(Algebraic) Geometry and phase retrieval
, (Based on *Projections and phase retrieval*, arXiv:1506.00674)
FACG, Bremen, July 31, 2015.

Dan Edidin
University of Missouri

Original (complete) phase retrieval problem. Given a collection of N vectors (aka a frame) $v_1, \ldots, v_N$ in $\mathbb{R}^M$ or $\mathbb{C}^M$ what conditions on the v_i ensure that every vector x can be recoverd (up to a global phase factor) from the non-negative real vector $(|\langle v_1, x\rangle|, \ldots, |\langle v_N, x\rangle|)$?
This problem is equivalent to asking when the map

$$\mathbb{R}^M/\pm 1 \to \mathbb{R}^N_{\geq 0}, x \mapsto \left(|\langle v_1, x\rangle|^2, \ldots, |\langle v_N, x\rangle|^2\right)$$

or

$$\mathbb{C}^M/S^1 \to \mathbb{R}^N_{\geq 0}, x \mapsto \left(|\langle v_1, x\rangle|^2, \ldots, |\langle v_N, x\rangle^2|\right)$$

is injective?

In the real case there is a complete solution
Theorem $\mathbb{R}$. (Balan, Casazza, Edidin ACHA2006) Phase retrieval is possible with $v_1, \ldots, v_N$ if and only if for every subset $S \subset \{1, \ldots, N\}$ at least one of the collection of vectors $\{v_i\}_{i \in S}$ or $\{v_j\}_{j \in S^c}$ spans (complement property).

The complement property condition implies that if $N < 2d - 1$ then no frame admits complete phase retrieval.

In the complex case things are a bit messier.

Theorem $\mathbb{C}$ (Conca, Edidin, Hering, Vinzat ACHA2015) If $N \geq 4M - 4$ then a generic collection of vectors $v_1, \ldots, v_N \in \mathbb{C}^M$ admits phase retrieval. Moreover this bound is sharp if $N = 2^k + 1$ for some integer k.

Remark. The $4M - 4$ bound is not sharp. Cynthia Vinzant (2014) has an example of an 11 element frame in $\mathbb{C}^4$ which admits phase retrieval. Worse, we have no intrinsic characterization of the complement of the generic set of "good" frames. In particular, while any given complex frame of size $4M - 4$ or larger admits phase retrieval with probability 1, we have no way to test whether this property holds. (In principal we do know one hypersurface containing the locus of "bad" frames, but its degree is exponential in M^2.)

Generalization of the phase retrieval problem. Replace the vectors v_i by orthogonal projections.

Problem. Given a collection $\Phi = \{P_1, \ldots, P_N\}$. of orthogonal projections in $\mathbb{R}^M$ (or $\mathbb{C}^M$), determine conditions on the P_i which ensure that we recover all vectors x from the real numbers, $||P_1 x||, \ldots, ||P_N x||$.

Remark. If the $\{v_1, \ldots, v_N\}$ is a collection of (non-zero) vectors and P_{L_i} is the projection onto the line determined by v_i then $|\langle x, v_i\rangle|$ is the magnitude of the vector $\frac{\langle x,v\rangle}{v,v} v$ which is the formula for projection of one vector onto another. So when the ranks of the P_i are 1 this is the usual phase retrieval problem.

Remark. The question of phase retrieval for projections was first raised (to my knowledge) in the paper *Phase retrieval by projections* by Cahill, Casazza, Peterson, and Woodland (arxiv:1305.6626).

Theorem. (CCPW13) For $N = 2M - 1$ there exist collections $P_1, \ldots, P_N$ of projections of any (non-zero) rank which admit phase retrieval.

They also raise a number of interesting (to me anyway) questions including

Problem 1. What is the minimal number of N such that there exists a collection of projections $P_1, \ldots, P_N$ which admits phase retrieval. Does this number depend on the ranks?

Problem 2. The construction of the collection in the Theorem above is very structured (you play games with orthonormal bases). Does a random collection of $2M - 1$ admit phase retrieval?

Using (Algebro) Geometric techniques I was able to answer Problem 2 and say something about Problem 1.

Theorem 1. (Edidin 2015) Retrieval is possible if and only if for every $x \in R^M$, the vectors $P_1 x, \ldots, P_N x$ span.

Easy Corollary 1. If the P_i all have rank one and are determined by vectors $v_1, \ldots, v_N$, then phase retrieval is possible if and only the collection $\{v_1, \ldots, v_N\}$ satisfies the complement property.

