

# Statistical Estimation in the Presence of Group Actions

Alex Wein  
MIT Mathematics

# In memoriam

Amelia Perry  
1991 – 2018



## My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)

## My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)
  - | Community detection (stochastic block model)
  - | Spiked matrix/tensor problems
  - | Synchronization / group actions (today)

## My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)
  - | Community detection (stochastic block model)
  - | Spiked matrix/tensor problems
  - | Synchronization / group actions (today)
- | Connections to...

## My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)
  - | Community detection (stochastic block model)
  - | Spiked matrix/tensor problems
  - | Synchronization / group actions (today)
- | Connections to...
  - | Statistical physics
    - | Phase transitions: easy, hard, impossible

## My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)
  - | Community detection (stochastic block model)
  - | Spiked matrix/tensor problems
  - | Synchronization / group actions (today)
- | Connections to...
  - | Statistical physics
    - | Phase transitions: easy, hard, impossible
  - | Algebra
    - | Group theory, representation theory, invariant theory

# My research interests

- | Statistical and computational limits of average-case inference problems (signal planted in random noise)
  - | Community detection (stochastic block model)
  - | Spiked matrix/tensor problems
  - | Synchronization / group actions (today)
- | Connections to...
  - | Statistical physics
    - | Phase transitions: easy, hard, impossible
  - | Algebra
    - | Group theory, representation theory, invariant theory
- | Today: problems involving group actions
  - | A meeting point of statistics, algebra, signal processing computer science, statistical physics, ...



# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

- | Biological imaging method: determine structure of molecule

# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

- | Biological imaging method: determine structure of molecule
- | 2017 Nobel Prize in Chemistry

# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

- | Biological imaging method: determine structure of molecule
- | 2017 Nobel Prize in Chemistry
- | Given many noisy 2D images of a 3D molecule, taken from different unknown angles

# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

- | Biological imaging method: determine structure of molecule
- | 2017 Nobel Prize in Chemistry
- | Given many noisy 2D images of a 3D molecule, taken from different unknown angles
- | Goal is to reconstruct the 3D structure of the molecule

# Motivation: cryo-electron microscopy (cryo-EM)

Image credit: [Singer, Shkolnisky '11]

- | Biological imaging method: determine structure of molecule
- | 2017 Nobel Prize in Chemistry
- | Given many noisy 2D images of a 3D molecule, taken from different unknown angles
- | Goal is to reconstruct the 3D structure of the molecule
- | Group action by  $SO(3)$  (rotations in 3D)

## Other examples

Other problems involving random group actions:

## Other examples

Other problems involving random group actions:

- | Image registration

Image credit: [Bandeira, PhD thesis '15]

Group:  $SO(2)$  (2D rotations)



## Other examples

Other problems involving random group actions:

| Image registration

| Multi-reference alignment

Image credit: [Bandeira, PhD thesis '15]

Group:  $SO(2)$  (2D rotations)

Image credit: Jonathan Weed

Group:  $\mathbb{Z}=p$  (cyclic shifts)

## Other examples

Other problems involving random group actions:

- | Image registration
- | Multi-reference alignment

Image credit: [Bandeira, PhD thesis '15]

Image credit: Jonathan Weed

Group:  $SO(2)$  (2D rotations)

Group:  $\mathbb{Z}=p$  (cyclic shifts)

- | Applications: computer vision, radar, structural biology, robotics, geology, paleontology, ...

## Other examples

Other problems involving random group actions:

- | Image registration
- | Multi-reference alignment

Image credit: [Bandeira, PhD thesis '15]

Image credit: Jonathan Weed

Group:  $SO(2)$  (2D rotations)

Group:  $\mathbb{Z}=p$  (cyclic shifts)

- | Applications: computer vision, radar, structural biology, robotics, geology, paleontology, ...
- | Methods used in practice often lack provable guarantees...

