

The Algebraic Approach to Phase Retrieval, and Explicit Inversion at the Identifiability Threshold

Franz J. Király* Martin Ehler†

February 18, 2014

Abstract

We study phase retrieval from magnitude measurements of an unknown signal as an algebraic estimation problem. Indeed, phase retrieval from rank-one and more general linear measurements can be treated in an algebraic way. It is verified that a certain number of generic rank-one or generic linear measurements are sufficient to enable signal reconstruction for generic signals, and slightly more generic measurements yield reconstructability for all signals. Our results solve a few open problems stated in the recent literature. Furthermore, we show how the algebraic estimation problem can be solved by a closed-form algebraic estimation technique, termed ideal regression, providing non-asymptotic success guarantees.

1. Introduction

Intensity measurements in diffraction imaging, microscopy, and x -ray crystallography represent magnitudes of Fourier samples, and the recovery of their phases is a difficult problem in optical physics. Within a finite model, phase retrieval is the task of reconstructing a vector in \mathbb{K}^d from the magnitude of finitely many rank-1 projections. Classical algorithms are due to Gerchberg/Saxton [14] and Fienup [13] involving alternate projection schemes and fit into standard methods from convex optimization [7], but signal reconstruction is not guaranteed. Sparse nonconvex optimization is applied in [2]. Semidefinite programming is used in [10], but success guarantees are only obtained asymptotically with growing dimension. Algebraic reconstruction formulas were derived in [5], but require the number of measurements to scale quadratically with the dimension. Jointly, algebraic reconstruction and semidefinite programs were applied in [1] to treat rank- k projectors. For further approaches rooted in signal processing, we refer to [12, 19] and references therein.

To successfully reconstruct, measurements must contain sufficient information about the signal. If the number of rank-one magnitude measurements is sufficiently large, then generic measurements allow identifiability of all signals, and there is a range of fewer measurements, in which at least generic signals can still be identified, cf. [4]. Measurements using orthogonal projectors of arbitrary rank have been discussed in [9], from where we cite the following open problems:

- (1) What is the minimal number of orthogonal projectors enabling phase retrieval for all signals in the real case?
- (2) Do sufficiently many generic orthogonal projectors enable phase retrieval for all signals in the real case?

*Department of Statistical Science, University College London; and MFO; f.kiraly@ucl.ac.uk

†Department of Mathematics, University of Vienna, martin.ehler@univie.ac.at

- (3) Does the minimal number of required orthogonal projectors for retrieving phases for all signals in the complex case depend on the rank of the projectors?

In view of investigating the above mentioned transition range from generic to identifiability of all signals, we derive three additional questions

(4-6) by replacing “for all signals” in (1-3) with “generic signals”.

Furthermore, the results in [3, 8] directly lead to one more question, which is formulated as a conjecture in [6]:

- (7) Do $4n - 4$ generic rank-one measurements allow phase retrieval for all signals in the complex case?

So besides the aim for a better understanding of the structure of phase retrieval in general, we are also left with 7 open problems that we intend to solve.

In this paper, we claim that phase retrieval is in its core an algebraic problem and emphasize the potential of algebraic tools. This change of perspective enables us to not only answer all of the 7 above questions, but we can also apply symbolic computations and schemes from approximate algebra to design a reconstruction algorithm. Indeed, we observe that phase retrieval can be tackled by ideal regression as introduced in [17] leading to an algebraic signal reconstruction algorithm for few measurements with nonasymptotic success guarantees.

A short note on question 7

We would like to note that after submission of this paper, question 7 has independently been answered in [11] by different techniques. The approach of [11] is more specifically designed for that question, and uses very explicit computations which are not essentially required to obtain the result since it follows from general principles, as we show. On the same note, the article [11] contains interesting structural results which can be appreciated independently from question 7.

2. The Algebra of Phase Retrieval

2.1. Algebraization of Phase Retrieval

In this section, we will describe how phase retrieval can be viewed as an algebraic problem. This will be crucial in deriving algebraic solution techniques for phase retrieval. In the usual formulation, the two variants of phase retrieval pose two differently flavoured major obstacles to amenability for algebraic tools: in the real formulation, the mapping is algebraic, but the ground field, the real numbers \mathbb{R} , is not algebraically closed. In the complex formulation, the ground field \mathbb{C} is algebraically closed, but the measurement mapping includes complex conjugation, making it non-algebraic. The latter problem can be overcome - as it has been demonstrated for example in [4], by treating the real and imaginary part separately, making the mapping algebraic, but the ground field real in its stead, and therefore reducing the second problem to the first one.

We will overcome this obstacle by, again, regarding the algebraic mapping over the complex numbers as base field, and restricting back to the reals when necessary. This procedure will allow us to algebraize the measurement process, derive theoretical bounds on reconstructability, and develop accurate reconstruction algorithms.

First we recapitulate the measurement process:

Problem 2.1 (Phase Retrieval, original version). Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. Let $z \in \mathbb{K}^n$ be an unknown vector. Let $P_1, \dots, P_k \in \mathbb{K}^{r \times n}$ be known matrices. Reconstruct z from the measurements

$$b_i = \|P_i z\|^2 = \text{Tr}(z z^* \cdot P_i^* P_i), \quad 1 \leq i \leq k,$$

and the knowledge of the P_i .

In the usual phase retrieval scenario, the P_i are projectors of rank one. The slightly generalized setting above can be treated with the same mathematical and algorithmical tools, so it means no loss of generality or specificity. Also note that if $\mathbb{K} = \mathbb{R}$, then z can be reconstructed only up to sign, and if $\mathbb{K} = \mathbb{C}$, then only up to phase.

We will now stepwise reformulate the problem, in order to make it amenable to algebraic tools. First we note that phase retrieval is known to be an inverse problem. That is, there is a so-called forward mapping, which takes the (unknown to the observer) signal z , and outputs the (observed) values b_i . The backward problem is then to obtain z from the b_i . Since z can be obtained only up to sign or phase, this is equivalent to obtaining the matrix $Z = z z^*$. Writing all of this explicitly, we obtain as a reformulation of the original Problem 2.1 the following inverse problem:

Problem 2.2. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. Consider the forward mapping

$$\begin{aligned} \phi : (\mathbb{K}^{r \times n})^k \times \mathbb{K}^{n \times n} &\rightarrow (\mathbb{K}^{r \times n})^k \times \mathbb{K}^k \\ (P_1, \dots, P_k, Z) &\mapsto (P_1, \dots, P_k, \text{Tr}(Z \cdot P_1^* P_1), \dots, \text{Tr}(Z \cdot P_k^* P_k)). \end{aligned}$$

Reconstruct $\tau := (P_1, \dots, P_k, Z)$, given $\phi(\tau)$, and assuming that Z is rank one and Hermitian.

Note that we have deliberately included the P_i in the range and the image of ϕ , in order to mathematically model the fact that the projectors P_i are known to the observer; and for technical reasons - equivalent to the latter - which will become apparent further on. Furthermore, assuming that Z is rank one and Hermitian is equivalent to assuming that $Z = z z^*$ for suitable z , since knowing Z is equivalent to know z up to sign/phase.

As said in the beginning, there are two major difficulties in applying algebraic techniques to Problem 2.2. The first is that (A) the base field is not algebraically closed if $\mathbb{K} = \mathbb{R}$, the second being that (B) the mapping ϕ is not algebraic if $\mathbb{K} = \mathbb{C}$, since it includes complex conjugation. The solution approach for problem (A) is relatively straightforward: since the mapping ϕ includes only transposes, it is algebraic, therefore we consider the same mapping over the complex numbers. Also, we replace the matrices $P_i \in \mathbb{R}^{r \times n}$ by matrices $A_i := P_i^\top P_i$ for reason of convenience:

Problem 2.3. Let $z \in \mathbb{C}^n$ be an unknown vector. Consider the forward mapping

$$\begin{aligned} \phi : (\mathbb{C}^{n \times n})^k \times \mathbb{C}^{n \times n} &\rightarrow (\mathbb{C}^{n \times n})^k \times \mathbb{C}^k \\ (A_1, \dots, A_k, Z) &\mapsto (A_1, \dots, A_k, \text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_k)) \end{aligned}$$

Reconstruct $\tau := (A_1, \dots, A_k, Z)$, given $\phi(\tau)$, and assuming that Z is symmetric rank one, and that the A_i are symmetric of rank r .

There are now several things to note: first, the map ϕ is algebraic, and range and image are now complex. In particular, the measurements can be complex. Note that we want both Z and A_i to be symmetric, not Hermitian, otherwise the problem would not be algebraic.

Most importantly, however, Problem 2.3 is a problem which is a-priori different from Problem 2.2, since we have enlarged image and range. When restricting to reals, we obtain the original phase retrieval Problem 2.2, but there is no a-priori reason to believe that the behavior of the complex variant is fundamentally the same as for the original problem.

However, as will turn out, Problem 2.3 is much easier amenable to tools from algebraic geometry, both on the theoretical and the practical side, and results and algorithms will give rise to

solutions for questions and tasks over the reals, as it will be explained in the following section.

We proceed treating the variant of the phase retrieval problem 2.2 where complex signals are allowed. Recall that the problem was that (B) the map ϕ is not algebraic. The solution for this is to “algebraize” the map by considering real and imaginary part separately. Namely, writing $P_i = Q_i + \iota \cdot S_i$ with $Q_i, S_i \in \mathbb{R}^{m \times n}$ and $z = x + \iota y$, where ι denotes the imaginary unit, we obtain:

Problem 2.4. Let $x, y \in \mathbb{R}^n$ be unknown vectors, write $R := xx^\top + yy^\top$ and $\Phi := yx^\top - xy^\top$. Also, write $B_i := Q_i^\top Q_i + S_i^\top S_i$ and $C_i := Q_i^\top S_i - S_i^\top Q_i$ for $Q_i, S_i \in \mathbb{R}^{m \times n}$. Consider the forward mapping

$$\begin{aligned} \phi : (\mathbb{R}^{n \times n})^{2k} \times \mathbb{R}^n &\rightarrow (\mathbb{R}^{n \times n})^{2k} \times \mathbb{R}^k \\ (B_1, C_1, \dots, B_k, C_k, R, \Phi) &\mapsto (B_1, C_1, \dots, B_k, C_k, \text{Tr}(R \cdot B_1 + \Phi \cdot C_1), \dots, \text{Tr}(R \cdot B_n + \Phi \cdot C_n)) \end{aligned}$$

Reconstruct $\tau = (B_1, C_1, \dots, B_k, C_k, R, \Phi)$, given $\phi(\tau)$, assuming that B_i, C_i, R, Φ were of the above form.

An elementary computation shows that Problem 2.4 is equivalent to the original complex phase retrieval problem 2.1: namely, $zz^* = R + \iota\Phi$, so knowing R and Φ is equivalent to knowing z up to phase. Observe that ϕ is now an algebraic map, since the rule is algebraic, and so is the possible set of B_i, C_i, X, Y . However, the mapping ϕ is now over the reals, a field which is not algebraically closed, entailing an analogue of complication (A) which we have treated in the real case by allowing complex matrices in the range. We will once more do the same and allow a complex range. The set of matrices though have a very specific structure, so we introduce notation for them in our final formulation of the complex phase retrieval problem:

Problem 2.5 (algebraized phase retrieval of complex signal). Define the following sets of matrices:

$$\begin{aligned} \mathcal{S}_{\mathbb{C}} &:= \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{C}^n\} \subseteq \mathbb{C}^{n \times n} \times \mathbb{C}^{n \times n} \\ \mathcal{P}_{\mathbb{C}}(r) &:= \{(Q^\top Q + S^\top S, Q^\top S - S^\top Q) : S, Q \in \mathbb{C}^{r \times n}\} \subseteq \mathbb{C}^{n \times n} \times \mathbb{C}^{n \times n} \end{aligned}$$

Consider the forward mapping

$$\begin{aligned} \phi : \mathcal{P}_{\mathbb{C}}(r)^k \times \mathcal{S}_{\mathbb{C}} &\rightarrow \mathcal{P}_{\mathbb{C}}(r)^k \times \mathbb{C}^k \\ (B_1, C_1, \dots, B_k, C_k, R, \Phi) &\mapsto (B_1, C_1, \dots, B_k, C_k, \text{Tr}(R \cdot B_1 + \Phi \cdot C_1), \dots, \text{Tr}(R \cdot B_n + \Phi \cdot C_n)) \end{aligned}$$

Given $\tau = \phi(B_1, C_1, \dots, B_k, C_k, R, \Phi)$, determine $\phi^{-1}(\tau)$.