Easy Corollary 2. If at least $M-1$ of the P_i have rank one then at least M other projections are necessary for phase retrieval. Likewise, if $M-2$ of the projections have rank $M-1$ then at least M other projections are necessary.

Theorem 2. (Edidin 2015) If $N \geq 2M - 1$ then a generic collection of projections of any (non-zero) ranks admits phase retrieval. Additionally, if $M = 2^k + 1$ then no collection of $2M - 2$ projections admits phase retrieval.

Remark. The second statement of the theorem was proved independently by Zhiqiang Xu (arxiv 1505.07204) who also used Vinzant's technique to construct an example of 6 rank 2 projections in $\mathbb{R}^4$ which admit phase retrieval.

Remark. Theorem 2 answers Problem 2 of CCPW13.

Definition. A map $f: X \to Y$ of manifolds is a *global immersion* if an only if for every point $x \in X$ the linear map $df_x: T_{x,X} \to T_{f(x),Y}$ is injective.

Remark. If f is an immersion then it is locally in the source an embedding, but it doesn't need to be globally injective. Conversely, an injective map need not be an immersion.

Example. The map $f: \mathbb{R}^1 \to \mathbb{R}^2$, $t \mapsto (t^2, t^3 - t)$ is a global immersion which is not an embedding, since the derivative never vanishes but $f(1) = f(-1) = (1, 0)$. On the other hand, $t \mapsto (t^2, t^3)$ is injective but not a global immersion since the derivative vanished when $t = 0$.

Proof of Theorem 1.

Observation. If $\mathcal{A} = \{P_1, \ldots, P_N\}$ is a collection of projections then $\mathcal{A}$ admits phase retrieval if and only if the quadratic map

$$\Phi_{\mathcal{A}} \colon \mathbb{R}^M/\pm 1 \to \mathbb{R}^N_{\geq 0},\ x \mapsto \left(||P_1 x||^2, \ldots, ||P_N x||^2\right)$$

is injective.

Lemma. Let $P \colon \mathbb{R}^M \to \mathbb{R}^M$ be a rank k projection and let $f \colon \mathbb{R}^M \to \mathbb{R}$ be defined by $x \mapsto \langle Px, Px \rangle$. For any $x \in \mathbb{R}^M$, $df_x(y) = 2\langle Px, y\rangle$ where we identify $T_x\mathbb{R}^M = \mathbb{R}^M$ and $T_{f(x)}\mathbb{R} = \mathbb{R}$.

Proof. Since P is a projection there is an orthonormal basis of eigenvectors for P. With respect to this basis $P = \operatorname{diag}(1, \ldots 1, 0, \ldots, 0)$. If we choose coordinates determined by this basis then $f(x_1, \ldots, x_M) = x_1^2 + x_2^2 + \ldots x_k^2$, so $\partial f/\partial x_i = 2x_i$ if $i \leq k$ and $\partial f/\partial x_i = 0$ if $i > k$. Thus the derivative at a point $x = (a_1, \ldots, a_M) \in \mathbb{R}^M$ is the linear operator that maps $y = (b_1, \ldots, b_M)$ to $2\sum_{i=1}^k a_i b_i = 2\langle Px, y\rangle$

Proof of Theorem 1 continued...

Proposition 1. The map $\mathcal{A}_\Phi$ is an immersion at $\overline{x} \in \left(\mathbb{R}^M \setminus \{0\}\right) / \pm 1$ if and only if $P_1 x, \ldots, P_N x$ span an M-dimensional subspace of $\mathbb{R}^M$ where x is either lift of $\overline{x}$ to $\mathbb{R}^N \setminus \{0\}$.

Proof. Consider the map $\mathcal{B}_\Phi \colon \mathbb{R}^M \setminus \{0\} \to \mathbb{R}^N$, $x \mapsto (\langle P_1 x, P_1 x\rangle, \ldots, \langle P_N x, P_N x\rangle)$. The map $\mathcal{B}_\Phi$ is the composition of $\mathcal{A}_\Phi$ with the double cover $\mathbb{R}^M \setminus \{0\} \to \left(\mathbb{R}^M \setminus \{0\}\right) / \pm 1$. Since the derivative of a covering map is an isomorphism, it suffices to prove the proposition for the map $\mathcal{B}_\Phi$. Applying our Lemma to each component of $\mathcal{B}_\Phi$ we see that $d\mathcal{B}_\Phi$ is the linear transformation $y \mapsto 2(\langle P_1 x, y\rangle, \ldots, \langle P_N x, y\rangle)$. Hence $(d\mathcal{B}_\Phi)_x$ and thus $(d\mathcal{A}_\Phi)_x$ is injective if and only if there is no non-zero vector y which is orthogonal to each $P_i x$, or equivalently the vectors $P_i x$ span all of $\mathbb{R}^M$.