## Part I: Synchronization

# Synchronization problems

The **synchronization** approach [1]: learn the group elements

---

[1] Singer '11

[2] Singer, Shkolnisky '11

# Synchronization problems

The **synchronization** approach [1]: learn the group elements

- | Fix a group  $G$ 
  - | e.g.  $SO(3)$

---

[1] Singer '11

[2] Singer, Shkolnisky '11

# Synchronization problems

The **synchronization** approach [1]: learn the group elements

- | Fix a group  $G$ 
  - | e.g.  $SO(3)$
- |  $g \in G^n$  – vector of unknown group elements
  - | e.g. rotation of each image

---

[1] Singer '11

[2] Singer, Shkolnisky '11

# Synchronization problems

The **synchronization** approach<sup>[1]</sup>: learn the group elements

- | Fix a group  $G$ 
  - | e.g.  $SO(3)$
- |  $g \in G^n$  { vector of unknown group elements
  - | e.g. rotation of each image
- | Given pairwise information: for each  $i < j$ , a noisy measurement of  $g_i g_j^{-1}$ 
  - | e.g. by comparing two images

---

[1] Singer '11

[2] Singer, Shkolnisky '11



# Synchronization problems

The **synchronization** approach<sup>[1]</sup>: learn the group elements

- | Fix a group  $G$ 
  - | e.g.  $SO(3)$
- |  $g \in G^n$  { vector of unknown group elements
  - | e.g. rotation of each image
- | Given pairwise information: for each  $i < j$ , a noisy measurement of  $g_i g_j^{-1}$ 
  - | e.g. by comparing two images
- | Goal: recover  $g$  up to global right-multiplication
  - | can't distinguish  $(g_1; \dots; g_n)$  from  $(g_1 h; \dots; g_n h)$

---

[1] Singer '11

[2] Singer, Shkolnisky '11

# Synchronization problems

The **synchronization** approach<sup>[1]</sup>: learn the group elements

- | Fix a group  $G$ 
  - | e.g.  $SO(3)$
- |  $g \in G^n$  { vector of unknown group elements
  - | e.g. rotation of each image
- | Given pairwise information: for each  $i < j$ , a noisy measurement of  $g_i g_j^{-1}$ 
  - | e.g. by comparing two images
- | Goal: recover  $g$  up to global right-multiplication
  - | can't distinguish  $(g_1; \dots; g_n)$  from  $(g_1 h; \dots; g_n h)$

In cryo-EM: once you learn the rotations, it is possible to reconstruct a de-noised model of the molecule<sup>[2]</sup>

---

[1] Singer '11

[2] Singer, Shkolnisky '11

## A simple model: Gaussian synchronization

$$G = Z = f \quad 1g$$

## A simple model: Gaussian $\mathbb{Z}_2$ synchronization

- |  $G = \mathbb{Z}_2 = \{1, g\}$
- | True signal  $x = (x_1, \dots, x_n)$  (vector of group elements)

## A simple model: Gaussian synchronization

- |  $G = \mathbb{Z}_2 = \{1, g\}$
- | True signal  $x = \sum_{n=1}^N g^n$  (vector of group elements)
- | For each  $i, j$  observe  $x_i x_j + N(0, \sigma^2)$

## A simple model: Gaussian synchronization

- |  $G = Z = \mathbb{Z}_2 = \{1, g\}$
- | True signal  $x \in \mathbb{Z}_2^n$  (vector of group elements)
- | For each  $i, j$  observe  $x_i x_j + N(0, \sigma^2)$
- | Specifically, observed  $n \times n$  matrix  $Y = \underbrace{-xx^T}_{\text{signal}} + \underbrace{\frac{1}{\rho} W}_{\text{noise}}$
- |  $\rho > 0$  { signal-to-noise parameter}
- |  $W$  { random noise matrix: symmetric with entries  $N(0, 1)$ }

