Generic Results in Phaseless Reconstruction

Dongmian Zou

February 26, 2015
Outline

1. Motivation
2. Problem setting
3. Injectivity results
4. 4n-4 Conjecture
Analysis of speech
- Speech signal enhancement
- Speech recognition

Let \( \{x(t), t = 1, 2, \cdots, T\} \) be the samples of a speech signal. The samples are transformed into the time-frequency domain by

\[
X(k, \omega) = \sum_{t=0}^{M-1} g(t) x(t + kN) e^{-2\pi i \omega t / M}, \quad k = 0, 1, \cdots, \frac{T - M}{N}
\]

In most algorithms, we only use the modulus of the transformed signal \( |X(k, \omega)| \). If we do not use the phase, can we reconstruct the signal?
In X-ray crystallography, the diffraction data contains only the amplitude of the transformed electron density. To determine the structure of the crystal, it is important to retrieve the phase information.

**Figure : X-ray Crystallography**
Problem setting
Phase retrieval

- $\mathcal{H}$: Hilbert space with inner product $\langle \cdot , \cdot \rangle$
- $\mathcal{F}$: $\mathcal{F} = \{ f_i : i \in \mathcal{I} \}$ is a frame in $\mathcal{H}$

**Definition**

$\mathcal{F} = \{ f_i : i \in \mathcal{I} \}$ is a frame in $\mathcal{H}$ if there exist two constants $A, B > 0$ such that for every $x \in \mathcal{H}$,

$$ A \|x\|^2 \leq \sum_{i \in \mathcal{I}} |\langle x, f_i \rangle|^2 \leq B \|x\|^2 $$
Problem setting
Phase retrieval

- $\hat{\mathcal{H}} = \mathcal{H} / \sim$
  - $x \sim y$ if and only if there is a scalar $|c| = 1$ such that $y = cx$
- Consider the nonlinear map

$$\alpha : \hat{\mathcal{H}} \to l^2(I), \quad \alpha(\hat{x}) = \{ |\langle x, f_i \rangle| \}_{i \in I}, \quad x \in \hat{x}$$

**Definition**

$\mathcal{F}$ is **phase retrievable** if the map $\alpha$ is injective.
Problem setting

Questions of interest

- When is a frame phase retrievable?
- Is phaseless reconstruction stable under small perturbation?
- Is there an algorithm for phase retrieval with good performance?

Today we introduce some results on the first question.
Problem setting

Questions of interest

- When is a frame phase retrievable?
- Is phaseless reconstruction stable under small perturbation?
- Is there an algorithm for phase retrieval with good performance?

Today we introduce some results on the first question.
Problem setting  
Finite dimensional case  

Case to consider: \( \mathcal{H} \) is finite dimensional  
- In this case, \( F \) is a frame for \( \mathcal{H} \) if and only if \( F \) spans \( \mathcal{H} \)  

Suppose \( F = \{f_1, \cdots, f_m\} \) for some \( m \in \mathbb{Z} \), the map we consider reads  
\[
\alpha : \hat{\mathcal{H}} \rightarrow \mathbb{R}^m, \quad \alpha(\hat{x}) = \{|| \langle x, f_i \rangle ||\}_{i=1}^m, \quad x \in \hat{x}
\]
Problem setting
Finite dimensional case

In some cases, it is useful to look at the map that is the square of $\alpha$, explicitly,

$$
\beta : \hat{\mathcal{H}} \rightarrow \mathbb{R}^m, \quad \beta(\hat{x}) = \{|\langle x, f_i \rangle|^2\}_{i=1}^m, \quad x \in \hat{x}
$$

where in the case that $\mathcal{H} = \mathbb{R}^n$ or $\mathbb{C}^n$,

$$
|\langle x, f_i \rangle|^2 = f_i^*xx^*f_i = \text{tr}(f_i f_i^* xx^*)
$$

In this case the map $\alpha$ induces a linear map $A$ from $\text{Sym}(\mathcal{H}) = \{T : \mathcal{H} \rightarrow \mathcal{H}, \quad T = T^*\}$ to $\mathbb{R}^m$:

$$
A : \text{Sym}(\mathcal{H}) \rightarrow \mathbb{R}^m, \quad A(T) = (\langle Tf_i, f_i \rangle)_{i=1}^m
$$
Outline