The set $\mathcal{S}_{\mathbb{C}}$ parameterizes the possible signals, while $\mathcal{P}_{\mathbb{C}}(r)$ parameterizes the possible projections (of rank r). Note that $\mathcal{S}_{\mathbb{C}} = \mathcal{P}_{\mathbb{C}}(1)$; nevertheless we make this notational distinction between $\mathcal{S}_{\mathbb{C}}$ and $\mathcal{P}_{\mathbb{C}}(\cdot)$ for clarity.

We reformulate the phase retrieval problem for real signals in analogy, by defining symbols for the space of matrices, yielding in the final version:

Problem 2.6 (algebraized phase retrieval of real signal). Define the following sets of matrices:

$$\begin{aligned} \mathcal{S}_{\rho} &:= \{zz^\top : z \in \mathbb{C}^n\} \subseteq \mathbb{C}^{n \times n} \\ \mathcal{P}_{\rho}(r) &:= \{P_i^\top P_i : P_i \in \mathbb{C}^{r \times n}\} \subseteq \mathbb{C}^{n \times n} \end{aligned}$$

Consider the forward mapping

$$\begin{aligned} \phi : \mathcal{P}_{\mathbb{R}}(r)^k \times \mathcal{S}_{\mathbb{R}} &\rightarrow \mathcal{P}_{\mathbb{R}}(r)^k \times \mathbb{C}^k \\ (A_1, \dots, A_k, Z) &\mapsto (A_1, \dots, A_k, \text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_n)) \end{aligned}$$

Given $\tau = \phi(A_1, \dots, A_k, Z)$, determine $\phi^{-1}(\tau)$.

Observe that \mathcal{S}_ρ models the possible signals, and is exactly the set of symmetric complex matrices of rank 1 (or less), whereas $\mathcal{P}_\rho(r)$ models the projections, and is exactly the set of symmetric complex matrices of rank r (or less). Note that we have formulated both the real and the complex problem with almost the same forward mapping, the difference lies in the different sets of projection matrices, where in the real case we have single matrices, and in the complex case we have related pairs. Also, for the complex variant of phase retrieval, we have related pairs of matrices R and Φ instead of the single matrix Z .

In order to make the notation uniform for both the real and complex cases, we introduce the following convention:

Notation 2.7. Let $Z, A \in \mathbb{C}^{n \times n} \times \mathbb{C}^{n \times n}$, with $Z = (X, Y)$ and $A = (B, C)$. Then, we will write, by convention,

$$\text{Tr}(Z \cdot A) := \text{Tr}(X \cdot B + Y \cdot C).$$

2.2. Identifiability and Genericity

A signal z is called *identifiable* if it is uniquely determined in \mathbb{K}^n by the measurements b_i up to a global phase factor, which is an ambiguity one cannot avoid. The choice of k generic measurements by means of rank-1 projectors yield identifiability of generic signals if and only if $k \geq n + 1$ in the real and $k \geq 2n$ in the complex case, cf. [4, Theorems 2.9 and 3.4]. Generic rank-1 projectors yield identifiability for all signals if and only if $k \geq 2n - 1$ in the real case. For the complex setting, examples with $k \geq 4n - 4$ that allow reconstruction are known, and this bound is conjectured to be necessary [8].

We will generalize the statements to the scenario of general linear projections. As described earlier, the strategy is to consider first the corresponding algebraized problem over an algebraically closed field, namely \mathbb{C} , instead of \mathbb{R} , and then descend the results back to the real numbers \mathbb{R} . Again, it is important to note that this is subtly different from considering the projection problem over the complex numbers, since instead of complex conjugation, we consider transposition in order to keep the problem algebraic.

A Short Note on Technical Conditions The following exposition will use some technical conditions on varieties and maps, namely them being *irreducible*, and (generically) *unramified*. These are standard notions in algebraic geometry and can be found in most introductory books - we refrain from explaining them here as this is beyond the scope of the paper; the logic in the proofs can be understood without knowing what these mean exactly - a glossary of definitions can be found in Appendix A.1. Intuitively, an algebraic set being irreducible means that there is only one prototypical behaviour for its elements. Unramifiedness is a point-wise algebraic certificate for a mapping staying stable under perturbation in a certain sense. In our case, unramifiedness will certify for identifiability which is stable under perturbation of signals or measurements.

2.2.1. Identifiability of Signals In this paragraph, we translate identifiability of a signal into an algebraic statement. The main concepts will be identifiability, and identifiability which is stable under perturbation, both corresponding to certain algebraic properties of the signal.

Notation 2.8. We fix some notation and technical assumptions that will be valid in the relevant cases of real and complex phase recognition:

- (i) The signals will be modelled by an irreducible variety $\mathcal{S} \subseteq (\mathbb{C}^{n \times n})^\gamma$, with $\gamma = 1$ in the real and $\gamma = 2$ in the complex case. For example, $\mathcal{S} = \mathcal{S}_\rho$ or $\mathcal{S} = \mathcal{S}_{\mathbb{C}}$, as in Section 2.1.

(ii) A measurement scheme will be modelled by the tuple $A = (A_1, \dots, A_k) \in ((\mathbb{C}^{n \times n})^\gamma)^k$ with $k \in \mathbb{N}$ being the number of measurements.

(iii) The measurement process is the formal forward mapping

$$\phi_A : \mathcal{S} \rightarrow \mathbb{C}^k, \quad Z \mapsto (\text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_k)).$$

The condition that \mathcal{S} is irreducible is fulfilled in the cases discussed in the introductory Section 2.1. Namely, both \mathcal{S}_ρ and $\mathcal{S}_\mathbb{C}$ are irreducible varieties, as it is proved in Proposition B.3

We recapitulate a statement from the last section which expresses identifiability in this formal, slightly more technical setting:

Remark 2.9 — By definition, the following are the same:

(i) $Z \in \mathcal{S}$ is identifiable from $\phi_A(Z)$.

(ii) $\#\phi_A^{-1}\phi_A(Z) = 1$.

The following statement is crucial in obtaining our local-to-global principle for identifiability. It characterizes signals which are identifiable and stably so under perturbation just in terms of the signal itself, therefore allowing to remove any reference to open neighbourhoods.

Proposition 2.10. *Assume that ϕ_A is generically unramified. Let $Z \in \mathcal{S}$. Then, the following three statements are equivalent:*

(i) Z is identifiable from $\phi_A(Z)$, and remains identifiable under infinitesimal perturbation. (That is, there is a relatively Borel-open neighborhood $U \subseteq \mathcal{S}$ with $Z \in U$ such that for all $Y \in U$, it holds that $\#\phi_A^{-1}\phi_A(Z) = 1$.)

(ii) Z is identifiable from $\phi_A(Z)$, and ϕ_A is unramified over Z .

(iii) A generic $Y \in \mathcal{S}$ is identifiable from $\phi_A(Z)$. (That is, the set of non-identifiable $Y \in \mathcal{S}$ is a proper Zariski closed subset and therefore Hausdorff measure zero subset of \mathcal{S} .)

In particular, condition (i) is a Zariski open condition on the signal Z ; that is, the set of signals Z with property (i) is a Zariski open subset of \mathcal{S} .

Proof. This is implied by Proposition A.10 in the appendix. □

The condition that ϕ_A is generically unramified is slightly technical and fulfilled in the prototypical cases, see Proposition B.4 in the appendix for a proof. The condition that ϕ_A is *unramified* over Z , on the other hand, is the crucial local property to which we translate perturbation-stability. Intuitively, Proposition 2.10 (iii) means that an identifiable signal which remains so under perturbation certifies for the whole signal space. It is also important to note that condition (ii) in Proposition 2.10 is essentially independent from the choice of \mathcal{S} while (i) and (iii) are a-priori not. We introduce terminology for the condition described in (i):

Definition 2.11. For brevity, we will call a signal $Z \in \mathcal{S}$ that is identifiable from $\phi_A(Z)$, and remains identifiable under infinitesimal perturbation, a *perturbation-stably identifiable* signal (by Proposition 2.10 (ii), this is equivalent to Z being identifiable and ϕ_A being unramified over Z).

We can reformulate Proposition 2.10 as a principle of excluded middle, stating that either almost all signals are perturbation-stably identifiable, or none:

Corollary 2.12. (i) *If there exists a signal $Z \in \mathcal{S}$ which is perturbation-stably identifiable from $\phi_A(Z)$, then a random signal $Y \in \mathcal{S}$ is perturbation-stably identifiable with probability one under any Hausdorff continuous probability density on \mathcal{S} .*

- (ii) It cannot happen that there are sets $\mathcal{A}, \mathcal{B} \subseteq \mathcal{S}$, both with positive Hausdorff measure, such that all signals $Z \in \mathcal{A}$ are perturbation-stably identifiable, and all signals $Z \in \mathcal{B}$ are not perturbation-stably identifiable.

Proof. This is a direct consequence of Proposition 2.10, using that by taking Radon-Nikodym derivatives, \mathcal{S} -Hausdorff zero sets are as well probability measure zero sets for any continuous probability measure. \square

We give an example to illustrate that for a signal, being identifiable is different from being perturbation-stably identifiable:

Example 2.13. Consider the situation where the signals $\mathcal{S} = \{zz^\top : z \in \mathbb{C}^3\}$ are symmetric rank one matrices (i.e., the usual phase recognition setting), and our matrices are chosen as

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

For $\ell = 1, 2, 3$, write $\mathcal{Z}_\ell := \{zz^\top : z \in \mathbb{C}^3, z_i = -z_j, \text{ where } \{1, 2, 3\} = \{\ell, i, j\}\}$ and $\mathcal{C}_\ell := \{zz^\top : z \in \mathbb{C}^3, z_\ell = 0\}$. Write $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \mathcal{Z}_3$ and $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. Then, one can check, by an elementary computation:

- (i) the perturbation-stably identifiable signals are exactly the signals in $\mathbb{C}^{3 \times 3} \setminus \mathcal{Z}$.
- (ii) the signals in $\mathcal{Z} \setminus \mathcal{C}$ are not identifiable.
- (iii) the signals in $\mathcal{Z} \cap \mathcal{C}$ are identifiable, but due to (ii) not perturbation-stably identifiable.

Note that $\mathcal{Z} \cap \mathcal{C}$ is the image of six lines under the map $z \mapsto zz^\top$, three of which are the coordinate axes.

2.2.2. Identifyingness as a Measurement Property In Corollary 2.12, it has been shown that if one signal is perturbation-stably identifiable, then almost all signals are. Therefore the fact whether almost all signals are identifiable can be regarded as a property of the measurement regime. The following theorem makes this statement exact and states that measurement regimes fall into exactly one of three classes:

Theorem 1. For a fixed measurement regime (A_1, \dots, A_k) , consider the three cases

- (a) A generic signal $Z \in \mathcal{S}$ is not identifiable from $\phi_A(Z)$.
- (b) A generic, but not all signals $Z \in \mathcal{S}$, are identifiable from $\phi_A(Z)$.
- (c) All signals $Z \in \mathcal{S}$ are identifiable from $\phi_A(Z)$.

