathbb{P}[\mathbf{x} \in \mathcal{U}] \geq 1 - \varepsilon \right\}. \end{aligned}$$

and the upper Minkowski dimension compression rate as

$$\overline{R}_{\mathbb{B}}(\varepsilon) = \limsup_{n \rightarrow \infty} \overline{a}_n(\varepsilon), \quad \text{where}$$

$$\overline{a}_n(\varepsilon) = \inf \left\{ \frac{\overline{\dim}_{\mathbb{B}}(\mathcal{U})}{n} \mid \mathcal{U} \subset \mathbb{R}^n, \mathbb{P}[\mathbf{x} \in \mathcal{U}] \geq 1 - \varepsilon \right\}.$$

The sets  $\mathcal{U}$  in the definitions for  $\underline{a}_n(\varepsilon)$  and  $\overline{a}_n(\varepsilon)$  are assumed to be nonempty and bounded.

*Example 1.* The source vector  $\mathbf{x}$  from Definition 1 has a mixed discrete-continuous distribution if for each  $n \in \mathbb{N}$  the random variables  $x_i$ ,  $i \in \{1, \dots, n\}$ , are independent and distributed according to

$$\mu_{x_i} = (1 - \lambda)\mu_d + \lambda\mu_c, \quad i \in \{1, \dots, n\}$$

where  $0 \leq \lambda \leq 1$  is the mixing parameter,  $\mu_c$  is a distribution on  $(\mathbb{R}, \mathcal{B}_{\mathbb{R}})$ , absolutely continuous with respect to Lebesgue measure, and  $\mu_d$  is a discrete distribution. Then, [13, Th. 15]

$$\underline{R}_{\mathbb{B}}(\varepsilon) = \overline{R}_{\mathbb{B}}(\varepsilon) = \lambda, \quad 0 < \varepsilon < 1.$$

The following result states that every rate  $R > \underline{R}_{\mathbb{B}}(\varepsilon)$  is  $\varepsilon$ -achievable for Lebesgue a.a. matrices  $A$ .

**Theorem 1.** Let  $0 < \varepsilon < 1$  and  $\mathbf{x}$  as in Definition 1. Then, for Lebesgue a.a. matrices  $A \in \mathbb{R}^{m \times n}$  with  $m = \lfloor Rn \rfloor$ ,  $R$  is an  $\varepsilon$ -achievable rate provided that  $R > \underline{R}_{\mathbb{B}}(\varepsilon)$ .

*Proof.* Since  $R > \underline{R}_{\mathbb{B}}(\varepsilon)$  and  $m = \lfloor Rn \rfloor$ , Definition 4 implies that there exists a sequence of nonempty bounded sets  $\mathcal{U}_n \subseteq \mathbb{R}^n$  and an  $N(\varepsilon) \in \mathbb{N}$  such that

$$\underline{\dim}_{\mathbb{B}}(\mathcal{U}) < m \tag{1}$$

$$\mathbb{P}[\mathbf{x} \in \mathcal{U}] \geq 1 - \varepsilon \tag{2}$$

for all  $\mathcal{U} = \mathcal{U}_n$  with  $n \geq N(\varepsilon)$ . In the remainder of the proof we assume that  $n$  is sufficiently large for (1) and (2) to hold. The claim now follows from Proposition 1 below.  $\square$

**Proposition 1.** Let  $\varepsilon \geq 0$ ,  $\mathbf{x} \in \mathbb{R}^n$  a random vector, and  $\mathcal{U} \subseteq \mathbb{R}^n$  a nonempty bounded set with  $\mathbb{P}[\mathbf{x} \in \mathcal{U}] \geq 1 - \varepsilon$ . Then, for Lebesgue a.a. matrices  $A \in \mathbb{R}^{m \times n}$ , there exists a decoder  $g$  with  $\mathbb{P}[g(|A\mathbf{x}|) \not\sim \mathbf{x}] \leq \varepsilon$  provided that  $\underline{\dim}_{\mathbb{B}}(\mathcal{U}) < m$ .

*Proof.* See Section III.  $\square$

*Remark 1.* By [15, Sec. 3.2, Properties (i)–(iii)], the lower Minkowski dimension of any bounded nonempty subset in  $\mathbb{R}^n$  containing only vectors with no more than  $s$  nonzero entries is at most  $s$ . Therefore, Proposition 1 implies that any  $s$ -sparse random vector  $\mathbf{x} \in \mathbb{R}^n$  can be recovered with arbitrarily small probability of error (by increasing the size of the set  $\mathcal{U}$  in Proposition 1), provided that  $m > s$ . This result holds for an arbitrary distribution of  $\mathbf{x}$  and a.a. matrices  $A \in \mathbb{R}^{m \times n}$ . The best known recovery threshold for deterministic  $s$ -sparse vectors is  $m \geq 2s$  [12].