1. Motivation
2. Problem setting
3. Injectivity results
4. 4n-4 Conjecture
Injectivity results

Real case

\( \mathcal{H} = \mathbb{R}^n \)

**Theorem (R. Balan, P. Casazza, D. Edidin, 2005)**

*For \( \mathcal{H} = \mathbb{R}^n \), the nonlinear map \( \alpha \) is injective if and only if for any disjoint partition \( \mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \), either \( \mathcal{F}_1 \) spans \( \mathcal{H} \) or \( \mathcal{F}_2 \) spans \( \mathcal{H} \)*

**Theorem (R. Balan, P. Casazza, D. Edidin, 2005)**

1. If \( \alpha \) is injective, then \( m \geq 2n - 1 \);
2. If \( m \leq 2n - 2 \) then \( \alpha \) is not injective;
3. If \( m = 2n - 1 \) then \( \alpha \) is injective if and only if \( \mathcal{F} \) is full spark (any subset of \( n \) elements is linearly independent);
4. If \( m \geq 2n - 1 \) and \( \mathcal{F} \) is full spark then \( \alpha \) is injective.
Injectivity results
Complex case

\[ \mathcal{H} = \mathbb{C}^n \]

**Theorem (B. G. Bodmann, 2007)**

∀ \( n \in \mathbb{N} \), there is a frame of \( m = 4n - 4 \) elements such that \( \alpha \) is injective;

**Theorem (T. Heinosaari, L. Mazzarella, M. Wolf, 2013)**

If \( \alpha \) is injective then

\[
m \geq 4n - 2 - 2\beta + \begin{cases} 
2, & \text{if } n \text{ odd and } \beta = 3 \mod 4 \\
1, & \text{if } n \text{ odd and } \beta = 2 \mod 4 \\
0, & \text{elsewhere}
\end{cases}
\]

where \( \beta \) is the number of 1’s in the binary expansion of \( n - 1 \).
Injectivity results

Complex case

Conjecture

If $\alpha$ is injective, then $m \geq 4n - 4$. 

Dongmian Zou

Generic Results in Phaseless Reconstruction

February 26, 2015
Definition
Let $\mathbb{K}$ be a field. A set $X \subset \mathbb{K}^n$ is called an **algebraic variety** if there are polynomials $p_1, \cdots, p_m$ such that

\[ X = \{ x \in \mathbb{K}^n : p_1(x) = \cdots = p_m(x) = 0 \}. \]

Definition
The **Zarisky topology** is the induced topology in which algebraic varieties are closed.

Definition
We say that a **generic** point of $\mathbb{K}^d$ for a field $\mathbb{K}$ has a certain property if there is a non-empty Zarisky open set of points with that property.
Injectivity results

For $\mathcal{H} = \mathbb{K}^n$, a frame $\mathcal{F} = \{f_1, \cdots, f_m\}$ can be identified as an $n$-by-$m$ matrix $[f_1, \cdots, f_m]$ of full rank. Let $\mathcal{F}(n, m)$ denote the set of all such matrices.

$\mathcal{F}(n, m)$ is a Zarisky open set in $\mathbb{K}^{n \times m}$.

A nonempty Zarisky open set is open and dense in Euclidean topology. Therefore, a generic frame being phase retrievable implies that with probability 1, a randomly chosen frame will be phase retrievable.
Injectivity results
Generic results

Theorem (R. Balan, P. Casazza, D. Edidin, 2005)

For $\mathcal{H} = \mathbb{R}^n$, if $m \geq 2n - 1$, then a generic frame $\mathcal{F}$ is phase retrievable.

What about the complex case? That is the ”4n-4 conjecture”.
Outline

1 Motivation

2 Problem setting

3 Injectivity results

4 4n-4 Conjecture
**Conjecture**

*For $\mathcal{H} = \mathbb{C}^n$,*

(a) If $m < 4n - 4$, then $\alpha$ cannot be injective.

(b) If $m \geq 4n - 4$, then $\alpha$ is injective for generic $F$.

In *An Algebraic Characterization of Injectivity in Phase Retrieval* by A. Conca, D. Edidin, M. Hering, C. Vinzant, the authors proved (b) and a special case of (a).
From now on, we fix $\mathcal{H} = \mathbb{C}^n$.
The following lemma is used to translate the injectivity problem into a question in algebraic geometry.