The three cases above are mutually exclusive and exhaustive, and equivalent to

- (a) No signal $Z \in \mathcal{S}$ is perturbation-stably identifiable from $\phi_A(Z)$.
- (b) A generic, but not all signals $Z \in \mathcal{S}$, are perturbation-stably identifiable from $\phi_A(Z)$.
- (c) All signals $Z \in \mathcal{S}$ are perturbation-stably identifiable from $\phi_A(Z)$.

Proof. This is implied by Theorem 12 in the appendix. \square

Recall Example 2.13 which shows that the set of identifiable and perturbation-stably identifiable signals in case (b) of Theorem 1 may differ. The following example shows that the set of identifiable and perturbation-stably identifiable signals may differ in case (a) of Theorem 1 as well.

Example 2.14. Consider the situation where the signals $\mathcal{S} = \{zz^\top : z \in \mathbb{C}^3\}$ are symmetric rank one matrices (i.e., the usual phase recognition setting), and our matrices are chosen as

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

For $\ell = 1, 2, 3$, write $\mathcal{C}_\ell := \{zz^\top : z \in \mathbb{C}^3, z_\ell = 0\}$ and $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. One can check, by an elementary computation:

- (i) No signal is perturbation-stably identifiable.
- (ii) the signals in $\mathbb{C}^{3 \times 3} \setminus \mathcal{C}$ are not identifiable.
- (iii) the signal in \mathcal{C} are identifiable, but not perturbation-stably identifiable.

This is not the simplest example of this kind, since choosing $n = 1$ and one single non-zero (1×1) -matrix exposes the same behavior, with the origin being the simple identifiable point. However, it is informative to compare this example to Example 2.13, in which one more measurement is taken. In this example, the ramification locus (= the set of ramified points) is the union of the coordinate axes \mathcal{C} , a Zariski closed set. There is no non-empty set such that the restriction of ϕ_A to it is unramified or bijective. In particular, while ϕ_A restricted to the origin $(0, 0, 0)$ is bijective as a map, and therefore an isomorphism of sets, it is generically ramified, since the origin is contained in \mathcal{C} .

Moreover, the identifiable signals in Example 2.13 consist exactly of the union of this Zariski closed set, and the Zariski open set of perturbation-stably identifiable signals, explaining why the set of identifiable signals in the other example are neither Zariski closed nor Zariski open.

Theorem 1 allows to regard the different grades of identifiability (a), (b), (c) as properties of the measurement regime. We therefore introduce the following abbreviating notation:

Definition 2.15. We call a measurement tuple $A = (A_1, \dots, A_k)$:

- (a) *non-identifying* for signals in \mathcal{S} , if no signal $Z \in \mathcal{S}$ is perturbation-stably identifiable from $\phi_A(Z)$.
- (b) *generically identifying* for signals in \mathcal{S} , if generic signals $Z \in \mathcal{S}$ are (perturbation-stably) identifiable from $\phi_A(Z)$, and *incompletely identifying*, if generic, but not all signals $Z \in \mathcal{S}$ are (perturbation-stably) identifiable from $\phi_A(Z)$.
- (c) *completely identifying* for signals in \mathcal{S} , if all signals $Z \in \mathcal{S}$ are (perturbation-stably) identifiable from $\phi_A(Z)$.

If \mathcal{S} is obvious from the context, we will omit the qualifier “for signals in \mathcal{S} ”, always keeping in mind that the terminology depends on \mathcal{S} .

Theorem 1 then can be rephrased that a measurement regime A_1, \dots, A_k is either non-identifying, incompletely identifying, or completely identifying - note that due to the theorem, it does not matter whether the “perturbation-stably” in the brackets is there or not. We will now show that being non-identifying, generically and completely identifying are properties of the space of possible measurements, just as identifiability is not only a property of the signal, but of signal space.

Notation 2.16. We introduce some notation modelling the space of measurements:

(iv) The space of measurements of type (A_1, \dots, A_k) will be modelled by irreducible varieties $\mathcal{P}_1, \dots, \mathcal{P}_k \subseteq (\mathbb{C}^{n \times n})^\gamma$, with $\gamma = 1$ in the real and $\gamma = 2$ in the complex case. We will write $\mathcal{P}^{(k)} = \mathcal{P}_1 \times \dots \times \mathcal{P}_k$ for the space of measurement tuples of size k . For example, $\mathcal{P}^{(k)} = \mathcal{P}_{\mathbb{C}}(r)^k$ for complex signals, or $\mathcal{P}^{(k)} = \mathcal{P}_\rho(r)^k$ for real ones.

(v) The extended measurement process will be modelled by the formal forward mapping

$$\begin{aligned} \phi : \mathcal{P}^k \times \mathcal{S} &\rightarrow \mathcal{P}^k \times \mathbb{C}^k \\ (A_1, \dots, A_k, Z) &\mapsto (A_1, \dots, A_k, \text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_n)) \end{aligned}$$

The condition that the \mathcal{P}_i is irreducible is fulfilled in the cases discussed in the introductory Section 2.1: both $\mathcal{P}_\rho(r)$ and $\mathcal{P}_{\mathbb{C}}(r)$ are irreducible varieties, see Proposition B.3. Our main result is an analogue to the characterization in Proposition 2.10, now for the measurement matrices:

Proposition 2.17. *Assume that ϕ is generically unramified. Then, the following three statements are equivalent:*

- (i) $Z \in \mathcal{S}$ is identifiable from $\phi(A, Z)$, and remains identifiable under infinitesimal perturbation of A and Z . (That is, there is a relatively Borel-open neighborhood $U \subseteq \mathcal{P}^k \times \mathcal{S}$ with $(A, Z) \in U$ such that for all $Y \in U$, it holds that $\#\phi^{-1}\phi(Y) = 1$.)
- (ii) (A, Z) is identifiable from $\phi(A, Z)$, and ϕ is unramified over (A, Z) .
- (iii) For generic $B \in \mathcal{P}^k$, a generic $Y \in \mathcal{S}$ is identifiable from $\phi(A, Y)$. (That is, the set of $(B, Y) \in \mathcal{P}^k \times \mathcal{S}$ where $Y \in \mathcal{S}$ is non-identifiable from $\phi(B, Y)$ is a proper Zariski closed subset and therefore Hausdorff measure zero subset of $\mathcal{P}^k \times \mathcal{S}$.)

In particular, condition (i) is a Zariski open property on the measurement-signal-pair (A, Z) ; that is, the set of measurement-signal-pairs (A, Z) with property (i) is a Zariski open subset of $\mathcal{P}^k \times \mathcal{S}$.

Proof. The statement follows from Proposition A.10, applied to the irreducible variety $\mathcal{X} = \mathcal{P}^k \times \mathcal{S}$. □

The main obstacle in generalizing Theorem 1 to an algebraic characterization, or a local-global-property of measurements lies in the fact that the perturbation can occur in both the signal Z and the measurement regime A . We therefore need to provide an intermediate result which removes the dependence on the measurement:

Proposition 2.18. *Assume that ϕ is generically unramified. Then, the following two conditions on measurement regimes $A \in \mathcal{P}^k$ are (Zariski) open conditions:*

- (i) A is generically identifying and remains generically identifying under perturbation. That is, there is a (relatively Borel-) open neighborhood $U \subseteq \mathcal{P}^k$ with $A \in U$ such that all $B \in U$ are generically identifying.
- (ii) A is completely identifying and remains completely identifying under perturbation. That is, there is a (relatively Borel-) open neighborhood $U \subseteq \mathcal{P}^k$ with $A \in U$ such that all $B \in U$ are completely identifying.

Proof. Consider the maps

$$\begin{aligned} \phi : \mathcal{P}^{(k)} \times \mathcal{S} &\rightarrow \mathcal{P}^{(k)} \times \mathbb{C}^k, (A_1, \dots, A_k, Z) \mapsto (A_1, \dots, A_k, \text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_n)), \\ \psi : \mathcal{P}^{(k)} \times \mathcal{S} &\rightarrow \mathcal{P}^{(k)}, (A_1, \dots, A_k, Z) \mapsto (A_1, \dots, A_k), \\ \pi : \mathcal{P}^{(k)} \times \mathcal{S} &\rightarrow \mathcal{S}, (A_1, \dots, A_k, Z) \mapsto Z. \end{aligned}$$

(i) Consider the set $\mathcal{Y} = \{x \in \mathcal{P}^{(k)} \times \mathcal{S} : \phi(x) \text{ is identifiable and unramified}\}$. By Proposition 2.17 \mathcal{Z} is a Zariski open set (and possibly empty). Since ψ is surjective, the set $\psi(\mathcal{Y})$ is therefore an open subset of $\mathcal{P}^{(k)}$, and by construction, describes the condition (i), therefore proving its openness.

(ii) Keep the notations above, and consider the set-complement \mathcal{Y}^C of \mathcal{Y} in $\mathcal{P}^{(k)} \times \mathcal{S}$. Since \mathcal{Y} is open, \mathcal{Y}^C is closed, and $\mathcal{V} := \psi(\mathcal{Y}^C)$ is closed as well. Therefore, the set-complement \mathcal{V}^C in $\mathcal{P}^{(k)}$ is open. By construction, \mathcal{V}^C describes condition (ii), therefore openness of condition (ii) follows. \square

Definition 2.19. We call a measurement regime $A \in \mathcal{P}^{(k)}$:

- (a) *stably non-identifying* in $\mathcal{P}^{(k)}$, if A is non-identifying and remains non-identifying under perturbation, as in Proposition 2.18 (i).
- (b) *stably generically identifying* in $\mathcal{P}^{(k)}$, if A is generically identifying and remains generically identifying under perturbation, as in condition (i). *stably incompletely identifying* in $\mathcal{P}^{(k)}$, if A is incompletely identifying and remains incompletely identifying under perturbation, as in Proposition 2.18 (i).
- (c) *stably completely identifying* in $\mathcal{P}^{(k)}$, if A is completely identifying and remains completely identifying under perturbation, as in Proposition 2.18 (ii).

If $\mathcal{P}^{(k)}$ is obvious from the context, we will omit the qualifier “in $\mathcal{P}^{(k)}$ ”, always keeping in mind that the terminology depends on $\mathcal{P}^{(k)}$.

Note that a measurement regime can be, at the same time, neither stably non-identifying, stably generically identifying, nor stably completely identifying. However, by definition, stably non-identifying is mutually exclusive to stably generically identifying, and stably incompletely identifying is mutually exclusive to stably completely identifying.

Proposition 2.18 can be reformulated as a local-to-global-principle:

Corollary 2.20. *Keep the notations of Proposition 2.18. Then:*

- (ia) *If there exists a stably generically identifying measurement regime $A \in \mathcal{P}^{(k)}$, a generic measurement $B \in \mathcal{P}^{(k)}$ is stably generically identifying.*
- (ib) *If there exists a stably completely identifying measurement regime $A \in \mathcal{P}^{(k)}$, a generic measurement $B \in \mathcal{P}^{(k)}$ is stably completely identifying.*
- (iia) *If there exists a stably non-identifying measurement regime $A \in \mathcal{P}^{(k)}$, a generic measurement $B \in \mathcal{P}^{(k)}$ is stably non-identifying, and no measurement is stably incompletely identifying or stably completely identifying.*
- (iib) *If there exists a stably incompletely identifying measurement regime $A \in \mathcal{P}^{(k)}$, a generic measurement $B \in \mathcal{P}^{(k)}$ is stably incompletely identifying, and no measurement is stably completely identifying.*

Proof. (ia) and (ib) follow from Zariski-openness of the conditions asserted in Proposition 2.18. (iia) and (iib) can be derived as negations. \square

Proposition 2.18 also allows to prove an analogue of Theorem 1, now for classes of measurements instead of a single measurement regime:

Theorem 2. *Assume that ϕ is generically unramified. Consider the three cases*

- (a) *A generic measurement regime $A \in \mathcal{P}^k$ is non-identifying.*

(b) A generic measurement regime $A \in \mathcal{P}^k$ is incompletely identifying.

(c) A generic measurement regime $A \in \mathcal{P}^k$ is completely identifying.

