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

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

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 $z \in U$, if 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 $f : \mathcal{X} \to \mathcal{Y}$ 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 7. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of algebraic varieties. The function $\mathcal{Y} \to \mathbb{N}$, $y \mapsto \dim f^{-1}(y)$ is upper semicontinuous in the Zariski topology.*

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

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

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

Theorem 8. *Let $f : \mathcal{X} \to \mathcal{Y}$ 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 $\{y \in \mathcal{Y} \; : \; \text{condition (*) holds for } y\}$ is a Zariski open subset of $\mathcal{Y}$.*

(i) $\dim f^{-1}(y) \le d$.

(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 $\dim f^{-1}(y) \le 0$ which is equivalent to $\dim f^{-1}(y) = 0$ due to surjectivity of f, and (iii). $\square$

Corollary A.9. *Let $f : \mathcal{X} \to \mathcal{Y}$ 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) $\{y \; : \; \dim f^{-1}(y) \ne d\}$

(ii) $\{y \; : \; f \text{ is ramified at } y\}$

(iii) $\{y \; : \; f \text{ is ramified at } y\} \cup \{y \; : \; \#f^{-1}(y) \ne v\}$

Proof. This is implied by Theorem 8 (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 $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of algebraic varieties, with $\mathcal{Y}$ irreducible. Then, the following are equivalent:*

(i) *f is unramified over y and $\#f^{-1}(y) = \nu$.*

(ii) *There is a Borel open neighborhood $U \subseteq \mathcal{Y}$ of $y \in U$, such that f is unramified over U and $\#f^{-1}(z) = \nu$ 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 $\#f^{-1}(z) = \nu$ 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 8 (ii) and irreducibility of $\mathcal{Y}$. $\qquad\square$

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 [19, section 1.1], $\mathcal{X}$ is contained in some complete intersection variety $\mathcal{X}' = \mathrm{V}(f_1, \dots, f_k)$. 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 $\mathcal{Y} := \mathrm{V}(g_1, \dots, g_k)$ 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. $\qquad\square$

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 [19, section 1.1], $\mathcal{X}_{\mathbb{R}}$ is contained in some complete intersection variety $\mathcal{X}' = \mathrm{V}(f_1, \dots, f_k)$, 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 $f_i \in \mathrm{I}(\mathcal{X})$. Therefore, $\mathcal{X} \subseteq \mathrm{V}(f_1, \dots, f_k)$, which imples $\dim \mathcal{X} \leq n - k$, 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 $\varnothing$ 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. $\qquad\square$

Theorem 9. *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 $\dim \mathcal{Z}$ $\dim \mathcal{X}$. 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 $\dim \mathcal{Z}_{\mathbb{R}}$ $\dim \mathcal{X}_{\mathbb{R}}$. 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. $\qquad\square$

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

$$\Upsilon : \mathbb{C}^{r \times n} \times \mathbb{C}^{r \times n} \to \mathcal{P}_\rho(r), \ (Q, S) \mapsto Q^\top S,$$

$$\Upsilon_{\mathbb{C}} : \mathbb{C}^{r \times n} \times \mathbb{C}^{r \times n} \to \mathcal{P}_{\mathbb{C}}(r),$$

$$(Q, S) \mapsto (Q^\top Q + S^\top S, Q^\top S - S^\top Q).$$

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 $\mathcal{S}_{\rho}$. Then ϕ_A is generically unramified for any $A \in \left((\mathbb{C}^{n \times n})^{\gamma}\right)^k$. 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 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 B.5. *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 $\mathrm{Tr}(Z \cdot A_1), \ldots, \mathrm{Tr}(Z \cdot A_k)$ hold:*

(i) *If $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$ 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 $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$ 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 $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$ 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 $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$.*

(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 $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$.*

(vi) *If $\mathcal{P}$ is completely identifying, then all signals $Z \in \mathcal{S}_{\mathbb{R}}$ can be perturbation-stably identified by a generic $(A_1, \ldots, A_k) \in \mathcal{P}_{\mathbb{R}}$.*

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 $\mathcal{P}_{\mathbb{R}}$.

B.3 Proofs

Proof of Proposition 2.9

The statement is implied by Proposition A.10. $\square$

Proof of Proposition 2.14

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

Proof of Proposition 2.15

Consider the maps

$$\phi : \mathcal{P}^{(k)} \times \mathcal{S} \to \mathcal{P}^{(k)} \times \mathbb{C}^k,$$
$$(A_1, \ldots, A_k, Z) \mapsto (A_1, \ldots, A_k, \mathrm{Tr}(Z \cdot A_1), \ldots, \mathrm{Tr}(Z \cdot A_n)),$$
$$\psi : \mathcal{P}^{(k)} \times \mathcal{S} \to \mathcal{P}^{(k)}, (A_1, \ldots, A_k, Z) \mapsto (A_1, \ldots, A_k),$$
$$\pi : \mathcal{P}^{(k)} \times \mathcal{S} \to \mathcal{S}, (A_1, \ldots, A_k, Z) \mapsto Z.$$

(i) Consider the set $\mathcal{Y} = \{x \in \mathcal{P}^{(k)} \times \mathcal{S} : \phi(x) \text{ is identifiable and unramified}\}$. By Proposition 2.14 $\mathcal{Z}$ 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 $\mathcal{V} := \psi\left(\mathcal{Y}^C\right)$ 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. □

Proofs of Theorems 1 and 2

This section contains the technical proofs for Theorems 1 and 2, which are stated in a slightly longer versions for this purpose.