## A simple model: Gaussian synchronization

- |  $G = Z = \{g^k\}_{k=0}^{n-1}$
- | True signal  $x = (x_0, \dots, x_{n-1})^T$  (vector of group elements)
- | For each  $i, j$  observe  $y_{ij} = x_i x_j + N(0, \sigma^2)$
- | Specifically, observe  $n \times n$  matrix  $Y = \underbrace{-xx^T}_{\text{signal}} + \underbrace{\frac{1}{\rho} W}_{\text{noise}}$
- |  $\rho > 0$  { signal-to-noise parameter}
- |  $W$  { random noise matrix: symmetric with entries  $N(0, 1)$ }
- |  $Y_{ij}$  is a noisy measurement of  $x_i x_j$  (same/diff)

## A simple model: Gaussian synchronization

- |  $G = Z = f \cdot 1g$
- | True signal  $x \in \mathbb{R}^n$  (vector of group elements)
- | For each  $i, j$  observe  $x_i x_j + N(0; \sigma^2)$
- | Specifically, observe  $n \times n$  matrix  $Y = \underbrace{-xx^T}_{\text{signal}} + \underbrace{\frac{1}{\rho} W}_{\text{noise}}$
- |  $\rho$  { signal-to-noise parameter
- |  $W$  { random noise matrix: symmetric with entries  $N(0; 1)$
- |  $Y_{ij}$  is a noisy measurement of  $x_i x_j$  (same/diff)
- | Normalization: MMSE is a constant (depending on)



## A simple model: Gaussian synchronization

- |  $G = Z = 2 = f \quad 1g$
- | True signal  $x \in \mathbb{R}^n$  (vector of group elements)
- | For each  $i, j$  observe  $x_i x_j + N(0; \sigma^2)$
- | Specifically, observed  $n \times n$  matrix  $Y = \frac{1}{\rho} \underbrace{xx^T}_{\text{signal}} + \underbrace{W}_{\text{noise}}$
- |  $\rho$  { signal-to-noise parameter
- |  $W$  { random noise matrix: symmetric with entries  $N(0; 1)$
- |  $Y_{ij}$  is a noisy measurement of  $x_i x_j$  (same/di)
- | Normalization: MMSE is a constant (depending on)

This is a **spiked Wigner model**: in general  $P$  (some prior)

## A simple model: Gaussian synchronization

- |  $G = Z = f \cdot 1g$
- | True signal  $x \in \mathbb{R}^n$  (vector of group elements)
- | For each  $i, j$  observe  $x_i x_j + N(0; \sigma^2)$
- | Specifically, observe  $n \times n$  matrix  $Y = \underbrace{-xx^T}_{\text{signal}} + \underbrace{\frac{1}{\rho} W}_{\text{noise}}$
- |  $\rho$  { signal-to-noise parameter
- |  $W$  { random noise matrix: symmetric with entries  $N(0; 1)$
- |  $Y_{ij}$  is a noisy measurement of  $x_i x_j$  (same/diff)
- | Normalization: MMSE is a constant (depending on)

This is a **spiked Wigner model**: in general  $P$  (some prior)

**Statistical physics** makes extremely precise (non-rigorous) predictions about this type of problem

- | Often later proved correct

## A simple model: Gaussian synchronization

- |  $G = Z = 2 = f \quad 1g$
- | True signal  $x \in \mathbb{R}^n$  (vector of group elements)
- | Observed matrix  $Y = \underbrace{-xx^T}_{\text{signal}} + \underbrace{\rho^{-1}W}_{\text{noise}}$

# Statistical physics and inference

What does statistical physics have to do with Bayesian inference?

# Statistical physics and inference

What does statistical physics have to do with Bayesian inference?

In inference, observe  $\mathbf{y} = \frac{1}{n} \mathbf{X} \mathbf{x}^* + \frac{1}{n} \mathbf{W}$  and want to infer  $\mathbf{x}^*$

# Statistical physics and inference

What does statistical physics have to do with Bayesian inference?