The three cases above are mutually exclusive and exhaustive, and equivalent to

(a) A generic measurement regime $A \in \mathcal{P}^k$ is stably non-identifying. No measurement regime $A \in \mathcal{P}^k$ is stably generically identifying.

(b) A generic measurement regime $A \in \mathcal{P}^k$ is stably incompletely identifying.

(c) A generic measurement regime $A \in \mathcal{P}^k$ is stably completely identifying.

Proof. A proof by analogy is described in the appendix, as Theorem 13 □

We can therefore define terminology that describe cases (a) to (c) shortly:

Definition 2.21. Keep the notations of Theorem 2. We will call a the set of measurements \mathcal{P}^k *generically unramified* if ϕ is generically unramified. We will call a generically unramified \mathcal{P}^k :

(a) *non-identifying* if a generic measurement $A \in \mathcal{P}^k$ is non-identifying.

(b) *generically identifying* if a generic measurement $A \in \mathcal{P}^k$ is generically identifying. *incompletely identifying* if a generic measurement $A \in \mathcal{P}^k$ is incompletely identifying.

(c) *completely identifying* if a generic measurement $A \in \mathcal{P}^k$ is completely identifying.

Note that, somewhat differently as it happens in Theorem 1 for signals, generically identifying measurements can exist in generically non-identifying measurement regimes - with other words, there can be a measurement in \mathcal{P}^k which identifies a generic signal, while a generic measurement in \mathcal{P}^k does not identify a generic signal. This does not contradict the above discussion since a generically non-identifying measurement regime does include perturbation-stability with respect to the measurements, while a generically identifying measurement does not. Algebraically spoken, ϕ_A does not ramify for generic signals Z , while ϕ is ramified at (A, Z) for all Z . An explicit example for this behaviour is given in section 2.7.

2.3. Transfer Results for Identifyingness

In this section we will collect different results that allow to transfer identifyingness properties from one set of potential measurements to another:

Notation 2.22. We will consider irreducible varieties $\mathcal{P}^{(k)} = \mathcal{P}_1 \times \dots \times \mathcal{P}_k$ and $\mathcal{Q}^{(k)} = \mathcal{Q}_1 \times \dots \times \mathcal{Q}_k$, with corresponding forward maps ϕ, φ .

The first lemma allows to obtain identifiability for a broader measurement space, if it is already established for a smaller:

Lemma 2.23. Assume $\mathcal{P}_i \subseteq \mathcal{Q}_i$ for all i , that is, $\mathcal{P}^{(k)} \subseteq \mathcal{Q}^{(k)}$. Then:

(i) If $\mathcal{P}^{(k)}$ is generically unramified, then so is $\mathcal{Q}^{(k)}$.

(ii) If $\mathcal{P}^{(k)}$ is generically identifying, then so is $\mathcal{Q}^{(k)}$.

(iii) If $\mathcal{P}^{(k)}$ is completely identifying, then so is $\mathcal{Q}^{(k)}$.

Proof. (i) follows from Theorem 10 (ii) in the appendix. For (ii), the characterization in Theorem 13 yields that is birational. Therefore, there is $(A, Z) \in \mathcal{P}^{(k)} \times \mathcal{S}$ above which ϕ is unramified and for which $\#\phi^{-1}\phi(A, Z) = 1$. Since ϕ remembers A exactly, this is equivalent to $\#\varphi^{-1}\varphi(A, Z) = 1$; also φ is unramified above (A, Z) . We can therefore apply Proposition A.10 to infer that φ is birational, which implies the statement by Theorem 13. (iii) follows in analogy, repeating the argument for all $Z \in \mathcal{S}$. \square

As Example 2.14 shows, the reverse implications do not hold in general.

We prove another lemma, which is specific to the case of matrices stratified by rank, and which will allow to restrict to orthogonal or unitary matrices, once properties of all matrices of fixed rank are established:

Lemma 2.24. *Assume the $\mathcal{P}_i \subseteq (\mathbb{C}^{n \times n})^r$ are all spaces of rank at most r_i matrices, that is, of the form $\mathcal{P}_\rho(r_i)$ or $\mathcal{P}_\mathbb{C}(r_i)$. Assume that the \mathcal{Q}_i are the corresponding variety of orthogonal/unitary projection matrices of rank exactly r_i . Then:*

- (i) $\mathcal{P}^{(k)}$ is generically identifying if and only if $\mathcal{Q}^{(k)}$ is.
- (ii) $\mathcal{P}^{(k)}$ is completely identifying if and only if $\mathcal{Q}^{(k)}$ is.

Proof. Let A_1, \dots, A_k be generic in $\mathcal{P}_1, \dots, \mathcal{P}_k$; we will treat the A_i as single matrices. Since $z^*Az = \frac{1}{2}z^*(A^* + A)z$, we can assume that the A_i are symmetric/Hermitian and generic. (i) (A_1, \dots, A_k) are generically identifying if for generic z , one can reconstruct z up to phase/sign from the $z^*A_i z$. By definition, there is an invertible matrix S_1 such that $U_1 = S_1^*A_1S_1$ is an orthogonal/unitary projector of rank a_i . Since S_1 is invertible, a vector z is generic if and only if the vector $S_1 \cdot z$ is generic, therefore (A_1, \dots, A_k) is generically identifying if and only if $(U_1, S_1^*A_2S_1, \dots, S_1^*A_kS_1)$ is generically identifying. Since $A_j, j \geq 2$ was generic, the matrices $S_1^*A_2S_1, \dots, S_1^*A_kS_1$ are also generic, and independent of U_1 therefore they can be replaced anew by generic A_2, \dots, A_k . Repeating the argument k times yields the claim. The proof for (ii) is analogous, noting that identifiability holds for generic (A_1, \dots, A_k) , but all z . \square

In our terminology, Proposition 2.18 also implies that the behavior of random projectors is completely determined by their number, and no other properties. This motivates the following:

Definition 2.25. Consider an arbitrary family of irreducible varieties $\mathcal{P}_i, i \in \mathbb{N}$. We will denote

- (i) in case of existence, the smallest number k such that $(\mathcal{P}_1, \dots, \mathcal{P}_k)$ is generically identifying by $\lambda(\mathcal{P}_1, \mathcal{P}_2, \dots)$. We will denote the number, if clear from the context, by $\lambda(\mathcal{P})$, and call it the *generic identifiability threshold*.
- (ii) in case of existence, the smallest number k such that $(\mathcal{P}_1, \dots, \mathcal{P}_k)$ is completely identifying by $\kappa(\mathcal{P}_1, \mathcal{P}_2, \dots)$. We will denote the number, if clear from the context, by $\kappa(\mathcal{P})$, and call it the *complete identifiability threshold*.

If $\mathcal{P}_i = \mathcal{X}$ for all i , for some variety \mathcal{X} , we also write $\lambda(\mathcal{X})$ and $\kappa(\mathcal{X})$ instead of $\lambda(\mathcal{P}_1, \mathcal{P}_2, \dots)$ and $\kappa(\mathcal{P}_1, \mathcal{P}_2, \dots)$.

2.4. From Complex to Real Identifiability

Before deriving identifiability statements in the given terminology, we briefly derive results which allow to return to the original phase retrieval problem 2.1; that is, we state the principle of excluded middle for real measurements and signals. It implies that the conclusions of our main theorems 1 and 2 hold for the non-algebraized, real formulation as well:

Proposition 2.26. Write $\mathcal{S}_{\mathbb{R}} := \mathcal{S} \cap (\mathbb{R}^{n \times n})^{\gamma}$ and $\mathcal{P}_{\mathbb{R}} := (\mathcal{P}_1 \cap (\mathbb{R}^{n \times n})^{\gamma}) \times \cdots \times (\mathcal{P}_k \cap (\mathbb{R}^{n \times n})^{\gamma})$ for their real parts. Assume that \mathcal{S} and \mathcal{P} are observable over the reals (as defined in appendix A.3). Then, the following statements, about identifying signals $Z \in \mathcal{S}$ from $\text{Tr}(Z \cdot A_1), \dots, \text{Tr}(Z \cdot A_k)$ hold:

- (i) If $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$ is not generically identifying (viewed as an element of \mathcal{P}), then no signal $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified.
- (ii) If $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$ is generically identifying (viewed as an element of \mathcal{P}), then a generic signal $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified.
- (iii) If $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$ is completely identifying (viewed as an element of \mathcal{P}), then all signals $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified.
- (iv) If \mathcal{P} is not generically identifying, then no signal $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified by a generic $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$.
- (v) If \mathcal{P} is generically identifying, then a generic signal $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified by a generic $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$.
- (vi) If \mathcal{P} is completely identifying, then all signals $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified by a generic $(A_1, \dots, A_k) \in \mathcal{P}_{\mathbb{R}}$.

Here, in the statements above, generic means that all objects fulfill the statement, except possibly a Hausdorff measure zero set, where the Hausdorff measure is taken to be positive only on the highest dimensional components.

Furthermore, all statements hold when replacing $\mathcal{S}_{\mathbb{R}}$ by any positive measure subset $\mathcal{S}'_{\mathbb{R}}$ such that the Zariski closure of $\mathcal{S}'_{\mathbb{R}}$ is $\mathcal{S}_{\mathbb{R}}$, or replacing $\mathcal{P}_{\mathbb{R}}$ by any positive measure subset $\mathcal{P}'_{\mathbb{R}}$ such that the Zariski closure of $\mathcal{P}'_{\mathbb{R}}$ is $\mathcal{P}_{\mathbb{R}}$.

Proof. Statements (i) and (iv) follow already from the definitions, and Proposition 2.18. The other numbered statements are implied by Theorem 11 in the appendix, noting that all properties above (or their negations) are algebraic. The last statement follows from the fact that if a set $V \subseteq \mathcal{S}_{\mathbb{R}}$ containing no, generic, or all elements of $\mathcal{S}_{\mathbb{R}}$, the set $V \cap \mathcal{S}'_{\mathbb{R}}$ contains no, generic, or all elements of $\mathcal{S}'_{\mathbb{R}}$, and the analogue for $\mathcal{P}_{\mathbb{R}}$ and $\mathcal{P}'_{\mathbb{R}}$. \square

Remark 2.27 — There are several remarks to make:

- (i) The assumption that \mathcal{P} and \mathcal{S} are observable over the reals are valid for our prototypical cases, see Proposition B.3.
- (ii) An analogue of Proposition 2.26 could be derived for the projections A_i allowed to be complex and z restricted to real signals or vice versa.

2.5. Identifiability of Real Signals

For the reals, there are natural lower bounds on the identifiability thresholds:

Proposition 2.28. Consider identifiability from real signals $\mathcal{S} = \{zz^{\top}, z \in \mathbb{C}^n\}$. For any family of irreducible varieties $\mathcal{P}_i \subseteq \mathbb{C}^{n \times n}, i \in \mathbb{N}$, with $n \geq 2$, it holds that $\kappa(\mathcal{P}) \geq \lambda(\mathcal{P})$, and $\lambda(\mathcal{P}) \geq n + 1$.

Proof. It suffices to show that no $(A_1, \dots, A_n) \in (\mathbb{C}^{n \times n})^n$ can be stably generically identifying. We proceed by contradiction and assume the contrary. Proposition 2.17 then implies that $(\mathbb{C}^{n \times n})^n$ is generically identifying, so we may replace A_1, \dots, A_n by a generic choice in $(\mathbb{C}^{n \times n})^n$. Fixing

$z^\top A_1 z, \dots, z^\top A_n z$ yields n equations on z , of degree 2. By Bezout's theorem, and using that the A_i are generic, those equations have 2^n solutions. Sign ambiguity leaves $2^{n-1} \gtrsim 1$ solutions, yielding a contradiction. \square

Note that there are (A_1, \dots, A_n) which are generically identifying but not stably so.