*Remark 2.* It is worth noting that formally phase retrieval can be formulated as a matrix completion problem with measurements  $y_i^2 = \text{tr}(a_i a_i^{\top} \mathbf{x} \mathbf{x}^{\top})$  using rank-one measurement matrices  $A_i = a_i a_i^{\top}$ ,  $i = 1, \dots, m$ . However, compared to the rank-one measurement matrices used in the matrix completion problem [16], [17], the matrices  $a_i a_i^{\top}$  are symmetric. This complicates the proof of Proposition 1 significantly and forces us to develop a novel concentration of measure result (Lemma

3). On the other hand, in phase retrieval we are interested in recovering symmetric rank-one matrices  $\mathbf{x}\mathbf{x}^\top$  (which is equivalent to the recovery of  $[\mathbf{x}]$ ), whereas matrix completion deals with the recovery of arbitrary low-rank matrices.

In the mixed discrete-continuous case we can strengthen the result of Theorem 1 through the following lemma.

**Lemma 1.** *Let  $0 < \varepsilon < 1$  and  $\mathbf{x}$  be distributed according to the mixed discrete-continuous distribution in Example 1 with mixing parameter  $\lambda$ . Then, for Lebesgue a.a. matrices  $\mathbf{A} \in \mathbb{R}^{m \times n}$  with  $m = \lfloor Rn \rfloor$ ,  $R$  is  $\varepsilon$ -achievable provided that  $R > \lambda$ . Moreover,  $R \geq \lambda$  is also a necessary condition for  $R$  being  $\varepsilon$ -achievable.*

*Proof.* Achievability: Follows from Theorem 1 and Example 1. Converse: Suppose that a rate  $R < \lambda$  is  $\varepsilon$ -achievable for some  $\varepsilon$  with  $0 < \varepsilon < 1$ . This implies that there exists a set  $\mathcal{K} \subseteq \mathbb{R}^n$  and a matrix  $\mathbf{A} \in \mathbb{R}^{m \times n}$  with  $m = \lfloor Rn \rfloor$  such that

- (a)  $\Pr[\mathbf{x} \in \mathcal{K}] \geq 1 - \varepsilon$ ;
- (b)  $|\mathbf{A} \cdot |$  is one-to-one on  $\mathcal{K}_\sim$

for  $n$  sufficiently large. From (b) it follows that there can be at most one equivalence class  $[\mathbf{u}] \in \mathcal{K}_\sim$  with  $\mathbf{A}\mathbf{u} = \mathbf{A}(-\mathbf{u}) = \mathbf{0}$  (if there was more than one such equivalence class then the mapping  $|\mathbf{A} \cdot |$  would not be one-to-one on  $\mathcal{K}_\sim$ ).

Suppose first that there is no equivalence class  $[\mathbf{u}] = \{\mathbf{u}, -\mathbf{u}\} \in \mathcal{K}_\sim$  with  $\mathbf{A}\mathbf{u} = \mathbf{A}(-\mathbf{u}) = \mathbf{0}$  and  $\mathbf{u} \neq \mathbf{0}$ . Then, (b) implies that  $\mathbf{A}$  is one-to-one on  $\mathcal{K}$  which, together with (a) and  $R < \lambda$ , leads to a contradiction to the converse part of [13, Thm. 6].

Now suppose that there is an equivalence class  $[\mathbf{u}] = \{\mathbf{u}, -\mathbf{u}\} \in \mathcal{K}_\sim$  with  $\mathbf{A}\mathbf{u} = \mathbf{A}(-\mathbf{u}) = \mathbf{0}$  and  $\mathbf{u} \neq \mathbf{0}$ . Let  $\tilde{R}$  be such that  $R < \tilde{R} < \lambda$  and set  $\tilde{m} = \lfloor \tilde{R}n \rfloor$ . Then,  $\tilde{m} > m$  for  $n$  sufficiently large. Let  $\tilde{\mathbf{A}} = (\mathbf{A}^\top, \mathbf{u}, 0, \dots, 0)^\top \in \mathbb{R}^{\tilde{m} \times n}$ . Then, (b) implies that  $\tilde{\mathbf{A}}$  is one-to-one on  $\mathcal{K}$  which, together with (a) and  $\tilde{R} < \lambda$ , leads to a contradiction to the converse part of [13, Thm. 6].  $\square$