**Lemma (A. Bandeira, J. Cahill, D. Mixon, A. Nelson, 2013)**

The map $\alpha$ is not injective if and only if there is a nonzero Hermitian matrix $Q \in \mathbb{C}^{n \times n}$ for which

$$
\text{rank}(Q) \leq 2 \quad \text{and} \quad f_k^* Q f_k = 0, \quad \forall \ 1 \leq k \leq m
$$
Lemma (A. Bandeira, J. Cahill, D. Mixon, A. Nelson, 2013)

The map $\alpha$ is not injective if and only if there is a nonzero Hermitian matrix $Q \in \mathbb{C}^{n \times n}$ for which

$$\text{rank}(Q) \leq 2 \quad \text{and} \quad f_k^* Q f_k = 0, \quad \forall \ 1 \leq k \leq m$$

Proof.

($\Rightarrow$) Suppose $\alpha(x) = \alpha(y)$ with $\hat{x} \neq \hat{y}$, take

$$Q = xx^* - yy^*$$

Then $\forall \ 1 \leq k \leq m$, we have $f_k^* Q f_k = (\alpha(x) - \alpha(y))_k = 0$. 
Lemma (A. Bandeira, J. Cahill, D. Mixon, A. Nelson, 2013)

The map $\alpha$ is not injective if and only if there is a nonzero Hermitian matrix $Q \in \mathbb{C}^{n \times n}$ for which

$$\text{rank}(Q) \leq 2 \quad \text{and} \quad f_k^* Q f_k = 0, \forall 1 \leq k \leq m$$

Proof (Cont’d).

$(\Leftarrow)$ (Q rank 1) $Q = xx^*$ for some $x \neq 0$. $\alpha(x) = \alpha(0) = 0$.

(Q rank 2) $Q = \lambda_1 xx^* + \lambda_2 yy^*$ where $\lambda_1, \lambda_2 \in \mathbb{R} \setminus \{0\}$. Then

$$0 = f_k^* Q f_k = \lambda_1 (\alpha(x))_k + \lambda_2 (\alpha(y))_k$$

Take $x' = |\lambda_1|^{1/2} x$, $y' = |\lambda_2|^{1/2} y$. $\alpha(x') - \alpha(y') = 0$. \qed
Definition

Let $B_{n,m}$ denote the subset (and in fact a subvariety) of
\[ \mathbb{P}(\mathbb{C}^{n \times m} \times \mathbb{C}^{n \times m}) \times \mathbb{P}\left( \mathbb{C}_{\text{sym}}^{n \times n} \times \mathbb{C}_{\text{skew}}^{n \times n} \right) \]
consisting of quadruples of matrices $([U, V], [X, Y])$ for which

\[ \text{rank}(X + iY) \leq 2 \]

and

\[ u_k^T X u_k + v_k^T X v_k - 2u_k^T Y v_k = 0 \quad \forall \ 1 \leq k \leq m \]

where $u_k$ and $v_k$ are the $k$-th column of $U$ and $V$, respectively.
Let $\mathcal{F} = \{f_k\}_{k=1}^m \subset \mathbb{C}^m$ be a complex frame. Write $f_k = u_k + iv_k$. Let $U$ (resp. $V$) be the real matrix with columns $u_k$ (resp. $v_k$). Then the map $\alpha$ is injective if and only if $[U, V]$ does not belong to the projection $\pi_1((\mathcal{B}_{n,m})_\mathbb{R})$.

This is based on the above lemma and the relation

$$(u_k + iv_k)^*(X + iY)(u_k + iv_k) = u_k^T X u_k + v_k^T X v_k - 2u_k^T Y v_k$$
By Proposition (♠), all "bad frames" are contained in $\pi_1((B_{n,m})_\mathbb{R})$. We want to prove that the set $\pi_1((B_{n,m})_\mathbb{R})$ is small. We want to bound the dimension of $\pi_1(B_{n,m})$. The following theorem gives the dimension of $B_{n,m}$ itself.

**Theorem**

*The projective complex variety $B_{n,m}$ has dimension $2nm + 4n - m - 6$.***
4n-4 Conjecture

Proof.

STEP 1: Define $\mathcal{B}_{n,m}'$ with the same dimension as $\mathcal{B}_{n,m}$.