In inference, observe  $\mathbf{y} = \frac{1}{n} \sum_{i=1}^n \mathbf{x}_i + \frac{1}{n} \sum_{i=1}^n \mathbf{w}_i$  and want to infer  $\mathbf{x}$

Posterior distribution:  $\Pr[\mathbf{x} | \mathbf{y}] \propto \exp(-\mathbf{x}^T \mathbf{y})$

# Statistical physics and inference

What does statistical physics have to do with Bayesian inference?

In inference, observe  $\mathbf{y} = \frac{1}{n} \sum \mathbf{x} \mathbf{x}^T + \frac{1}{n} \sum W$  and want to infer  $\mathbf{x}$

Posterior distribution:  $\Pr[\mathbf{x} | \mathbf{y}] \propto \exp(-\mathbf{x}^T \mathbf{y})$

In physics, this is called a **Boltzmann/Gibbs** distribution:

$$\Pr[\mathbf{x}] \propto \exp(-\beta H(\mathbf{x}))$$

- | Energy ("Hamiltonian")  $H(\mathbf{x}) = \mathbf{x}^T \mathbf{y} \mathbf{x}$
- | Temperature  $\beta = 1/T$

# Statistical physics and inference

What does statistical physics have to do with Bayesian inference?

In inference, observe  $\mathbf{y} = \frac{1}{n} \sum x_i x_i^T + \frac{1}{n} \sum W$  and want to infer  $x$

Posterior distribution:  $\Pr[x | \mathbf{y}] \propto \exp(-\sum x_i y_i)$

In physics, this is called a **Boltzmann/Gibbs** distribution:

$$\Pr[x] \propto \exp(-\beta H(x))$$

- | Energy ("Hamiltonian")  $H(x) = \sum x_i y_i$
- | Temperature  $\beta = 1/T$

So posterior distribution of Bayesian inference obeys the same equations as a disordered physical system (e.g. magnet, spin glass)



# BP and AMP

"Axiom" from statistical physics: the best algorithm for every\*  
problem is BP (belief propagation)[1]

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)**[1]

- | Each unknown  $x_i$  is a "node"

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)**[1]

- | Each unknown  $x_i$  is a "node"
- | Each observation ("interaction")  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)**[1]

- | Each unknown  $x_i$  is a "node"
- | Each observation (interaction)  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph
- | Nodes iteratively pass "messages" or "beliefs" to each other along edges, and then update their own beliefs

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)**[1]

- | Each unknown  $x_i$  is a "node"
- | Each observation (interaction)  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph
- | Nodes iteratively pass "messages" or "beliefs" to each other along edges, and then update their own beliefs
- | Hard to analyze

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)** [1]

- | Each unknown  $x_i$  is a "node"
- | Each observation (interaction)  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph
- | Nodes iteratively pass "messages" or "beliefs" to each other along edges, and then update their own beliefs
- | Hard to analyze

In our case (since interactions are "dense"), we can use a simplification of BP called **AMP (approximate message passing)** [2]

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)** [1]

- | Each unknown  $x_i$  is a "node"
- | Each observation (interaction)  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph
- | Nodes iteratively pass "messages" or "beliefs" to each other along edges, and then update their own beliefs
- | Hard to analyze

In our case (since interactions are "dense"), we can use a simplification of BP called **AMP (approximate message passing)** [2]

- | Easy/possible to analyze

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09

# BP and AMP

"Axiom" from statistical physics: **the best algorithm for every\* problem is BP (belief propagation)** [1]

- | Each unknown  $x_i$  is a "node"
- | Each observation (interaction)  $Y_{ij}$  is an "edge"
  - | In our case, a complete graph
- | Nodes iteratively pass "messages" or "beliefs" to each other along edges, and then update their own beliefs
- | Hard to analyze

In our case (since interactions are "dense"), we can use a simplification of BP called **AMP (approximate message passing)** [2]

- | Easy/possible to analyze
- | Provably optimal mean squared error for many problems