### III. PROOF OF PROPOSITION 1

Let

$$\mathcal{F}(y) = \left\{ \mathbf{u} \in \mathbb{R}^n \mid \mathbf{u} \in \mathcal{U}, |\mathbf{A}\mathbf{u}| = y \right\} \\ \cup \left\{ \mathbf{u} \in \mathbb{R}^n \mid -\mathbf{u} \in \mathcal{U}, |\mathbf{A}\mathbf{u}| = y \right\}, \quad y \in \mathbb{R}_{\geq}^m.$$

For a vector  $\mathbf{u} \in \mathcal{F}(y) \setminus \{0\}$ , let  $\bar{\mathbf{u}}$  denote the first nonzero component of  $\mathbf{u}$ . We then define the reduced set

$$\bar{\mathcal{F}}(y) = \left\{ \mathbf{u} \in \mathcal{F}(y) \setminus \{0\} \mid \bar{\mathbf{u}} = |\bar{\mathbf{u}}| \right\} \cup (\mathcal{F}(y) \cap \{0\}), \quad y \in \mathbb{R}_{\geq}^m.$$

We define the decoder  $g: \mathbb{R}_{\geq}^m \rightarrow \mathbb{R}^n$  by

$$g(y) = \begin{cases} \mathbf{u}, & \text{if } \bar{\mathcal{F}}(y) = \{\mathbf{u}\} \\ \mathbf{e}, & \text{else} \end{cases}$$

where  $\mathbf{e}$  is some fixed vector in the complement of  $\mathcal{U}$  (used to declare a decoding error). Then, we have

$$\Pr[g(|\mathbf{A}\mathbf{x}|) \not\sim \mathbf{x}] \\ = \Pr[g(|\mathbf{A}\mathbf{x}|) \not\sim \mathbf{x}, \mathbf{x} \in \mathcal{U}] + \Pr[g(|\mathbf{A}\mathbf{x}|) \not\sim \mathbf{x}, \mathbf{x} \notin \mathcal{U}]$$

$$\leq \Pr[g(|\mathbf{A}\mathbf{x}|) \not\sim \mathbf{x}, \mathbf{x} \in \mathcal{U}] + \varepsilon \\ = \Pr[\exists \mathbf{u} \in \mathcal{U} \mid \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|, \mathbf{x} \in \mathcal{U}] + \varepsilon \quad (3)$$

where (3) follows from the definition of the decoder. Fix an arbitrary  $r > 0$ . Suppose that we can show that

$$P(\mathbf{x}) = \Pr[\exists \mathbf{u} \in \mathcal{U} \text{ with } \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|] = 0, \quad \mathbf{x} \in \mathcal{U} \quad (4)$$

where  $\mathbf{A} \in \mathbb{R}^{m \times n}$  has independent rows that are uniformly distributed on  $\mathcal{B}_n(0, r)$ . Then,

$$\int_{\mathcal{A}(r)} \Pr[\exists \mathbf{u} \in \mathcal{U} \mid \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|, \mathbf{x} \in \mathcal{U}] d\mu_{\mathbf{A}} \\ = \int_{\mathcal{U}} \Pr[\exists \mathbf{u} \in \mathcal{U} \text{ with } \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|] d\mu_{\mathbf{x}} \\ = 0 \quad (5)$$

where we used Fubini's Theorem and set  $\mathcal{A}(r) = \mathcal{B}_n(0, r) \times \dots \times \mathcal{B}_n(0, r)$ . Since  $r$  is arbitrary, (5) implies that

$$\Pr[\exists \mathbf{u} \in \mathcal{U} \mid \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|, \mathbf{x} \in \mathcal{U}] = 0 \quad (6)$$

for Lebesgue a.a. matrices  $\mathbf{A}$ . Hence, combining (3) and (6) proves the Proposition provided that we can show that (4) holds, which is done in Section IV.

### IV. PROOF OF (4)

Suppose first that  $\mathbf{x} = \mathbf{0}$ . Then,  $P(\mathbf{x}) = 0$  if and only if

$$\Pr[\exists \mathbf{u} \in \mathcal{U} \setminus \{0\} \text{ with } \mathbf{A}\mathbf{u} = \mathbf{0}] = 0. \quad (7)$$

Since  $\dim_{\mathbb{B}}(\mathcal{U}) < m$ , (7) follows from [14, Prop. 1]. Therefore, we can assume in what follows that  $\mathbf{x} \neq \mathbf{0}$ .