Theorem 10. *For a fixed measurement regime $(A_1, \ldots, A_k)$, 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 2.9 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 2.9 then establishes the equivalence of the second and third triple. □

Theorem 11. *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 10. □

Proof of Corollary 2.11

This is a direct consequence of Proposition 2.9, using that by taking Radon-Nikodym derivatives, $\mathcal{S}$-Hausdorff zero sets are as well probability measure zero sets for any continuous probability measure. □

Proof of Proposition B.5

Statements (i) and (iv) follow already from the definitions, and Proposition 2.15. The other numbered statements are implied by Theorem 9 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 $\mathcal{P}'_{\mathbb{R}}$. □

Proof of Lemma 2.19

We prove the statement separately for $\mathcal{P}^{(k)}$ being (i) generically unramified (ii) generically identifying, and (iii) completely identifying. (i) follows from Theorem 8 (ii). For (ii), the characterization in Theorem 11 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 11. (iii) follows in analogy, repeating the argument for all $Z \in \mathcal{S}$. □

Proof of Lemma 2.20

We prove the statement separately for $\mathcal{P}^{(k)}$ being (i) generically identifying, and (ii) completely identifying. Let $A_1, \ldots, A_k$ be generic in $\mathcal{P}_1, \ldots, \mathcal{P}_k$; 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) $(A_1, \ldots, A_k)$ are generically identifying if for generic z, one can reconstruct z up to phase/sign from the z^*A_iz. 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 $(A_1, \ldots, A_k)$ is generically identifying if and only if $(U_1, S_1^*A_2S_1, \ldots, S_1^*A_kS_1)$ is generically identifying. Since $A_j, j \geq 2$ was generic,

the matrices $S_1^*A_2S_1, \ldots, S_1^*A_kS_1$ are also generic, and independent of U_1 therefore they can be replaced anew by generic $A_2, \ldots, A_k$. Repeating the argument k times yields the claim. The proof for (ii) is analogous, noting that identifiability holds for generic $(A_1, \ldots, A_k)$, but all z. □

Proof of Proposition 2.22

If suffices to show that no $(A_1, \ldots, A_n) \in (\mathbb{C}^{n \times n})^n$ can be stably generically identifying. We proceed by contradiction and assume the contrary. Proposition 2.14 then implies that $(\mathbb{C}^{n \times n})^n$ is generically identifying, so we may replace $A_1, \ldots, A_n$ by a generic choice in $(\mathbb{C}^{n \times n})^n$. Fixing $z^\top A_1z, \ldots, z^\top A_nz$ 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} 1 solutions, yielding a contradiction. □

Proof of Theorem 3

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 2.15 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 2.22, we obtain the statement. □

Proof of Theorem 4

$\lambda(\mathcal{P}) \geq n+1$ is implied by Proposition 2.22. $\kappa(\mathcal{P}) \geq 2n-1$ 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 2.19. The statement for orthogonal projectors follows from Lemma 2.20. □

Proof of Theorem 5

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 2.20, 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 B.5, noting that identifiability of $Z = zz^\top \in \mathbb{R}^{n \times n}$ is equivalent to identifiability of z up to sign. □

B.4 Identifiability of Complex Signals

Proposition B.6. *Consider identifiability from complex signals, corresponding to the complex signal variety $\mathcal{S}_\iota = \{(xx^\top + yy^\top, yx^\top - xy^\top) : x, y \in \mathbb{C}^n\}$. 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 $\dim \mathcal{S}_\iota = 2n - 1$, therefore the fiber

$\phi^{-1}(\phi(A_1, \ldots, A_k, Z))$ can be finite only if $k \geq 2n - 1$. Since S_ι is non-linear, it has degree strictly bigger than one, implying by Bezout's theorem that $\phi^{-1}(\phi(A_1, \ldots, A_k, Z))$ is not finite for $k = 2n - 1$. Therefore, $\lambda(\mathcal{P}) \geq 2n$. $\qquad\square$

Theorem 12. *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:*
$$\lambda(\mathcal{P}) = 2n, \quad and \quad \kappa(\mathcal{P}) \leq 4n - 4.$$

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 2.15 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 B.6, this yields the statement. $\qquad\square$

Theorem 13. *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:*
$$\lambda(\mathcal{P}) = 2n, \quad and \quad \kappa(\mathcal{P}) \leq 4n - 4.$$ *The result remains unaltered if the projectors* $\mathcal{P}$ *are restricted to be unitary.*

Proof. $\lambda(\mathcal{P}) \geq 2n$ is implied by Proposition B.6. Lower bounds $\lambda(\mathcal{P}) \leq 2n$ and $\kappa(\mathcal{P}) \leq 4n - 4$ are implied by combining Theorem 12 and Lemma 2.19. The statement for unitary projectors follows from Lemma 2.20. $\qquad\square$

Proof of Theorem 6

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 2.20, we can thus assume that we have generic A_i of rank r_i. The statement is then implied by Theorem 13 (i) and Proposition B.5, noting that identifiability of (X, Y) is equivalent to identifiability of $X + \iota Y = zz^* \in \mathbb{C}^{n \times n}$, up to phase. $\qquad\square$