Conclusion of the proof of Theorem 1.

Proposition 2. The map $\mathcal{A}_\Phi$ is injective if and only if it is a global immersion.

Proof. First assume that $\mathcal{A}_\Phi$ is not an immersion. By Proposition 1 there exists an $x \neq 0$ such that $P_1x, \ldots, P_Nx$ fail to span $\mathbb{R}^M$. Let y be a non-zero vector orthogonal to all the P_ix and consider the vectors $x' = x + y$ and $y' = x - y$. Then

$$\begin{aligned} |P_ix'||^2 &= \langle P_ix', x'\rangle \text{ since } P_i \text{ is an orthogonal projection} \\ &= \langle P_ix, x\rangle + \langle P_iy, y\rangle + \langle P_iy, x\rangle + \langle P_ix, y\rangle \\ &= ||P_ix||^2 + ||P_iy||^2 \end{aligned}$$

where the last equality holds because

$$\langle P_iy, x\rangle = \langle P_iy, P_ix\rangle = \langle P_ix, P_iy\rangle = \langle P_ix, y\rangle = 0.$$

Likewise $||P_iy'||^2 = ||P_ix||^2 + ||P_iy||^2$. Hence, either $\mathcal{A}_\Phi$ is not injective or $x' = \pm y'$. However, if $x' = \pm y'$ then either $x = 0$ or $y = 0$ which is not the case. Thus $\mathcal{A}_\Phi$ is not injective.

Proof of Proposition 2 continued.
Conversely, suppose that $\mathcal{A}_\Phi$ is an immersion and suppose that there exist x and y such that $||P_i x|| = ||P_i y||$ for all i. We wish to show that $x = \pm y$. Suppose that $x \neq y$. Then $x - y \neq 0$.
Thus the linear transformation

$$(d\mathcal{A}_\Phi)_{x-y} \colon \mathbb{R}^M \to \mathbb{R}^N,\ z \mapsto (\langle P_i(x-y), z\rangle)_{i=1}^M$$

is injective.
On the other hand

$$\langle P_i(x-y), x+y\rangle = \langle P_i x, x\rangle - \langle P_i y, y\rangle = ||P_i x||^2 - ||P_i y||^2 = 0.$$

(Here we again use the fact that P_i is an orthogonal projection so $\langle P_i x, x\rangle = \langle P_i x, P_i x\rangle$). Hence $x + y = 0$, ie $x = -y$.

The case of few measurments.

By Theorem 1 the map $\mathcal{A}_\Phi$ is not injective if and only there is a pair $(x, y) \in \mathbb{P}_{\mathbb{R}}^{M-1} \times \mathbb{P}_{\mathbb{R}}^{M-1}$ such that $y^t P_i x = 0$ for all i.

Observation. The equation $y^t P_i x = 0$ is bihomegenous of degree 1 in x and y, so we can consider the subvariety $Z \subset \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ defined by the vanishing of the $2M - 2$ bilinear forms $\{y^T P_i x\}_{i=1}^{2M-2}$. Complete phase retrieval is impossible if and only if this variety has a real point .

Problem. Are there bounds L which only depend on the M and the ranks of the P_i which guarantee that Z has a real point when $N < L$?

Example. (another proof of the BCE06 Theorem) If P has rank one then the quadratic equation $y^T P x = 0$ factors a product of two linear forms. Thus, when all P_i have rank one solving the system $\{y^T P_i x = 0\}_{i=1}^N$ is equivalent to solving any one of 2^N linear systems. If $N < 2M - 1$ at least one of these systems has a solutions, so the variety Z has lots of real points.

Example (sketch of the proof the 2nd statement in Theorem 2). If $N = 2M - 2$ then we expect the variety Z to have complex dimension 0. The intersection cycle in $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ determined by Z has degree $\binom{2M-2}{M-1}$. If $N = 2^k + 1$ then this binomial is divisible by 2 but not 4. On the other hand the involution $(x, y) \mapsto (y, x)$ acts on Z and hence on this cycle. Since we can easily show that Z contains no points of the diagonal we can conclude that the intersection cycle contains a real point. (If not, then our cycle would have to have degree divisible by 4 since the complex conjugation involution also acts freely on the intersection cycle.)

THANK YOU