We can upper-bound  $P(\mathbf{x}) \leq P_1(\mathbf{x}) + P_2(\mathbf{x})$  with

$$P_i(\mathbf{x}) = \Pr[\exists \mathbf{u} \in \mathcal{U}_i(\mathbf{x}) \text{ with } |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|], \quad i \in \{1, 2\}$$

where we defined

$$\mathcal{U}_1(\mathbf{x}) = \{\mathbf{u} \in \mathcal{U} \mid \text{rank}(\mathbf{x}, \mathbf{u}) = 2\} \\ \mathcal{U}_2(\mathbf{x}) = \{\mathbf{u} \in \mathcal{U} \mid \text{rank}(\mathbf{x}, \mathbf{u}) = 1\} \setminus \{\mathbf{u} \in \mathcal{U} \mid \mathbf{u} \sim \mathbf{x}\}.$$

We have to show that  $P_i(\mathbf{x}) = 0$  for  $i \in \{1, 2\}$ . First, we establish  $P_2(\mathbf{x}) = 0$ . We have (recall that  $\mathbf{x} \neq \mathbf{0}$ )

$$P_2(\mathbf{x}) \\ = \Pr[\exists \mathbf{u} \in \mathcal{U} \text{ with } \text{rank}(\mathbf{x}, \mathbf{u}) = 1, \mathbf{u} \not\sim \mathbf{x}, |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|] \\ = \Pr[\mathbf{A}\mathbf{x} = \mathbf{0}] \\ = 0$$

where we used [14, Prop. 1] together with  $\dim_{\mathbb{B}}(\{\mathbf{x}\}) = 0$  in the last step. It remains to show that  $P_1(\mathbf{x}) = 0$ . To this end, we first present an auxiliary lemma.

**Lemma 2.** *Let  $r > 0$ ,  $\emptyset \neq \mathcal{S} \subseteq \mathcal{B}_n(0, L)$ ,  $\rho > 0$ ,  $\mathbf{x} \in \mathcal{B}_n(0, L)$ , and  $\mathbf{A} \in \mathbb{R}^{m \times n}$  with independent rows that are uniformly distributed on  $\mathcal{B}_n(0, r)$ . Then, there exist  $s_1(\rho) \in \mathcal{S}$ ,*

$l = 1, \dots, N_S(\rho)$  with  $N_S(\rho)$  being the covering number of  $\mathcal{S}$ , such that

$$\begin{aligned} & \mathbb{P}[\exists \mathbf{u} \in \mathcal{S} \text{ with } \|\mathbf{A}\mathbf{u} - \mathbf{A}\mathbf{x}\| \leq \rho] \\ & \leq \sum_{l=1}^{N_S(\rho)} \mathbb{P}[|\mathbf{a}^\top \mathbf{s}_l(\rho)|^2 - |\mathbf{a}^\top \mathbf{x}|^2 \leq 2Lr(2r+1)\rho]^m \end{aligned} \quad (8)$$

where  $\mathbf{a}$  is uniformly distributed on  $\mathcal{B}_n(0, r)$ .

*Proof.* Let  $\mathcal{S} \subseteq \bigcup_{l \in \{1, \dots, N_S(\rho)\}} \mathcal{B}_n(\mathbf{v}_l(\rho), \rho)$ ,  $\mathbf{v}_l(\rho) \in \mathbb{R}^n$ , be a *minimal* covering of  $\mathcal{S}$  according to the definition of the covering number, cf. Definition 3. Then, there exist  $\mathbf{s}_l(\rho) \in \mathcal{S} \cap \mathcal{B}_n(\mathbf{v}_l(\rho), \rho)$  for all  $l = 1, \dots, N_S(\rho)$ . Hence, the balls  $\mathcal{B}_n(\mathbf{s}_l(\rho), 2\rho)$  cover the set  $\mathcal{S}$  and have centers in  $\mathcal{S}$ . We can upper bound the lhs in (8) by

$$\begin{aligned} & \mathbb{P}[\exists \mathbf{u} \in \mathcal{S} \text{ with } \|\mathbf{A}\mathbf{u} - \mathbf{A}\mathbf{x}\| \leq \rho] \\ & \leq \sum_{l=1}^{N_S(\rho)} \mathbb{P}[\exists \mathbf{u} \in \mathcal{S} \cap \mathcal{B}_n(\mathbf{s}_l(\rho), 2\rho) \text{ with } \|\mathbf{A}\mathbf{u} - \mathbf{A}\mathbf{x}\| \leq \rho] \\ & \leq \sum_{l=1}^{N_S(\rho)} \mathbb{P}[\exists \mathbf{u} \in \mathcal{S} \cap \mathcal{B}_n(\mathbf{s}_l(\rho), 2\rho) \text{ with } |\mathbf{a}^\top \mathbf{u} - \mathbf{a}^\top \mathbf{x}| \leq \rho]^m \end{aligned} \quad (9)$$