Definition

Let $\mathcal{B}_{n,m}'$ denote the subvariety of $\mathbb{P} (\mathbb{C}^{n \times m} \times \mathbb{C}^{n \times m}) \times \mathbb{P} (\mathbb{C}^{n \times n})$ consisting of triples of matrices $([U, V], [Q])$ for which

$$\text{rank}(Q) \leq 2 \quad \text{and} \quad (u_k + iv_k)^* Q(u_k + iv_k) = 0 \quad \forall \ 1 \leq k \leq m$$

$\mathcal{B}_{n,m}$ and $\mathcal{B}_{n,m}'$ are linearly isomorphic. In fact, we can identify $\mathbb{C}^{n \times n}_\text{sym} \times \mathbb{C}^{n \times n}_\text{skew}$ with $\mathbb{C}^{n \times n}$ by the map

$$(X, Y) \mapsto Q = X + iY$$
On the other hand, any complex matrix $Q$ can be uniquely written as $Q = X + iY$ where $X \in \mathbb{C}^{n \times n}_{\text{sym}}$ and $Y \in \mathbb{C}^{n \times n}_{\text{skew}}$. Explicitly, that is given by

$$X = \frac{Q + Q^T}{2}, \quad Y = \frac{Q - Q^T}{2i}$$

Hence it suffices to prove that $\mathcal{B}_{n,m}'$ has dimension $2nm - m + 4n - 6$. We determine the dimension of $\mathcal{B}_{n,m}'$ by finding the dimension of $\pi_2(\mathcal{B}_{n,m}')$ and $\pi_2^{-1}(Q)$ for $Q \in \mathbb{C}^{n \times n}$. 
Proof (Cont’d).

STEP 2: Find the dimension of $\pi_2(B'_{n,m})$.

Claim: $\pi_2(B'_{n,m}) = \{ Q \in \mathbb{P}(\mathbb{C}^{n\times n}) : \text{rank}(Q) \leq 2 \}$.

Proof: It suffices to show "⊃":
Take any $(u, v) \in \mathbb{C}^n \times \mathbb{C}^n$ for which

$$(u - iv)^T Q(u + iv) = 0$$

Let $U, V$ be matrices with columns $u_k = u, v_k = v$ for $1 \leq k \leq m$. Then $([U, V], [Q]) \in B'_{n,m}$ and $Q \in \pi_2(B'_{n,m})$. 
Proof (Cont’d).

Proposition (J. Harris, Proposition 12.2)

The variety $M_k \subset M$ of $m \times n$ matrices of rank $\leq k$ is irreducible of codimension $(m - k)(n - k)$ in $M$.

In our case, the set of matrices of rank at most 2 in $\mathbb{C}^{n \times n}$ has codimension $(n - 2)^2$, and thus dimension $n^2 - (n - 2)^2 = 4n - 4$. Therefore, its projectivization in $\mathbb{P}(\mathbb{C}^{n \times n})$ have dimension $4n - 5$. 
Proof (Cont’d).

STEP 3: Fix $Q$ in $\pi_2(B'_{n,m})$. Find the dimension of $\pi_2^{-1}(Q)$.

**Lemma**

For a nonzero matrix $Q = (q_{lk}) \in \mathbb{C}^{n \times n}$, the polynomial

$$q(u, v) = (u - iv)^T Q(u + iv) \in \mathbb{C}[u_1, \cdots, u_n, v_1, \cdots, v_n]$$

where $u = (u_1, \cdots, u_n)^T$, and $v = (v_1, \cdots, v_n)^T$, is not identically zero.
Proof of Lemma.

\[ q(u, v) = \sum_{1 \leq k \leq n} q_{kk}(u_k^2 + v_k^2) + \]
\[ \sum_{1 \leq l \leq k \leq n} (q_{lk} + q_{kl})(u_l u_k + v_l v_k) + i(q_{lk} - q_{kl})(u_l v_k - v_l u_k) \]

If \( q(u, v) \) is identically zero, we would have

\[ q_{kk} = 0 \quad \forall \ 1 \leq k \leq n \]
\[ q_{lk} + q_{kl} = 0 \quad \forall \ 1 \leq l \leq k \leq n \]
\[ q_{lk} - q_{kl} = 0 \quad \forall \ 1 \leq l \leq k \leq n \]

It follows that \( Q \) is the zero matrix.
By the lemma above, $Q$ defines a nonzero equation

$$(u_k - iv_k)^T Q(u_k + iv_k) = 0$$

For each pair of columns $(u_k, v_k)$, this defines a hypersurface of dimension $2n - 1$ in $(\mathbb{C}^n)^2$.