We now summarize some results which can be readily inferred from literature for real signals:

Theorem 3. *Consider identifiability from real signals, corresponding to the complex signal variety $\mathcal{S}_\rho = \{zz^\top, z \in \mathbb{C}^n\}$, and projectors $\mathcal{P} = \mathcal{S}$. Then:*

$$\lambda(\mathcal{P}) = n + 1, \quad \text{and} \quad \kappa(\mathcal{P}) = 2n - 1.$$

Proof. Note that once we have identifiability for signals $\mathcal{S}' = \{zz^\top, z \in \mathbb{R}^n\}$ and projectors $\mathcal{P}' = \mathcal{S}'$, we can use Proposition 2.18 to obtain the statement for the Zariski closure \mathcal{S} of \mathcal{S}' and \mathcal{P} of \mathcal{P}' . So $\lambda(\mathcal{P}) \leq n + 1$ can be inferred from [4, Theorems 2.9], and $\kappa(\mathcal{P}) = 2n - 1$ from [4, Theorem 2.2 and Corollary 2.7]. Combined with Proposition 2.28, we obtain the statement. \square

By virtue of Lemma 2.23, these results can immediately be broadened to include general linear projections, while Lemma 2.24 yields the case of orthogonal measurements:

Theorem 4. *Consider identifiability from real signals, corresponding to the complex signal variety $\mathcal{S} = \{zz^\top, z \in \mathbb{C}^n\}$, and the family $\mathcal{P}_i = \{P^\top \cdot P : P \in \mathbb{C}^{r_i \times n}\}, i \in \mathbb{N}$ of projectors of potentially different ranks $r_i \geq 1$. Then:*

$$\lambda(\mathcal{P}) = n + 1, \quad \text{and} \quad \kappa(\mathcal{P}) = 2n - 1.$$

The result remains unaltered if the projectors \mathcal{P} are restricted to be orthogonal.

Proof. $\lambda(\mathcal{P}) \geq n + 1$ is implied by Proposition 2.28. $\kappa(\mathcal{P}) \geq 2n - 1$ is implied by Theorem 3 and the definition of κ . Lower bounds $\lambda(\mathcal{P}) \leq n + 1$ and $\kappa(\mathcal{P}) \leq 2n - 1$ are implied by combining Theorem 3 and Lemma 2.23. The statement for orthogonal projectors follows from Lemma 2.24. \square

Using the tools introduced in Section 2.4, we obtain from this statement about the complexified problem one about the original phase retrieval problem for the reals:

Theorem 5. *Let $P_i \in \mathbb{R}^{r_i \times n}, 1 \leq i \leq k$ be generic. Then, a generic signal $z \in \mathbb{R}^n$ is identifiable from $b_i = \|P_i z\|^2, 1 \leq i \leq k$ up to sign if and only if $k \geq n + 1$. All signals $z \in \mathbb{R}^n$ are identifiable from $b_i = \|P_i z\|^2, 1 \leq i \leq k$ up to sign if and only if $k \geq 2n - 1$. The result remains unaltered if the projectors P_i are restricted to be orthogonal.*

Proof. Taking generic P_i is equivalent to having generic symmetric measurements of rank r_i , by Proposition B.2. By the same argument as in the beginning of Lemma 2.24, we can thus assume that we have generic A_i of rank r_i . The statement is then implied by Theorem 4 (i) and Proposition 2.26, noting that identifiability of $Z = zz^\top \in \mathbb{R}^{n \times n}$ is equivalent to identifiability of z up to sign. \square

This solves the open problems (1-6).

2.6. Identifiability of Complex Signals

The case of complex phase recognition is somewhat analogous to the real one, while more technical due to the special structure of the matrices involved.

Proposition 2.29. *Consider identifiability from complex signals, corresponding to the complex signal variety $\mathcal{S}_i = \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{C}^n\}$. For any family of irreducible varieties $\mathcal{P}_i \subseteq \mathbb{C}^{n \times n} \times \mathbb{C}^{n \times n}, i \in \mathbb{N}$, with $n \geq 2$, it holds that $\kappa(\mathcal{P}) \geq \lambda(\mathcal{P})$, and $\lambda(\mathcal{P}) \geq 2n$.*

Proof. Let ϕ be the forward map in Problem 2.5. It holds that $\dim \mathcal{S}_i = 2n - 1$, therefore the fiber $\phi^{-1}(\phi(A_1, \dots, A_k, Z))$ can be finite only if $k \geq 2n - 1$. Since \mathcal{S}_i is non-linear, it has degree strictly bigger than one, implying by Bezout's theorem that $\phi^{-1}(\phi(A_1, \dots, A_k, Z))$ is not finite for $k = 2n - 1$. Therefore, $\lambda(\mathcal{P}) \geq 2n$. \square

We now summarize some results which can be readily inferred from literature:

Theorem 6. *Consider identifiability from complex signals $\mathcal{S} = \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{C}^n\}$, and the family $\mathcal{P} = \mathcal{S}$. Then:*

$$\lambda(\mathcal{P}) = 2n, \quad \text{and} \quad \kappa(\mathcal{P}) \leq 4n - 4.$$

Proof. Note that once identifiability for signals $\mathcal{S}' = \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{R}^n\}$, and projectors $\mathcal{P}' = \mathcal{S}'$ is established, we can use Proposition 2.18 to obtain the statement for the Zariski closure \mathcal{S} of \mathcal{S}' and \mathcal{P} of \mathcal{P}' . Thus, $\lambda(\mathcal{P}) \leq 2n$ can be inferred from [4, Theorems 3.4]; the inequality $\kappa(\mathcal{P}) \leq 4n - 4$ can be obtained from [3, section 4]. Combined with Proposition 2.29, this yields the statement. \square

Again, Lemmata 2.23 and 2.24 yield a statement for general projectors:

Theorem 7. *Consider identifiability from complex signals $\mathcal{S} = \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{C}^n\}$, and the family $\mathcal{P}_i := \{(Q^\top Q + S^\top S, Q^\top S - S^\top Q) : S, Q \in \mathbb{C}^{r_i \times n}\}$. Then:*

$$\lambda(\mathcal{P}) = 2n, \quad \text{and} \quad \kappa(\mathcal{P}) \leq 4n - 4.$$

The result remains unaltered if the projectors \mathcal{P} are restricted to be unitary.

Proof. $\lambda(\mathcal{P}) \geq 2n$ is implied by Proposition 2.29. Lower bounds $\lambda(\mathcal{P}) \leq 2n$ and $\kappa(\mathcal{P}) \leq 4n - 4$ are implied by combining Theorem 6 and Lemma 2.23. The statement for unitary projectors follows from Lemma 2.24. \square

Now we can combine the algebraic results over the complex numbers in Theorem 7, with the connection to the reals given in Proposition 2.26 to deduce the identifiability theorems for the original (non-algebraized) complex phase retrieval problem:

Theorem 8. *Let $P_i \in \mathbb{C}^{r_i \times n}$, $1 \leq i \leq k$ be generic. Then, a generic signal $z \in \mathbb{C}^n$ is identifiable from $b_i = \|P_i z\|^2$, $1 \leq i \leq k$ up to phase if and only if $k \geq 2n$. All signals $z \in \mathbb{C}^n$ are identifiable from $b_i = \|P_i z\|^2$, $1 \leq i \leq k$ up to phase if $k \geq 4n - 4$. The result remains unaltered if the projectors P_i are restricted to be unitary.*

Proof. Taking generic P_i is equivalent to having generic symmetric measurements of rank r_i , by Proposition B.2. By the same argument as in the beginning of Lemma 2.24, we can thus assume that we have generic A_i of rank r_i . The statement is then implied by Theorem 7 (i) and Proposition 2.26, noting that identifiability of (X, Y) is equivalent to identifiability of $X + \iota Y = zz^* \in \mathbb{C}^{n \times n}$, up to phase. \square

This solves problem (7), and problems (1-6) for unitary projection matrices.

We would like to remark that Theorems 4 and 7, together with Proposition 2.26, not only yield the statements for general linear projections, but in fact state that any bound which can be proved for the rank one projectors directly extends to any (irreducible) set of linear projectors containing those. In particular, if one succeeds in proving a lower bound for complete identifiability for complex phase retrieval, the same bound automatically holds for linear projectors of arbitrary rank.

2.7. Generic Measurements are Crucial for the Identifiability Thresholds

The identifiability thresholds are defined by means of generic measurements. This section is dedicated to verify there are specific measurements such that signal recovery is possible below the identifiability threshold. In fact, we shall provide an example of n measurements in the real and $2n - 1$ measurements in the complex case, so that generic signals are uniquely determined up to their sign and phase, respectively.

Example 2.30. Consider the standard orthonormal basis vectors $\{e_i\}_{i=1}^n$ of \mathbb{R}^n , and define $A_j := e_1 e_1^\top + e_j e_j^\top + e_1 e_j^\top$, $j = 1, \dots, n$. We observe that, for all $Z = z z^\top$, $z \in \mathbb{R}^n$,

$$b_1 = |z_1|^2, \quad \text{and} \quad b_j = \text{Tr}(Z \cdot A_j) = |z_1|^2 + 2z_1 z_j, \quad j = 2, \dots, n.$$

For a generic signal z , we can always assume $z_1 \neq 0$. Since we must recover z only up to its sign, we may as well assume that the measurement b_1 determines z_1 and aim to reconstruct z_2, \dots, z_n exactly. A mere reformulation of the above equation then yields $z_j = \frac{b_j - z_1^2}{2z_1}$, for $j = 2, \dots, n$. Thus, the n measurements $\{A_j\}_{j=1}^n$ uniquely determine all signals $z \in \mathbb{R}^n$ with $z_1 \neq 0$ up to a global sign, hence generic signals.

A similar example can be derived for complex signals and $2n - 1$ measurements:

Example 2.31. We choose measurement matrices $A_1 := e_1 e_1^\top$ and $A_j := e_1 e_1^\top + e_j e_j^\top + e_1 e_j^\top$ as well as $\tilde{A}_j := e_1 e_1^\top + \iota e_j e_1^\top - \iota e_1 e_j^\top$, $j = 2, \dots, n$. This choice yields the measurements

$$b_1 = |z_1|^2, \quad \text{and} \quad b_j = |z_1|^2 + 2\Re(\bar{z}_1 z_j), \quad c_j = |z_1|^2 + 2\Im(\bar{z}_1 z_j), \quad j = 2, \dots, n.$$

Without loss of generality, we can choose z_1 real-valued and genericity allows to assume $z_1 \neq 0$, so that we obtain

$$\Re(z_j) = \frac{b_j - z_1^2}{2z_1}, \quad \Im(z_j) = \frac{c_j - z_1^2}{2z_1}, \quad j = 2, \dots, n.$$

Thus, the $2n - 1$ measurements determine a generic z up to a global phase factor.

The matrices A_2, \dots, A_n in Example 2.30 are all rank two, only A_1 is of rank one, similarly in Example 2.31; we would like to note that such an example does not exist for pure rank one measurements, that is, $A_i \in \mathcal{P}_\rho(1)$ or $A_i \in \mathcal{P}_\mathbb{C}(1)$. Namely, in the case of real signals, a rank one measurement regime of size n has either linearly dependent row-spans; otherwise, it is equivalent, by applying a linear transformation to z , to the measurements $A_j = e_j e_j^\top$, which generically has 2^n distinct solutions. Thus, it is generically non-identifying in both cases. The argument for complex signals is similar. Therefore, it is highly crucial for the perturbation results in [3] that the measurement scheme is rank one.

3. A Deterministic Inversion Formula

3.1. Phase Retrieval as Ideal Regression

In this section, we will show that the phase retrieval problem is a special case of an algebraic estimation problem, called ideal regression. This means that not only is the solvability and identifiability of the problem determined by algebraic invariants, such as n, k , or the kind of projectors, but that it is - in principle - also accessible to algorithmical estimation tools from approximate algebra, such as those presented in [17], yielding explicit and deterministic inversion formulae not only for $k = \Omega(n^2)$, but directly at the identifiability threshold $k \geq n + 1$.