where (9) follows from the fact that the rows of  $\mathbf{A}$  are independent and uniformly distributed on  $\mathcal{B}_n(0, r)$ . Using the triangle inequality we obtain

$$|\mathbf{a}^\top \mathbf{s}_l(\rho) - \mathbf{a}^\top \mathbf{x}| \leq |\mathbf{a}^\top \mathbf{x} - \mathbf{a}^\top \mathbf{u}| + |\mathbf{a}^\top \mathbf{u} - \mathbf{a}^\top \mathbf{s}_l(\rho)|. \quad (10)$$

The second term on the rhs of (10) can be further upper bounded by

$$\begin{aligned} |\mathbf{a}^\top \mathbf{u} - \mathbf{a}^\top \mathbf{s}_l(\rho)| & \leq |\mathbf{a}^\top (\mathbf{u} - \mathbf{s}_l(\rho))| \\ & \leq \|\mathbf{a}\| \|\mathbf{u} - \mathbf{s}_l(\rho)\| \\ & \leq 2r\rho \end{aligned} \quad (11)$$

where (11) follows from  $\mathbf{u} \in \mathcal{B}_n(\mathbf{s}_l(\rho), 2\rho)$  and  $\mathbf{a} \in \mathcal{B}_n(0, r)$ . Combining (10) and (11) gives

$$|\mathbf{a}^\top \mathbf{x} - \mathbf{a}^\top \mathbf{u}| \geq |\mathbf{a}^\top \mathbf{s}_l(\rho) - \mathbf{a}^\top \mathbf{x}| - 2r\rho. \quad (12)$$

Using (12) in (9) yields

$$\begin{aligned} & \mathbb{P}[\exists \mathbf{u} \in \mathcal{S} \text{ with } \|\mathbf{A}\mathbf{u} - \mathbf{A}\mathbf{x}\| \leq \rho] \\ & \leq \sum_{l=1}^{N_S(\rho)} \mathbb{P}[|\mathbf{a}^\top \mathbf{s}_l(\rho) - \mathbf{a}^\top \mathbf{x}| \leq (2r+1)\rho]^m \\ & \leq \sum_{l=1}^{N_S(\rho)} \mathbb{P}[|\mathbf{a}^\top \mathbf{s}_l(\rho)|^2 - |\mathbf{a}^\top \mathbf{x}|^2 \leq 2Lr(2r+1)\rho]^m \end{aligned} \quad (13)$$

where (13) follows from  $|\mathbf{a}^\top \mathbf{s}_l(\rho)|^2 - |\mathbf{a}^\top \mathbf{x}|^2 = (|\mathbf{a}^\top \mathbf{s}_l(\rho)| + |\mathbf{a}^\top \mathbf{x}|)(|\mathbf{a}^\top \mathbf{s}_l(\rho)| - |\mathbf{a}^\top \mathbf{x}|) \leq 2Lr(|\mathbf{a}^\top \mathbf{s}_l(\rho)| - |\mathbf{a}^\top \mathbf{x}|)$ .  $\square$

We now continue with the proof of  $P_1(\mathbf{x}) = 0$ . Since  $\mathcal{U}$  is a bounded set, there exists an  $L \in \mathbb{R}$  such that

$$\|\mathbf{u}\| \leq L, \quad \mathbf{u} \in \mathcal{U}. \quad (14)$$

We define the sets  $\mathcal{T}_j(\mathbf{x})$  by

$$\mathcal{T}_j(\mathbf{x}) = \left\{ \mathbf{u} \in \mathcal{U}_1(\mathbf{x}) \mid \sqrt{\|\mathbf{u}\|^2 \|\mathbf{x}\|^2 - |\mathbf{u}^\top \mathbf{x}|^2} > \frac{1}{j} \right\}, \quad j \in \mathbb{N}.$$

Since

$$P_1(\mathbf{x}) \leq \sum_{j \in \mathbb{N}} \mathbb{P}[\exists \mathbf{u} \in \mathcal{T}_j(\mathbf{x}) \text{ with } |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|]$$

it is sufficient to prove that

$$P_1^{(j)}(\mathbf{x}) = \mathbb{P}[\exists \mathbf{u} \in \mathcal{T}_j(\mathbf{x}) \text{ with } |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|] = 0$$

for all  $j \in \mathbb{N}$ . Suppose, by contradiction, that there exists a  $j \in \mathbb{N}$  such that  $P_1^{(j)}(\mathbf{x}) > 0$ . Then,

$$\liminf_{\rho \rightarrow 0} \frac{\log P_1^{(j)}(\mathbf{x})}{\log \frac{1}{\rho}} = 0. \quad (15)$$