Thus $\pi^{-1}_2(Q)$ is a product of $m$ copies of this hypersurface in $((\mathbb{C}^n)^2)^m$ and thus is of dimension $m(2n - 1)$.

After projectivization, $\pi^{-1}_2(Q)$ has dimension $m(2n - 1) - 1$. 

Proof (Cont’d).

STEP 4: Put together.

Following (J. Harris, Proposition 11.13), the dimension of the projective variety $B'_{n,m}$ is the sum of the dimension of $\pi_2(B'_{n,m})$ and the dimension of $\pi_2^{-1}(Q)$.

Therefore,

$$\dim(B'_{n,m}) = 4n - 5 + m(2n - 1) - 1 = 2nm + 4n - m - 6$$
Theorem (4n-4 Conjecture (b))

If \( m \geq 4n - 4 \), then \( \alpha \) is injective for a generic frame \( \mathcal{F} \).

Proof.

\[
\dim(\pi_1(\mathcal{B}_{n,m})) \leq \dim(\mathcal{B}_{n,m}) = 2nm + 4n - m - 6
\]

When \( m \geq 4n - 4 \),
\[
2nm + 4n - m - 6 \leq (2n - 1)(4n - 4) + 4n - 6 = 8n^2 - 12n - 10 < 8n^2 - 8n - 4 = 2nm - 1.
\]

The dimension of \( \mathbb{P}((\mathbb{C}^{n \times m})^2) \) is \( 2nm - 1 \). Thus \( \pi_1(\mathcal{B}_{n,m}) \) is contained in some hypersurface defined by the vanishing of some polynomial

\[
p_{m,n} = p_{m,n}^{\text{real}} + i \cdot p_{m,n}^{\text{imag}}.
\]

Consider now \( \pi_1((\mathcal{B}_{n,m})_R) \). It is contained in the hypersurface defined by the vanishing of \( p_{m,n}^{\text{real}} \) or \( p_{m,n}^{\text{imag}} \), whichever is non-zero.
Example: $n = 2, m = 4.$

$$U = (u_{jk}), \ V = (v_{jk}), \ Q = \begin{pmatrix} x_{11} & x_{12} + iy_{12} \\ x_{12} - iy_{12} & y_{11} \end{pmatrix}$$

$B_{2,4}$ is defined by $g_k = 0, k = 1, \ldots, 4,$ where

$$g_k = (u_{1k}^2 + v_{1k}^2)x_{11} + 2(u_{1k}u_{2k} + v_{1k}v_{2k})x_{12} + (u_{2k}^2 + v_{2k}^2)x_{22} + 2(u_{2k}v_{1k} - u_{1k}v_{2k})y_{12}$$
Example: $n = 2, m = 4$.

$\pi_1(B_{2,4})$ is determined by the hypersurface

\[
\begin{vmatrix}
  u_{11}^2 + v_{11}^2 & 2(u_{11}u_{21} + v_{11}v_{21}) & u_{21}^2 + v_{21}^2 & 2(u_{21}v_{11} - u_{11}v_{21}) \\
  u_{12}^2 + v_{12}^2 & 2(u_{12}u_{22} + v_{12}v_{22}) & u_{22}^2 + v_{22}^2 & 2(u_{22}v_{12} - u_{12}v_{22}) \\
  u_{13}^2 + v_{13}^2 & 2(u_{13}u_{23} + v_{13}v_{23}) & u_{23}^2 + v_{23}^2 & 2(u_{23}v_{13} - u_{13}v_{23}) \\
  u_{14}^2 + v_{14}^2 & 2(u_{14}u_{24} + v_{14}v_{24}) & u_{24}^2 + v_{24}^2 & 2(u_{24}v_{14} - u_{14}v_{24}) \\
\end{vmatrix} = 0
\]
What about Part(a) of the "4n-4 Conjecture"?