---

[1] Pearl '82

[2] Donoho, Maleki, Montanari '09



## AMP for Z=2 synchronization

$$Y = \frac{1}{n} \sum_{i=1}^n x_i^2 + \frac{1}{n} \sum_{i=1}^n W_i; \quad x \sim \mathcal{N}(0, 1), \quad W \sim \mathcal{N}(0, \sigma^2)$$

## AMP for $Z=2$ synchronization

$$Y = \frac{1}{n} x x^T + \frac{1}{n} W; \quad x \in \mathbb{R}^n \quad 1/n$$

AMP algorithm:

- | State  $v \in \mathbb{R}^n$  { estimate for  $x$

## AMP for $Z=2$ synchronization

$$Y = \frac{1}{n} x x^T + \frac{1}{n} W; \quad x \in \mathbb{R}^n \quad 1 \leq n$$

AMP algorithm:

- | State  $v \in \mathbb{R}^n$  { estimate for  $x$
- | Initialize  $v$  to small random vector

## AMP for $Z=2$ synchronization

$$Y = \frac{1}{n}xx^T + \frac{1}{n}W; \quad x \in \mathbb{R}^n \quad 1g^n$$

AMP algorithm:

- | State  $v \in \mathbb{R}^n$  { estimate for  $x$
- | Initialize  $v$  to small random vector
- | Repeat:
  1. Power iteration:  $v \leftarrow Yv$  (power iteration)

## AMP for $Z=2$ synchronization

$$Y = \frac{1}{n} x x^T + \frac{1}{n} W; \quad x \in \mathbb{R}^n \quad 1 \leq n$$

AMP algorithm:

- | State  $v \in \mathbb{R}^n$  { estimate for  $x$
- | Initialize  $v$  to small random vector
- | Repeat:
  1. Power iteration:  $v \leftarrow Yv$  (power iteration)
  2. Onsager:  $v \leftarrow v + [\text{Onsager term}]$

## AMP for $Z=2$ synchronization

$$Y = \frac{1}{n} x x^T + \frac{1}{n} W; \quad x \in \mathbb{R}^n, \quad 1 \leq i \leq n$$

AMP algorithm:

- | State  $v \in \mathbb{R}^n$  { estimate for  $x$
- | Initialize  $v$  to small random vector
- | Repeat:
  1. Power iteration:  $v \leftarrow Yv$  (power iteration)
  2. Onsager:  $v \leftarrow v + [\text{Onsager term}]$
  3. Entrywise soft projection:  $v_i \leftarrow \tanh(v_i)$  (for all  $i$ )
    - | Resulting values in  $[-1, 1]$

## AMP is optimal

$$Y = \frac{1}{n}xx^T + \rho \frac{1}{n}W; \quad x \in \mathbb{R}^n, \quad \rho \in \mathbb{R}$$

For  $Z=2$  synchronization, AMP is provably optimal.

# Free energy landscapes

What do physics predictions look like?



# Free energy landscapes

What do physics predictions look like?

$$f(\beta) = \frac{1}{N} \left[ \frac{2}{4} \frac{2}{4} + 1 \right] + \frac{1}{2} \left[ \frac{1}{2} + 1 \right] - \frac{1}{N} \sum_{z \in \mathbb{R}} \int_{(0;1)} E \log(2 \cosh(\beta z))$$

# Free energy landscapes

What do physics predictions look like?

$$f(\beta) = \frac{1}{\beta} - \frac{2}{4} \frac{2}{4} + 1 + \frac{1}{2} \frac{1}{2} + 1 \quad \mathbb{E}_{z \sim \mathcal{N}(0;1)} \log(2 \cosh(\beta z))$$

x-axis : correlation with true signal (related to MSE)

y-axis : **free energy** { AMP's "objective function" (minimize)

# Free energy landscapes

What do physics predictions look like?