The reformulation of the phase retrieval as an algebraic estimation problem bears similarities to the algebraization in Section 2.1. The major idea consist of converting the observation into polynomials, which are then manipulated to obtain the solution.

Assume we are in the case of the real phase recognition problem, wanting to identify a signal $z \in \mathbb{R}^n$. Then, let $X = (X_1, \dots, X_n)$ be a vector of formal variables. The k projection matrices P_i give rise to k polynomials

$$p_i(X_1, \dots, X_n) = X^\top A_i X - b_i$$

in the variables X_j , with $A_i = P_i^\top P_i$, such that, after substitution, we have $p_i(z) = 0$. By definition the polynomials p_i are contained in the ideal $\mathcal{J} := \mathcal{I}(z) \subseteq \mathbb{C}[X_1, \dots, X_n]$. Thus, the estimation problem becomes, for the real phase recognition problem:

Problem 3.1. Let $z \in \mathbb{R}^n$ be unknown, let $\mathfrak{s} = \langle X_1 - z_1, \dots, X_n - z_n \rangle \in \mathbb{C}[X_1, \dots, X_n]$. Let $p_1, \dots, p_k \in \mathcal{J}$ be known polynomials, of the form $p_i(X_1, \dots, X_n) = X^\top A_i X - b_i$, where $b_i = z^\top A_i z - b_i$. Then, reconstruct \mathfrak{s} , or equivalently, z , from the polynomials $p_1, \dots, p_k, 1 \leq i \leq k$.

What at first seems like a mere reformulation, contains the gist of the algebraic ideal regression method: instead of fitting a loss function or performing optimization on z , or taking the b_i, P_i as an input, we try to obtain the solution from manipulating the polynomials p_i as symbolic objects in their own right. Again, we note that we are working over the complex numbers in the polynomial ring $\mathbb{C}[X_1, \dots, X_n]$, similarly to the algebraization; we will again show that this is no major problem, from an algorithmic aspect.

The complex case is slightly different but can be treated similarly. Here, let $X = (X_1, \dots, X_n)$ and $Y = (Y_1, \dots, Y_n)$ be vectors of formal variables, and let $P_i = Q_i + \iota \cdot S_i$ with $Q_i, S_i \in \mathbb{R}^{m \times n}$. The projections give rise to k polynomials

$$p_i = (X, Y)^\top \begin{pmatrix} Q_i^\top Q_i + S_i^\top S_i & S_i^\top Q_i - Q_i^\top S_i \\ Q_i^\top S_i - S_i^\top Q_i & Q_i^\top Q_i + S_i^\top S_i \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

and those are, similar to the real case, contained in the ideal

$\mathcal{J} := \mathfrak{s}((X, Y) - \tilde{z}) \subseteq \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_n]$, where $\tilde{z} = (\Re z, \Im z) \in \mathbb{R}^{2n}$. So the estimation problem is, in the complex case:

Problem 3.2. Let $\tilde{z} \in \mathbb{R}^{2n}$ be an unknown point, let

$$\mathfrak{s} = \langle X_1 - \Re z_1, Y_1 - \Im z_1, \dots, X_n - \Re z_n, Y_n - \Im z_n \rangle \subseteq \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_n].$$

Let $p_1, \dots, p_k \in \mathfrak{s}$ be known polynomials, of the form as above. Reconstruct \mathfrak{s} , or equivalently \tilde{z} , from the $p_1, \dots, p_k, 1 \leq i \leq k$.

Note that the ideal regression formulation of phase retrieval Problem 3.2 differs fundamentally from the algebraized inverse problem version given in Problem 2.5, since in ideal regression, we split real and complex parts of the formal variables, whereas in the algebraization, we split real and complex parts of the matrices involved. Still, both problems are intrinsically related, and can be considered, in a certain sense, as each other's duals.

3.2. An Inversion Formula with Ideal Regression

We describe how the ideal regression formulation of the phase retrieval problem 3.1 can be solved by an approximate algebraic algorithm; we focus on the real case. If $k \geq \binom{n+1}{2}$, there exist explicit inversion formulae in which one computes an approximation for $\text{Tr}(A_i z z^\top) = b_i$, which is now considered as a linear system of k equations in the $\binom{n+1}{2}$ unknowns $z z^\top$; this can be written as

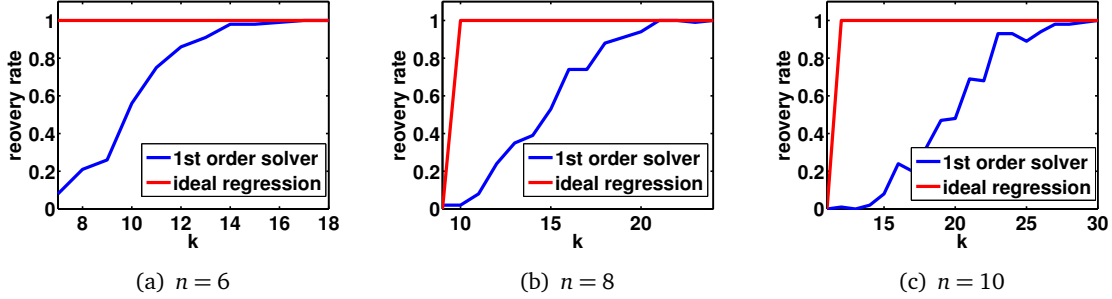


Figure 1: Recovery rates averaged over 100 repeats without any noise for ideal regression and for a first order solver in PhaseLift.

pseudo-inverting a matrix which has one row per A_i , and noise stability can be achieved by regularization, or by performing a singular value decomposition. On the other hand if $k \lesssim \binom{n+1}{2}$, such a direct approach will not work.

However, it is nevertheless possible to construct an explicit deterministic inversion formula, readily providing answers at the identifiability threshold $k \geq n + 1$, and which is numerically stable. The main idea is to use an ideal regression algorithm, namely Algorithms 1 and 2 in [17]; the ideal \mathfrak{s} we wish to estimate in our case is linear, namely $\mathfrak{s} = \langle X_1 - z_1, \dots, X_n - z_n \rangle$, and the input polynomials are of degree two, contained in \mathfrak{s} . Since \mathfrak{s} is inhomogenous, Algorithm 1 in [17] will output the homogenous part of \mathfrak{s} , namely $\mathfrak{s}_h = \mathfrak{s} \cap \langle X_1, \dots, X_n \rangle$ which is also linear, and can be used to estimate z .

Instantiating Algorithm 1 in [17] with $D = n, d = 1$, and polynomials $f_i := p_i/b_i - \bar{p}, 1 \leq i \leq k - 1$, where $\bar{p} = \sum_{i=1}^k p_i/b_i$, yields an estimate for generators ℓ_1, ℓ_{n-1} of \mathfrak{s}_h . The signal z fulfills $\ell_i(z) = 0$, therefore z is orthogonal to the coefficient vectors of the ℓ_i and can be determined up to a scalar multiple $z' = \alpha z$ from the ℓ_i . Thus, z can be determined by setting $z := z'/\alpha$ where α can be estimated as $\alpha := \exp\left(\sum_{i=1}^k \log\left((z')^\top A_i z\right) - \log b_i\right)$. We will refer to this strategy as the “explicit inversion” in the experiments section.

We refrain from actually explaining in detail how Algorithm 1 in [17] works, or from stating the algorithm itself, due to the amount of notational overhead which would be needed, and refer the reader to the original paper instead. We want to stress that Algorithm 1 is deterministic and numerically stable, therefore it yields a potentially explicit and regularizable inversion formula for the phase recognition problem.

4. Experiments

In this section we provide few numerical experiments illustrating that generic real signals can be identified from few generic magnitude measurements by using the inversion formula obtained from ideal regression as outlined in section 3.2. We also include a few comparisons to an alternative method. Classical phase retrieval algorithms such as Gerchberg/Saxton [14] and Fienup’s alternatives [13] are customized to Fourier measurements, hence are also limited to this setting. An approach that can deal with generic measurements is PhaseLift [10], which is based on finding the feasible point of a semidefinite program and is proposed to be solved using first order methods. The theoretical results in [10] are asymptotic in the ambient dimension n and no success guarantees are derived for fixed n . Nonetheless, PhaseLift is known to be quite successful and very robust against noise in practise. The complexity of ideal regression causes limits in the number of measurements that can be dealt with in practise, while it yields an explicit reconstruction formula. We shall study

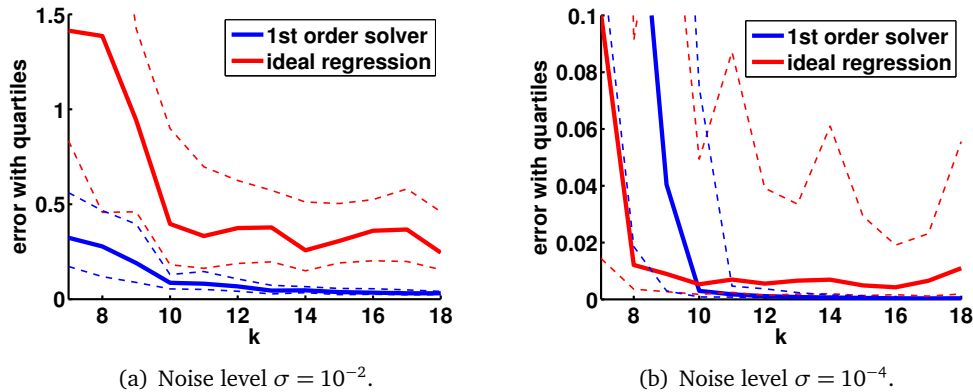


Figure 2: Mean squared error for $n = 6$ and quartiles for 100 repeats.

the performance of ideal regression and PhaseLift for few measurements.

In the numerical experiments, we choose the signal x uniformly distributed on the sphere. Measurements are performed by orthogonal rank-1 projectors, also uniformly distributed (according to the standard Haar measure on this set), and we deal with corrupted measurements $\tilde{b} = b + \eta$, where η is Gaussian white noise of variance σ . The outcome of performance comparisons between ideal regression and PhaseLift very much depend on the noise level. If measurements are exact, then ideal regression yields signal recovery for generic $n + 1 \leq k \leq 3n$ measurements, a range, in which PhaseLift performs rather poorly, see Fig. 1 for $n = 6, 8, 10$. For inexact yet still very accurate measurements, in other words very low noise levels ($\sigma \approx 10^{-4}$), ideal regression still outperforms PhaseLift when the number of measurements is close to the threshold $n + 1$, see Fig. 2(b), with a comparable accuracy for higher noise levels ($\sigma \approx 10^{-2}$), cf. Fig. 2(a). Nonetheless, it must be mentioned that with slightly larger and hence more common noise levels, especially when the number of measurements increases, then PhaseLift is eventually to be favored since error rates are then significantly smaller than within ideal regression. It is interesting to note that ideal regression performs well close to the identifiability threshold $k = n + 1$, whereas PhaseLift yields more accurate estimates as the number of samples increases.

Acknowledgements

ME is funded by the Vienna Science and Technology Fund (WWTF) through project VRG12-009. FK is supported by Mathematisches Forschungsinstitut Oberwolfach (MFO).

References

- [1] Christine Bachoc and Martin Ehler. Signal reconstruction from the magnitude of subspace components. *arXiv e-prints*, September 2012. arXiv:1209.5986.
- [2] R. Balan, P. Casazza, and D. Edidin. Equivalence of reconstruction from the absolute value of the frame coefficients to a sparse representation problem. *IEEE Signal Process. Lett.*, 14(5): 341–343, 2007.
- [3] Radu Balan. Stability of phase retrievable frames. *arXiv e-prints*, August 2013. arXiv:1308.5465.