Furthermore,  $\mathcal{T}_j(\mathbf{x}) \neq \emptyset$  and by [15, Sec. 3.2, Property (ii)] (recall that  $\mathcal{T}_j(\mathbf{x}) \subseteq \mathcal{U}_1(\mathbf{x}) \subseteq \mathcal{U}$ ) we get

$$\underline{\dim}_{\mathbb{B}}(\mathcal{T}_j(\mathbf{x})) < m. \quad (16)$$

We have

$$\begin{aligned} & \liminf_{\rho \rightarrow 0} \frac{\log P_1^{(j)}(\mathbf{x})}{\log \frac{1}{\rho}} \\ & = \liminf_{\rho \rightarrow 0} \frac{\log \mathbb{P}[\exists \mathbf{u} \in \mathcal{T}_j(\mathbf{x}) \text{ with } |\mathbf{A}\mathbf{u}| = |\mathbf{A}\mathbf{x}|]}{\log \frac{1}{\rho}} \\ & \leq \liminf_{\rho \rightarrow 0} \frac{\log \left( \sum_{l=1}^{N_{\mathcal{T}_j(\mathbf{x})}(\rho)} \mathbb{P}[|\mathbf{a}^\top \mathbf{s}_l^{(j)}(\rho, \mathbf{x})|^2 - |\mathbf{a}^\top \mathbf{x}|^2 \leq \tilde{\rho}]^m \right)}{\log \frac{1}{\rho}} \end{aligned} \quad (17)$$

$$\leq \liminf_{\rho \rightarrow 0} \frac{\log \left( \tilde{\rho}^m \sum_{l=1}^{N_{\mathcal{T}_j(\mathbf{x})}(\rho)} f(\tilde{\rho}, r, \mathbf{s}_l^{(j)}(\rho, \mathbf{x}), \mathbf{x})^m \right)}{\log \frac{1}{\rho}} \quad (18)$$

$$\leq \liminf_{\rho \rightarrow 0} \frac{\log \left( \tilde{\rho}^m N_{\mathcal{T}_j(\mathbf{x})}(\rho) \tilde{f}(\tilde{\rho}, r, L, j)^m \right)}{\log \frac{1}{\rho}} \quad (19)$$

$$\begin{aligned} & = \underline{\dim}_{\mathbb{B}}(\mathcal{T}_j(\mathbf{x})) - m + m \lim_{\rho \rightarrow 0} \frac{\log \tilde{f}(\tilde{\rho}, r, L, j)}{\log \frac{1}{\rho}} \\ & = \underline{\dim}_{\mathbb{B}}(\mathcal{T}_j(\mathbf{x})) - m \\ & < 0 \end{aligned} \quad (20)$$

where in (17) we applied Lemma 2 with  $\mathcal{S} = \mathcal{T}_j(\mathbf{x})$  and set  $\tilde{\rho} = 2Lr(2r+1)\rho$ , (18) follows from Lemma 3 below with  $\mathbf{u} = \mathbf{s}_l^{(j)}(\rho, \mathbf{x})$ ,  $\mathbf{v} = \mathbf{x}$ , and  $\delta = \tilde{\rho}$  where  $f$  is defined in (22), in (19) we used that

$$\begin{aligned} & f(\tilde{\rho}, r, \mathbf{s}_l^{(j)}(\rho, \mathbf{x}), \mathbf{x}) \\ & \leq \tilde{f}(\tilde{\rho}, r, L, j) \\ & = \frac{2(2r)^{n-2}j}{V(n, r)} \left( 1 + \log \left( 2 + \frac{8r^2 L^2}{\tilde{\rho}} \right) \right), \quad l = 1, \dots, N_{\mathcal{T}_j(\mathbf{x})}(\rho) \end{aligned}$$

which follows from (14) and the fact that  $\mathbf{s}_l^{(j)}(\rho, \mathbf{x}) \in \mathcal{T}_j(\mathbf{x})$ ,  $l = 1, \dots, N_{\mathcal{T}_j(\mathbf{x})}(\rho)$ , and in (20) we applied (16). But (20) is

a contradiction to (15). Therefore,  $P_1^{(j)}(x) = 0$  for all  $j \in \mathbb{N}$ , which implies in turn that  $P_1(x) = 0$  and concludes the proof of (4).