$$f(\beta) = \frac{1}{N} \ln \int \prod_i d\sigma_i \exp\left(-\beta \sum_{\langle ij \rangle} J_{ij} \sigma_i \sigma_j - \sum_i h_i \sigma_i\right) = \frac{1}{N} \ln \int \prod_i d\sigma_i \exp\left(-\beta \sum_{\langle ij \rangle} J_{ij} \sigma_i \sigma_j - \sum_i h_i \sigma_i\right)$$

x-axis : correlation with true signal (related to MSE)

y-axis : **free energy** { AMP's "objective function" (minimize)

**AMP** { gradient descent starting from  $\beta = 0$  (left side)

**STAT** (statistical) { global minimum

# Free energy landscapes

What do physics predictions look like?

$$f(\rho) = \frac{1}{2} \rho^2 - \frac{\rho^4}{4} + \frac{1}{2} \rho^2 + \frac{1}{2} \rho^2 + 1 \quad \mathbb{E}_{z \sim \mathcal{N}(0;1)} \log(2 \cosh(\rho z))$$

x-axis : correlation with true signal (related to MSE)

y-axis : **free energy** { AMP's "objective function" (minimize)

**AMP** { gradient descent starting from  $\rho = 0$  (left side)

**STAT** (statistical) { global minimum

So yields **computational** and **statistical** MSE for each

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group
  - | Significantly generalize  $\mathbb{Z}=2$  case

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group
  - | Significantly generalize  $\mathbb{Z}=2$  case
- | We give a precise analysis of the statistical and computational limits of this model

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat



# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group
  - | Significantly generalize  $k=2$  case
- | We give a precise analysis of the statistical and computational limits of this model
  - | Uses non-rigorous (but well-established) ideas from **statistical physics**
    - | Methods proven correct in related settings

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group
  - | Significantly generalize  $\mathbb{Z}=2$  case
- | We give a precise analysis of the statistical and computational limits of this model
  - | Uses non-rigorous (but well-established) ideas from **statistical physics**
    - | Methods proven correct in related settings
  - | Includes an AMP algorithm which we believe is optimal among all polynomial-time algorithms

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

# Our contributions

Joint work with Amelia Perry, Afonso Bandeira, Ankur Moitra

- | Using **representation theory** we define a very general Gaussian observation model for synchronization over any compact group
  - | Significantly generalize  $\mathbb{Z}=2$  case
- | We give a precise analysis of the statistical and computational limits of this model
  - | Uses non-rigorous (but well-established) ideas from **statistical physics**
    - | Methods proven correct in related settings
  - | Includes an AMP algorithm which we believe is optimal among all polynomial-time algorithms
- | Also some rigorous statistical lower and upper bounds

---

Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups to appear in CPAM

Perry, W., Bandeira, Moitra, Optimality and Sub-optimality of PCA for Spiked Random Matrices and Synchronization, part I to appear in Ann. Stat

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)
- | Observe

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)
- | Observe

$$Y^{(1)} = \frac{1}{n} x x^* + \frac{1}{n} W^{(1)}$$



## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)
- | Observe

$$Y^{(1)} = \frac{1}{n} x x^* + \frac{1}{n} W^{(1)}$$

$$Y^{(2)} = \frac{2}{n} x^2 x^{*2} + \frac{1}{n} W^{(2)}$$

$$Y^{(K)} = \frac{K}{n} x^K x^{*K} + \frac{1}{n} W^{(K)}$$

where  $x^k$  means **entry-wise**  $k$ th power.

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)
- | Observe

$$Y^{(1)} = \frac{1}{n} x x^* + \frac{1}{n} W^{(1)}$$

$$Y^{(2)} = \frac{2}{n} x^2 x^{*2} + \frac{1}{n} W^{(2)}$$

$$Y^{(k)} = \frac{k}{n} x^k x^{*k} + \frac{1}{n} W^{(k)}$$

where  $x^k$  means **entry-wise**  $k$ th power.