- [4] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Appl. Comput. Harmon. Anal.*, 20:345–356, 2006.
- [5] Radu Balan, Bernhard G. Bodmann, Peter G. Casazza, and Dan Edidin. Painless reconstruction from magnitudes of frame coefficients. *J. Fourier Anal. Appl.*, 15(4):488–501, 2009.
- [6] Afonso S. Bandeira, Jameson Cahill, Dustin G. Mixon, and Aaron A. Nelson. Saving phase: Injectivity and stability for phase retrieval. *arXiv e-prints*, February 2013. arXiv:1302.4618.
- [7] Heinz H. Bauschke, Patrick L. Combettes, and D. Russell Luke. Phase retrieval, error reduction algorithm, and Fienup variants: A view from convex optimization. *J. Opt. Soc. Amer. A*, 19:1334–1345, 2002.
- [8] Bernhard G. Bodmann and Nathaniel Hammen. Stable phase retrieval with low-redundancy frames. *arXiv e-prints*, February 2013. arXiv:1302.5487.
- [9] Jameson Cahill, Peter G. Casazza, Jesse Peterson, and Lindsey Woodland. Phase retrieval by projections. *arXiv e-prints*, May 2013. arXiv:1305.6226v3.
- [10] Emmanuel J. Candès, Thomas Strohmer, and Vladislav Voroninski. PhaseLift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 66(8):1241–1274, 2013.
- [11] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *arXiv e-prints*, December 2013. arXiv:1312.0158.
- [12] Valentina Davidoiu, Bruno Sixou, Max Langer, and Françoise Peyrin. Nonlinear phase retrieval using projection operator and iterative wavelet thresholding. *IEEE Signal Process. Lett.*, 19(9):579 – 582, 2012.
- [13] James R. Fienup. Phase retrieval algorithms: a comparison. *Applied Optics*, 21(15):2758–2769, 1982.
- [14] Ralph W Gerchberg and W. Owen Saxton. A practical algorithm for the determination of the phase from image and diffraction plane pictures. *Optik*, 35(2):237–246, 1972.
- [15] Alexander Grothendieck and Jean Dieudonné. Éléments de géométrie algébrique iv, deuxième partie. *Publ. Math. IHES*, 24, 1965.
- [16] Alexander Grothendieck and Jean Dieudonné. Éléments de géométrie algébrique iv, troisième partie. *Publ. Math. IHES*, 28, 1966.
- [17] Franz J. Király, Paul von Bünau, Jan Saputra Müller, Duncan Blythe, Frank Meinecke, and Klaus-Robert Müller. Regression for sets of polynomial equations. *JMLR Workshop and Conference Proceedings*, 22:628–637, 2012.
- [18] David Mumford. *The Red Book of Varieties and Schemes*. Lecture Notes in Mathematics. Springer-Verlag Berlin Heidelberg, 1999.
- [19] Andrew E. Yagle and Amy E. Bell. One- and two-dimensional minimum and nonminimum phase retrieval by solving linear systems of equations. *IEEE Trans. Signal Process.*, 47(11):2978–2989, 1999.

A. Algebraic Geometry Fundamentals

A.1. Algebraic Geometry Glossary

We briefly give a glossary of algebraic terms used in the main corpus. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.

Definition A.1. A set $\mathcal{X} \subseteq \mathbb{K}^n$ is called *algebraic variety* if there are polynomials f_1, \dots, f_n variables such that

$$\mathcal{X} = \{x \in \mathbb{K}^n : f_1(x) = \dots = f_n(x) = 0\}.$$

Definition A.2. The *Zariski topology* on \mathbb{K}^n is the induced topology in which algebraic varieties are open. That is, *Zariski closed* sets being finite unions of algebraic varieties, and *Zariski open* sets the complement. The Zariski topology on some variety \mathcal{X} is the induced relative topology.

Definition A.3. An algebraic variety $\mathcal{X} \subseteq \mathbb{K}^n$ is called *irreducible* if can not be written as a proper union of algebraic varieties. That is, if $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ for algebraic varieties $\mathcal{X}_1, \mathcal{X}_2$, then $\mathcal{X}_1 \subseteq \mathcal{X}_2$ or $\mathcal{X}_2 \subseteq \mathcal{X}_1$.

Definition A.4. Let f_1, \dots, f_m be polynomials in n variables, let $\mathcal{X} \subseteq \mathbb{K}^n$ and $\mathcal{Y} \subseteq \mathbb{K}^m$ be algebraic varieties. A mapping

$$\phi : \mathcal{X} \rightarrow \mathcal{Y}, \quad x \mapsto (f_1(x), \dots, f_m(x))$$

is called *algebraic map* or *morphism of algebraic varieties*.

Definition A.5. A morphism of algebraic varieties, as above, is called *unramified at $x \in \mathcal{X}$* and *unramified over $\phi(x) \in \mathcal{Y}$* , if there is a Borel-open neighbourhood $U \subseteq \mathbb{K}^n$ (cave: not $U \subseteq \mathcal{X}$), with $x \in U$ such that for all $z \in U$, it holds that $\#\phi^{-1}\phi(x) = \#\phi^{-1}\phi(z)$. If \mathcal{X} is irreducible, ϕ is called *generically unramified* if the points $x \in \mathcal{X}$ at which ϕ is ramified are contained in a proper Zariski closed subset of \mathcal{X} .

Definition A.6. A generically unramified morphism, as above, with \mathcal{X} and \mathcal{Y} irreducible, is called *birational* if there is a proper Zariski closed subset \mathcal{Z} of \mathcal{X} such that f , restricted to $\mathcal{X} \setminus \mathcal{Z}$, is bijective.

A.2. Open Conditions and Generic Properties of Morphisms

In this section, we will summarize some algebraic geometry results used in the main corpus. The following results will always be stated for algebraic varieties over \mathbb{C} .

Proposition A.7. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of algebraic varieties (over any field). Then, if \mathcal{X} is irreducible, so is $f(\mathcal{X})$. In particular, if f is surjective, and \mathcal{X} is irreducible, then \mathcal{Y} also is.

Proof. This is classical; suppose the converse, that is, $f(\mathcal{X}) = \mathcal{Z}_1 \cup \mathcal{Z}_2$ is a proper union of algebraic sets. Then, using that f is algebraic, and therefore continuous in the Zariski topology, it follows that \mathcal{X} is a proper union $\mathcal{X} = f^{-1}(\mathcal{Z}_1) \cup f^{-1}(\mathcal{Z}_2)$ of algebraic sets. This contradicts \mathcal{X} being irreducible, proving the statement by contraposition. \square

Theorem 9. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of algebraic varieties. The function

$$\mathcal{Y} \rightarrow \mathbb{N}, \quad y \mapsto \dim f^{-1}(y)$$

is upper semicontinuous in the Zariski topology.

Proof. This follows from [16, Théorème 13.1.3]. \square

Proposition A.8. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of algebraic varieties, with \mathcal{Y} be irreducible. Then, there is an open dense subset $V \subseteq \mathcal{Y}$ such that $f : U \rightarrow V$, where $U = f^{-1}(V)$, is a flat morphism.

Proof. This follows from [15, Théorème 6.9.1]. \square

Theorem 10. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of algebraic varieties. Let $d, v \in \mathbb{N}$. Then, the following are open conditions for $y \in \mathcal{Y}$; that is, the sets $\{y \in \mathcal{Y} : \text{condition } (*) \text{ holds for } y\}$ is a Zariski open subset of \mathcal{Y} .

- (i) $\dim f^{-1}(y) \leq d$.
- (ii) f is unramified over y .
- (iii) f is unramified over y , and the number of irreducible components of $f^{-1}(y)$ equals v .

In particular, if f is surjective, then the following is an open property as well:

- (iv) f is unramified over y , and $\#f^{-1}(y) = v$.

Proof. (i) follows from [15, Corollaire 6.1.2].

(ii) follows from [16, Théorème 12.2.4(v)].

(iii) follows from [16, Théorème 12.2.4(vi)].

(iv) follows from (i), applied in the case $\dim f^{-1}(y) \leq 0$ which is equivalent to $\dim f^{-1}(y) = 0$ due to surjectivity of f , and (iii). \square

Corollary A.9. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a generically unramified and surjective morphism of algebraic varieties, with \mathcal{Y} be irreducible. Then, there are unique $d, v \in \mathbb{N}$ such that the following sets are Zariski closed, proper subsets of \mathcal{Y} (and therefore Hausdorff zero sets):

- (i) $\{y : \dim f^{-1}(y) \neq d\}$
- (ii) $\{y : f \text{ is ramified at } y\}$
- (iii) $\{y : f \text{ is ramified at } y\} \cup \{y : \#f^{-1}(y) \neq v\}$

Proof. This is implied by Theorem 10 (i), (ii) and (iii), using that a non-zero open subset of the irreducible variety \mathcal{Y} must be open dense, therefore its complement in \mathcal{Y} is a closed and a proper subset of \mathcal{Y} . \square

Proposition A.10. Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of algebraic varieties, with \mathcal{Y} irreducible. Then, the following are equivalent:

- (i) f is unramified over y and $\#f^{-1}(y) = v$.
- (ii) There is a Borel open neighborhood $U \subseteq \mathcal{Y}$ of $y \in U$, such that f is unramified over U and $\#f^{-1}(z) = v$ for all $z \in U$.
- (iii) There is a Zariski open neighborhood $U \subseteq \mathcal{Y}$ of $y \in U$, dense in \mathcal{Y} , such that f is unramified over U and $\#f^{-1}(z) = v$ for all $z \in U$.

Proof. The equivalence is implied by Corollary A.9 and the fact that \mathcal{Y} is irreducible. Note that either condition implies that f is generically unramified due to Theorem 10 (ii) and irreducibility of \mathcal{Y} . \square

A.3. Real versus Complex Genericity

We derive some elementary results how generic properties over the complex and real numbers relate. While some could be taken for known results, they appear not to be folklore - except maybe Lemma A.12. In any case, they seem not to be written up properly in literature known to the authors.

Definition A.11. Let $\mathcal{X} \subseteq \mathbb{C}^n$ be a variety. We define the *real part* of \mathcal{X} to be $\mathcal{X}_{\mathbb{R}} := \mathcal{X} \cap \mathbb{R}^n$.

Lemma A.12. Let $\mathcal{X} \subseteq \mathbb{C}^n$ be a variety. Then, $\dim \mathcal{X}_{\mathbb{R}} \leq \dim \mathcal{X}$, where $\dim \mathcal{X}_{\mathbb{R}}$ denotes the Krull dimension of $\mathcal{X}_{\mathbb{R}}$, regarded as a (real) subvariety of \mathbb{R}^n , and $\dim \mathcal{X}$ the Krull dimension of \mathcal{X} , regarded as subvariety of \mathbb{C}^n .

Proof. Let $k = n - \dim \mathcal{X}$. By [18, section 1.1], \mathcal{X} is contained in some complete intersection variety $\mathcal{X}' = V(f_1, \dots, f_k)$. That is (f_1, \dots, f_k) is a complete intersection, with $f_i \in \mathbb{C}[X_1, \dots, X_n]$ and $\dim \mathcal{X}' = \dim \mathcal{X}$, such that f_i is a non-zero divisor modulo f_1, \dots, f_{i-1} . Define $g_i := f_i \cdot f_i^*$, one checks that $g_i \in \mathbb{R}[X_1, \dots, X_n]$, and define $\mathcal{Y} := V(g_1, \dots, g_k)$ and $\mathcal{Y}_{\mathbb{R}} := \mathcal{Y} \cap \mathbb{R}^n$. The fact that f_i is a non-zero divisor modulo f_1, \dots, f_{i-1} implies that g_i is a non-zero divisor modulo g_1, \dots, g_{i-1} ; since $g_i \cdot h \cong 0$ modulo g_1, \dots, g_{i-1} implies $f_i \cdot (h \cdot f_i^*) \cong 0$ modulo f_1, \dots, f_{i-1} . Therefore, $\dim \mathcal{Y}_{\mathbb{R}} \leq \dim \mathcal{X}$; by construction, $\mathcal{X}' \subseteq \mathcal{Y}$, and $\mathcal{X} \subseteq \mathcal{X}'$, therefore $\mathcal{X}_{\mathbb{R}} \subseteq \mathcal{Y}_{\mathbb{R}}$, and thus $\dim \mathcal{X}_{\mathbb{R}} \leq \dim \mathcal{Y}_{\mathbb{R}}$. Combining it with the above inequality yields the claim. \square

Definition A.13. Let $\mathcal{X} \subseteq \mathbb{C}^n$ be a variety. If $\dim \mathcal{X} = \dim \mathcal{X}_{\mathbb{R}}$, we call \mathcal{X} *observable over the reals*. If \mathcal{X} equals the (complex) Zariski-closure of $\mathcal{X}_{\mathbb{R}}$, we call \mathcal{X} *defined over the reals*.