### V. CONCENTRATION OF MEASURE RESULT

**Lemma 3.** *Let  $r > 0$ ,  $\mathbf{a}$  be uniformly distributed on  $\mathcal{B}_n(0, r)$ ,  $C = \mathbf{u}\mathbf{u}^\top - \mathbf{v}\mathbf{v}^\top$  with linearly independent vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ , and  $\delta > 0$ . Then,*

$$\mathbb{P}[|\mathbf{a}^\top C \mathbf{a}| \leq \delta] \leq \delta f(\delta, r, \mathbf{u}, \mathbf{v}) \quad (21)$$

with

$$f(\delta, r, \mathbf{u}, \mathbf{v}) = \frac{2(2r)^{n-2} \left( 1 + \log \left( 2 + \frac{2r^2 (\|\mathbf{u} + \mathbf{v}\| \|\mathbf{u} - \mathbf{v}\| - \|\mathbf{u}\|^2 - \|\mathbf{v}\|^2)}{\delta} \right) \right)}{\sqrt{\|\mathbf{u}\|^2 \|\mathbf{v}\|^2 - |\mathbf{u}^\top \mathbf{v}|^2} V(n, r)} \quad (22)$$

*Proof.* The detailed proof can be found in the arXiv version of this paper [18]. Here, we present a sketch of the proof. Since the two vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$  are linearly independent, the matrix  $C$  has two nonzero eigenvalues  $\lambda_1$  and  $-\lambda_2$ . It can be shown that one nonzero eigenvalue of  $C$ , say  $\lambda_1$ , is positive and the other nonzero eigenvalue of  $C$ , say  $-\lambda_2$ , is negative. Furthermore, we can assume without loss of generality that  $\lambda_1 \geq \lambda_2$ . We have

$$\begin{aligned} \mathbb{P}[|\mathbf{a}^\top C \mathbf{a}| \leq \delta] &= \frac{1}{V(n, r)} \int_{\mathcal{B}_n(0, r)} \chi_{\{\mathbf{a} \in \mathbb{R}^n \mid |\mathbf{a}^\top C \mathbf{a}| < \delta\}} d\mathbf{a} \\ &\leq \frac{(2r)^{n-2}}{V(n, r)} \int_{\mathcal{B}_2(0, r)} \chi_{\{\mathbf{b} \in \mathbb{R}^2 \mid |\lambda_1 b_1^2 - \lambda_2 b_2^2| < \delta\}} d\mathbf{b} \\ &= \frac{(2r)^{n-2}}{\sqrt{\lambda_1 \lambda_2} V(n, r)} \int_{\mathbb{R}^2} \chi_{\left\{ \mathbf{t} \in \mathbb{R}^2 \mid \frac{t_1^2}{\lambda_1} + \frac{t_2^2}{\lambda_2} \leq r^2 \right\}} \\ &\quad \times \chi_{\left\{ \mathbf{t} \in \mathbb{R}^2 \mid |t_1^2 - t_2^2| < \delta \right\}} dt \quad (23) \end{aligned}$$

$$\begin{aligned} &\leq \frac{(2r)^{n-2}}{\sqrt{\lambda_1 \lambda_2} V(n, r)} \int_{\mathbb{R}^2} \chi_{\left\{ \mathbf{t} \in \mathbb{R}^2 \mid t_1^2 \leq \lambda_1 r^2, t_2^2 \leq \lambda_2 r^2 \right\}} \\ &\quad \times \chi_{\left\{ \mathbf{t} \in \mathbb{R}^2 \mid |t_1^2 - t_2^2| < \delta \right\}} dt \quad (24) \end{aligned}$$

where in (23) we changed variables to  $\mathbf{t} = \text{diag}(\sqrt{\lambda_1}, \sqrt{\lambda_2})\mathbf{b}$ . The integral in (24) measures the area that is inside the rectangle  $\{\mathbf{t} \mid t_1^2 \leq \lambda_1 r^2, t_2^2 \leq \lambda_2 r^2\}$  and the two hyperbolas  $\{\mathbf{t} \mid t_1^2 - t_2^2 = \pm \delta\}$  (see Figure 1). The bound (21) can then be established by performing the following two steps:

- 1) finding an expression of the eigenvalues of  $C$  in terms of the vectors  $\mathbf{u}$  and  $\mathbf{v}$ ;
- 2) deriving an upper bound on the integral in (24).