- | This model has information on different frequencies

## Multi-frequency $U(1)$ synchronization

- |  $G = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  (angles)
- | True signal  $x \in U(1)^n$
- |  $W$  { complex Gaussian noise (GUE)
- | Observe

$$Y^{(1)} = \frac{1}{n} x x^* + \frac{1}{n} W^{(1)}$$

$$Y^{(2)} = \frac{2}{n} x^2 x^{*2} + \frac{1}{n} W^{(2)}$$

$$Y^{(K)} = \frac{K}{n} x^K x^{*K} + \frac{1}{n} W^{(K)}$$

where  $x^k$  means **entry-wise**  $k$ th power.

- | This model has information on different frequencies
- | Challenge: how to synthesize information across frequencies?

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} x^k x^{k*} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} x^{(k)} x^{(k)H} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^{(k)}; \dots; x_n^{(k)})$

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} x^k x^{k*} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^k; \dots; x_n^k)$

AMP algorithm:

- | Power iteration (separately on each frequency):  
$$v^{(k)} \leftarrow \frac{1}{n} Y^{(k)} v^{(k)}$$

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} \sum_{i=1}^n x_i^k x_i^{*k} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^k; \dots; x_n^k)$

AMP algorithm:

- | Power iteration (separately on each frequency):  
$$v^{(k)} = \frac{1}{n} Y^{(k)} v^{(k)}$$
- | "Soft projection" (separately on each index):  $v_i^{(k)} = F(v_i^{(k)})$ 
  - | This synthesizes the frequencies in a non-trivial way

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} \sum_{i=1}^n x_i^k x_i^{*k} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^k; \dots; x_n^k)$

AMP algorithm:

- | Power iteration (separately on each frequency):  
$$v^{(k)} \leftarrow \frac{1}{n} Y^{(k)} v^{(k)}$$
- | "Soft projection" (separately on each index):  $v_i^{(k)} \leftarrow F(v_i^{(k)})$ 
  - | This synthesizes the frequencies in a non-trivial way
- | Onsager correction term



## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} x^k x^{k*} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^k; \dots; x_n^k)$

AMP algorithm:

- | Power iteration (separately on each frequency):  
$$v^{(k)} \leftarrow Y^{(k)} v^{(k)}$$
- | "Soft projection" (separately on each index):  $v_i^{(k)} \leftarrow F(v_i^{(k)})$ 
  - | This synthesizes the frequencies in a non-trivial way
- | Onsager correction term

Analysis of AMP:

- | Exact expression for AMP's MSE (as a function of  $1; \dots; K$ )

## AMP for U(1) synchronization

$$Y^{(k)} = \frac{1}{n} \sum_{i=1}^n x_i^k x_i^{*k} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

Algorithm's state:  $v^{(k)} \in \mathbb{C}^n$  for each frequency  $k$

- |  $v^{(k)}$  is an estimate of  $(x_1^k; \dots; x_n^k)$

AMP algorithm:

- | Power iteration (separately on each frequency):  

$$v^{(k)} \leftarrow \frac{1}{n} Y^{(k)} v^{(k)}$$
- | "Soft projection" (separately on each index):  $v_i^{(k)} \leftarrow F(v_i^{(k)})$ 
  - | This synthesizes the frequencies in a non-trivial way
- | Onsager correction term

Analysis of AMP:

- | Exact expression for AMP's MSE (as  $n \rightarrow \infty$ ) as a function of  $1; \dots; K$
- | Also, exact expression for the statistically optimal MSE

## Results forU(1) synchronization

$$Y^{(k)} = \frac{k}{n} X^k X^k + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

## Results for U(1) synchronization

$$Y^{(k)} = \frac{k}{n} x^k x^k + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

- | Single frequency: given  $Y^{(k)}$ , can non-trivially estimate  $x^k$  if  $k > 1$

## Results for U(1) synchronization

$$Y^{(k)} = \frac{\alpha^k}{n} X^k + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