**Conjecture**

For $\mathcal{H} = \mathbb{C}^n$,

(a) If $m < 4n - 4$, then $\alpha$ cannot be injective.
(b) If $m \geq 4n - 4$, then $\alpha$ is injective for generic $\mathcal{F}$.

It is proved for some special values of $n$, Part(a) is true.
Proposition (❤)

If $m \leq 4n - 5$, then for every $[U, V] \in \mathbb{P}(\mathbb{C}^{n \times m})^2$, the preimage under the first projection $\pi_1^{-1}([U, V])$ is a non-empty variety of degree

$$d_{n,2} = \prod_{j=0}^{n-3} \frac{(n+j)}{\left(\frac{2+j}{2}\right)}$$

In particular, the projection $\pi_1(\mathcal{B}_{n,m})$ is all of $\mathbb{P}((\mathbb{C}^{n \times m})^2)$. 
Proof.

Let

\[ L_F = \{ Q \in \mathbb{P}(\mathbb{C}^{n \times n}) : (u_k - i v_k)^T Q (u_k + i v_k) = 0 \quad \forall \ 1 \leq k \leq m \} \]

\[ H_2 = \{ Q \in \mathbb{P}(\mathbb{C}^{n \times n}) : \text{rank}(Q) \leq 2 \} \]

We have \( \dim(L_F) \geq n^2 - 1 - m \). \( \dim(H_2) = 4n - 5 \).

When \( m \leq 4n - 5 \) we have \( \dim(L_F) + \dim(H_2) \geq n^2 - 1 \). Therefore there is a point in the intersection \( L_F \cap H_2 \). By (J. Harris, Example 19.10), we have the degree of \( H_2 = d_{n,2} \). Therefore, the degree of \( L_F \cap H_2 \) is also \( d_{n,2} \) given above.
Using Proposition (♠), we can restate the 4n-4 Conjecture (a) as follows:

**Conjecture (4n-4 Conjecture (a))**

If \( m \leq 4n - 5 \), then \( \pi_1((B_{n,m})_\mathbb{R}) = \mathbb{P}((\mathbb{R}^{n \times m})^2) \).

If we could show \( (\pi_1(B_{n,m}))_\mathbb{R} \subset \pi_1((B_{n,m})_\mathbb{R}) \), then by Proposition (♡) we would get the conjecture.

Unfortunately it is not an easy task.

In the paper the authors prove the case for \( n = 2^l + 1 \).
Lemma

When $n = 2^l + 1$, $d_{n,2}$ is odd.

Proof.

Legendre’s formula: Let $s_p(m)$ denote the sum of the digits in the base $p$ expansion of $m$. The highest power of a prime $p$ dividing $m!$ is given by

$$\nu_p(m!) = \frac{m - s_p(m)}{p - 1}$$

Recall that

$$d_{n,2} = \prod_{j=0}^{n-3} \frac{(n+j)}{2} \frac{2}{(2+j)}$$
Proof (Cont’d).

The highest power of 2 dividing $d_{n,2}$ is thus

$$\left(\sum_{j=0}^{n-3} s_2(n+j-2) - s_2(n+j)\right) - \left(\sum_{j=0}^{n-3} s_2(j) - s_2(j+2)\right)$$

For $n = 2^l + 1$ we have for $0 \leq m \leq n - 2$ that $s_2(n - 1 + m) = s_2(m) + 1$. Thus (43) simplifies to

$$s_2(n - 2) - s_2(n) - s_2(n - 3) + s_2(m - 1)$$

$$= l - 2 - (l - 1) + 1 = 0$$
Theorem

If \( n \leq 4m - 5 \) and \( n = 2^l + 1 \), then \( \alpha \) is not injective.

Proof.

It follows from the above lemma and the fact that any projective variety defined over \( \mathbb{R} \) with odd degree has real point. Now for \([U, V]\) real, \( \pi_1^{-1}([U, V]) \) contains a real point. Therefore \( \pi_1((\mathcal{B}_{n,m})_\mathbb{R}) = \mathbb{P}((\mathbb{R}^{n \times m})^2) \)
What about for a general $n$? It is false!
Recently, in *A Small Frame and a Certificate of its Injectivity*, C. Vinzant proved that for the case $n = 4$ and $m = 11$, the conjecture is false. The author found a polynomial that contains all the "non-injectivity" points.
Thank you!
References