□

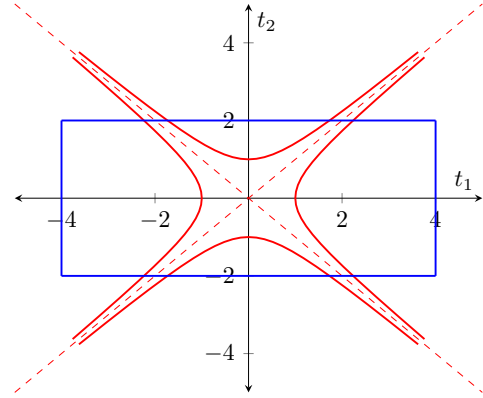


Fig. 1. Intersection of the rectangle  $\{\mathbf{t} \mid t_1^2 \leq \lambda_1 r^2, t_2^2 \leq \lambda_2 r^2\}$  with the two hyperbolas  $\{\mathbf{t} \mid t_1^2 - t_2^2 = \pm \delta\}$  for  $\delta = 1$ ,  $\lambda_1 = 16/r^2$ , and  $\lambda_2 = 4/r^2$ .

### REFERENCES

- [1] R. P. Millane, "Phase retrieval in crystallography and optics," *J. Opt. Soc. Am. A*, vol. 7, no. 3, pp. 394–411, 1990.
- [2] J. R. Fienup, J. C. Marron, T. J. Schulz, and J. H. Seldin, "Hubble space telescope characterized by using phase-retrieval algorithms," *Appl. Opt.*, vol. 32, no. 10, pp. 1747–1767, 1993.
- [3] H. M. Quiney, "Coherent diffractive imaging using short wavelength light sources," *J. Mod. Opt.*, vol. 57, no. 13, pp. 1109–1149, 2010.
- [4] Y. M. Bruck and L. Sodin, "On the ambiguity of the image reconstruction problem," *Opt. Comm.*, vol. 30, no. 3, pp. 304–308, 1979.
- [5] R. Balan, P. Casazza, and D. Edidin, "On signal reconstruction without phase," *Appl. Comput. Harmon. Anal.*, vol. 20, no. 3, pp. 345–356, 2006.
- [6] E. J. Candès and X. Li, "Solving quadratic equations via PhaseLift when there are about as many equations as unknowns," *Found. Comput. Mathematics*, vol. 14, no. 5, pp. 1017–1026, 2012.
- [7] E. J. Candès, Y. C. Eldar, T. Strohmer, and V. Voroninski, "Phase retrieval via matrix completion," *SIAM J. on Imag. Sciences*, vol. 6, no. 1, pp. 199–225, 2013.
- [8] I. Waldspurger, A. d'Aspremont, and S. Mallat, "Phase recovery, Max-Cut and complex semidefinite programming," *Mathematical Programming*, vol. 149, no. 1-2, pp. 47–81, 2015.
- [9] P. Netrapalli, P. Jain, and S. Sanghavi, "Phase retrieval using alternating minimization," in *Advances in Neural Information Processing Systems 26*, C. Burges, L. Bottou, M. Welling, Z. Ghahramani, and K. Weinberger, Eds. Curran Associates, Inc., 2013, pp. 2796–2804.
- [10] E. J. Candès, X. Li, and M. Soltanolkotab, "Phase retrieval via Wirtinger flow: Theory and algorithms," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1985–2007, April 2015.
- [11] Y. C. Eldar and S. Mendelson, "Phase retrieval: Stability and recovery guarantees," *Appl. Comput. Harmon. Anal.*, vol. 36, no. 3, pp. 473–494, 2014.
- [12] M. Akçakaya and V. Tarokh, "New conditions for sparse phase retrieval," 2014, arXiv:1310.1351 [cs.IT].
- [13] Y. Wu and S. Verdú, "Rényi information dimension: Fundamental limits of almost lossless analog compression," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3721–3748, Aug. 2010.
- [14] D. Stotz, E. Riegler, and H. Bölcskei, "Almost lossless analog signal separation," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, Jul. 2013, pp. 106–110.
- [15] K. Falconer, *Fractal Geometry*, 1st ed. New York, NY: Wiley, 1990.
- [16] T. T. Cai and A. Zhang, "Sparse representation of a polytope and recovery in sparse signals and low-rank matrices," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 122–132, Jan. 2014.
- [17] E. Riegler, D. Stotz, and H. Bölcskei, "Information-theoretic limits of matrix completion," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, arXiv:1504.04970 [cs.IT].
- [18] E. Riegler and G. Tauböck, "Almost lossless analog compression without phase information," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, arXiv:1504.03024 [cs.IT].