Proposition A.14. Let $\mathcal{X} \subseteq \mathbb{C}^n$ be a variety.

- (i) If \mathcal{X} is defined over the reals, then \mathcal{X} is also observable over the reals.
- (ii) The converse of (i) is false.
- (iii) If \mathcal{X} irreducible and observable over the reals, then \mathcal{X} is defined over the reals.

Proof. (i) Let $k = n - \dim \mathcal{X}_{\mathbb{R}}$. By [18, section 1.1], $\mathcal{X}_{\mathbb{R}}$ is contained in some complete intersection variety $\mathcal{X}' = V(f_1, \dots, f_k)$, with $f_i \in \mathbb{R}[X_1, \dots, X_n]$ a complete intersection. By an argument, analogous to the proof of Lemma A.12, one sees that the f_i are a complete intersection in $\mathbb{C}[X_1, \dots, X_n]$ as well. Since the Zariski-closure of $\mathcal{X}_{\mathbb{R}}$ and \mathcal{X} are equal, it holds that $f_i \in I(\mathcal{X})$. Therefore, $\mathcal{X} \subseteq V(f_1, \dots, f_k)$, which implies $\dim \mathcal{X} \leq n - k$, and by definition of k , as well $\dim \mathcal{X} \leq \dim \mathcal{X}_{\mathbb{R}}$. With Lemma A.12, we obtain $\dim \mathcal{X}_{\mathbb{R}} = \dim \mathcal{X}$, which was the statement to prove.

(ii) It suffices to give a counterexample: $\mathcal{X} = \{1, i\} \subseteq \mathbb{C}$. Alternatively (in a context where \emptyset is not a variety) $\mathcal{X} = \{(1, x) : x \in \mathbb{C}\} \cup \{(i, x) : x \in \mathbb{C}\} \subseteq \mathbb{C}^2$.

(iii) By definition of dimension, Zariski-closure preserves dimension. Therefore, the closure $\overline{\mathcal{X}_{\mathbb{R}}}$ is a sub-variety of \mathcal{X} , with $\dim \overline{\mathcal{X}_{\mathbb{R}}} = \dim \mathcal{X}$. Since \mathcal{X} is irreducible, equality $\overline{\mathcal{X}_{\mathbb{R}}} = \mathcal{X}$ must hold. \square

Theorem 11. Let $\mathcal{X} \subseteq \mathbb{C}^n$ be an irreducible variety which is observable over the reals, let $\mathcal{X}_{\mathbb{R}}$ be its real part. Let P be an algebraic property. Assume that a generic $x \in \mathcal{X}$ is P . Then, a generic $x \in \mathcal{X}_{\mathbb{R}}$ has property P as well.

Proof. Since P is an algebraic property, the P points of \mathcal{X} are contained in a proper sub-variety $\mathcal{Z} \subseteq \mathcal{X}$, with $\dim \mathcal{Z} \leq \dim \mathcal{X}$. Since \mathcal{X} is observable over the reals, it holds $\dim \mathcal{X} = \dim \mathcal{X}_{\mathbb{R}}$. By Lemma A.12, $\dim \mathcal{Z}_{\mathbb{R}} \leq \dim \mathcal{Z}$. Putting all (in-)equalities together, one obtains $\dim \mathcal{Z}_{\mathbb{R}} \leq \dim \mathcal{X}_{\mathbb{R}}$. Therefore, the $\mathcal{Z}_{\mathbb{R}}$ is a proper sub-variety of $\mathcal{X}_{\mathbb{R}}$; and the P points of $\mathcal{X}_{\mathbb{R}}$ are contained in it - this proves the statement. \square

B. Results on Phase Retrieval

B.1. Properties of the Forward Map

In this section we will check that the technical assumptions hold in the case of the relevant examples. We start with introducing notation for two maps which relate the signal/measurement varieties to projection matrices:

Notation B.1. In the following, we will denote

$$\begin{aligned}\Upsilon : \mathbb{C}^{r \times n} \times \mathbb{C}^{r \times n} &\rightarrow \mathcal{P}_\rho(r), & (Q, S) &\mapsto Q^\top S, \\ \Upsilon_{\mathbb{C}} : \mathbb{C}^{r \times n} \times \mathbb{C}^{r \times n} &\rightarrow \mathcal{P}_{\mathbb{C}}(r), & (Q, S) &\mapsto (Q^\top Q + S^\top S, Q^\top S - S^\top Q).\end{aligned}$$

The maps Υ and $\Upsilon_{\mathbb{C}}$ can be seen to be surjective; as an immediate consequence of this fact, we can relate genericity of projections to genericity of measurement matrices:

Proposition B.2. *Let $P, Q \in \mathbb{C}^{r \times n}$ be generic matrices. Then:*

- (i) $\Upsilon(P, Q)$ resp. $\Upsilon_{\mathbb{C}}(P, Q)$ are generic inside $\mathcal{P}_\rho(r)$ resp. $\mathcal{P}_{\mathbb{C}}(r)$
- (ii) $\Upsilon(P, P)$ resp. $\Upsilon_{\mathbb{C}}(P, P^*)$ are generic Hermitian matrices inside $\mathcal{P}_\rho(r)$ resp. $\mathcal{P}_{\mathbb{C}}(r)$

Proof. $P, Q \in \mathbb{C}^{r \times n}$ being generic, by convention, is equivalent to choosing open dense $U_1, U_2 \subseteq \mathbb{C}^{r \times n}$. Since Υ and $\Upsilon_{\mathbb{C}}$ are surjective (onto the Hermitian matrices in (ii)), and as algebraic maps continuous in the Zariski topology, the image of $U_1 \times U_2$ (or $U_1 \times U_1^*$) will be open dense in the image as well. \square

We now examine the signal and measurement varieties in more detail:

Proposition B.3. *Keep the notations of Section 2.1. For any $r \in \mathbb{N}$, the varieties $\mathcal{P}_{\mathbb{C}}(r)$ and $\mathcal{P}_\rho(r)$ are:*

- (i) *irreducible.*
- (ii) *observable over the reals.*
- (iii) *defined over the reals.*

In particular, this holds for $\mathcal{S}_{\mathbb{C}} = \mathcal{P}_{\mathbb{C}}(1)$ and $\mathcal{S}_\rho = \mathcal{P}_\rho(1)$ as well.

Proof. (i) For $\mathcal{P}_{\mathbb{C}}(r)$, irreducibility follows from surjectivity of $\Upsilon_{\mathbb{C}}$, Proposition A.7 and irreducibility of complex affine space. Similarly, for $\mathcal{P}_\rho(r)$, the statement follows from surjectivity of Υ , and Proposition A.7.

(ii) follows from considering the maps $\Upsilon_{\mathbb{C}}$ and Υ over the reals, observing that the rank its Jacobian is not affected by this.

(iii) follows from (i), (ii) and Proposition A.14 (iii). \square

Proposition B.4. *Keep the notations of Section 2.2.1 and 2.2.2. Assume that $\mathcal{S} = \mathcal{S}_{\mathbb{C}}$ or \mathcal{S}_ρ . Then ϕ_A is generically unramified for any $A \in ((\mathbb{C}^{n \times n})^r)^k$. Furthermore, if \mathcal{P} contains \mathcal{S} (that is, all rank one signals), then ϕ is generically unramified.*

Proof. \mathcal{S} and $\mathcal{P}^{(k)} \times \mathcal{S}$ are irreducible by Proposition B.3. By Proposition A.10, it therefore suffices to show that there exists x in the image of ϕ_A or ϕ such that x does not ramify - but a generic choice of signal and/or measurement will suffice. \square

B.2. Proofs of Main Theorems

This section contains the technical proofs for our main theorems, which are stated in a slightly longer version.

Theorem 12. *For a fixed measurement regime (A_1, \dots, A_k) , consider the three cases*

- (a) *A generic signal $Z \in \mathcal{S}$ is not identifiable from $\phi_A(Z)$.*
- (b) *A generic, but not all signals $Z \in \mathcal{S}$, are identifiable from $\phi_A(Z)$.*
- (c) *All signals $Z \in \mathcal{S}$ are identifiable from $\phi_A(Z)$.*

The three cases above are equivalent to

- (a) *No signal $Z \in \mathcal{S}$ is perturbation-stably identifiable from $\phi_A(Z)$.*
- (b) *A generic, but not all signals $Z \in \mathcal{S}$, are perturbation-stably identifiable from $\phi_A(Z)$.*
- (c) *All signals $Z \in \mathcal{S}$ are perturbation-stably identifiable from $\phi_A(Z)$.*

Any triple of cases above is furthermore equivalent to

- (a) *ϕ_A is not birational.*
- (b) *ϕ_A is birational, but not an isomorphism.*
- (c) *ϕ_A is an isomorphism.*

In particular, the three cases, in either of the three formulations, are mutually exclusive and exhaustive.

Proof. Mutual exclusivity and exhaustiveness of (a),(b),(c) follow from the third, algebraic formulation and elementary logic, once equivalence is established.

We prove equivalence of the first and second triple. Equivalence of (c) in the first and second triple follows from the fact that if all signals are identifiable, then all signals are perturbation-stably identifiable, since \mathcal{S} is an open neighborhood of any signal $Z \in \mathcal{S}$. The converse follows from the fact that perturbation-stably identifiable signals are identifiable. Equivalence of (a) and (b) the first and second triple then follows from the assertion in Proposition 2.10 that the perturbation-stably identifiable signals form a Zariski open subset of \mathcal{S} , and the perturbation-stable signals are a subset of the identifiable signals.

We will now prove equivalence of the second and third triple. For that, note that if ϕ_A is birational if and only if there is $Z \in \mathcal{S}$ with $\#\phi_A^{-1}\phi_A(Z) = 1$, and an isomorphism if and only if there is no $Z \in \mathcal{S}$ with $\#\phi_A^{-1}\phi_A(Z) \neq 1$. Proposition 2.10 then establishes the equivalence of the second and third triple. \square

Theorem 13. *Assume that ϕ is generically unramified. Consider the three cases*

- (a) *A generic measurement regime $A \in \mathcal{P}^k$ is non-identifying.*
- (b) *A generic measurement regime $A \in \mathcal{P}^k$ is incompletely identifying.*
- (c) *A generic measurement regime $A \in \mathcal{P}^k$ is completely identifying.*

The three cases above are equivalent to

- (a) *A generic measurement regime $A \in \mathcal{P}^k$ is stably non-identifying. No measurement regime $A \in \mathcal{P}^k$ is stably generically identifying.*

(b) A generic measurement regime $A \in \mathcal{P}^k$ is stably incompletely identifying.

(c) A generic measurement regime $A \in \mathcal{P}^k$ is stably completely identifying.

Any triple of cases above is furthermore equivalent to

(a) ϕ is not birational.

(b) ϕ is birational, and there is no open dense $U \subseteq \mathcal{P}^k$ such that ϕ is an isomorphism on $U \times \mathcal{S}$.

(c) ϕ is birational, and there is an open dense $U \subseteq \mathcal{P}^k$ such that ϕ is an isomorphism on $U \times \mathcal{S}$.

In particular, the three cases, in either of the three formulations, are mutually exclusive and exhaustive.

Proof. The proof is analogous to that of Theorem 12. □