- Single frequency: given  $Y^{(k)}$ , can non-trivially estimate  $\alpha^k$  if  $\alpha^k > 1$
- Information-theoretically, with  $\alpha^k = \frac{1}{K}$ , need  $\frac{1}{\log K} \log K = 1$  (for large  $K$ )

## Results for $U(1)$ synchronization

$$Y^{(k)} = \frac{\kappa}{n} x^k x^{k^*} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

- | Single frequency: given  $Y^{(k)}$ , can non-trivially estimate  $x^k$  if  $\kappa > 1$
- | Information-theoretically, with  $\kappa = 1$ , need  $\frac{1}{\log K} \approx \frac{1}{K}$  (for large  $K$ )
- | But AMP (and conjecturally, any poly-time algorithm) requires  $\kappa > 1$  for some  $k$

## Results for $U(1)$ synchronization

$$Y^{(k)} = \frac{\alpha^k}{n} X^k X^{*k} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

- | Single frequency: given  $Y^{(k)}$ , can non-trivially estimate  $\alpha^k$  if  $\alpha^k > 1$
- | Information-theoretically, with  $\alpha_1 = \dots = \alpha_K = \alpha$ , need  $\frac{1}{\log K} \approx \frac{1}{K}$  (for large  $K$ )
- | But AMP (and conjecturally, any poly-time algorithm) requires  $\alpha^k > 1$  for some  $k$ 
  - | Computationally hard to synthesize sub-critical ( $< 1$ ) frequencies

## Results for U(1) synchronization

$$Y^{(k)} = \frac{\alpha^k}{n} X^k X^{*k} + \frac{1}{n} W^{(k)} \quad \text{for } k = 1; \dots; K$$

- | Single frequency: given  $Y^{(k)}$ , can non-trivially estimate  $\alpha^k$  if  $\alpha^k > 1$
- | Information-theoretically, with  $\alpha^k = \frac{1}{K} = \frac{1}{K}$ , need  $\frac{1}{\log K} \approx \frac{1}{\log K}$  (for large  $K$ )
- | But AMP (and conjecturally, any poly-time algorithm) requires  $\alpha^k > 1$  for some  $k$ 
  - | Computationally hard to synthesize sub-critical ( $\alpha^k < 1$ ) frequencies
- | But once above the  $\alpha^k = 1$  threshold, adding frequencies helps reduce MSE of AMP



# Results for $U(1)$ synchronization

Solid: AMP ( $n = 100$ )

( $K = \text{num freq}$ )

Dotted: theoretical ( $n! - 1$ )

Same on each frequency

---

Image credit: Perry, W., Bandeira, Moitra, Message-passing algorithms for synchronization problems over compact groups, to appear in CPAM

## General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

## General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

How to even define the model?

- | Need to add "noise" to a group element  $g_j$

# General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

How to even define the model?

- | Need to add "noise" to a group element  $g_j$

**Answer:** Use **representation theory** to represent a group element as a matrix (and then add Gaussian noise)

# General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

How to even define the model?

- | Need to add "noise" to a group element  $g, g^{-1}$

**Answer:** Use **representation theory** to represent a group element as a matrix (and then add Gaussian noise)

- | A **representation** of  $G$  is a way to assign a matrix  $\rho(g)$  to each  $g \in G$
- | Formally, a homomorphism  $\rho : G \rightarrow GL(\mathbb{C}^d) = \text{set of } d \times d \text{ invertible matrices}$

# General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

How to even define the model?

- | Need to add "noise" to a group element  $g, g^{-1}$

**Answer:** Use **representation theory** to represent a group element as a matrix (and then add Gaussian noise)

- | A **representation** of  $G$  is a way to assign a matrix  $\rho(g)$  to each  $g \in G$
- | Formally, a homomorphism  $\rho: G \rightarrow GL(\mathbb{C}^d) = \{d \times d \text{ invertible matrices}\}$

**Frequencies** are replaced by **irreducible representations** of  $G$

- | Fourier theory for functions  $f: G \rightarrow \mathbb{C}$

# General groups

All of the above extends to any compact group

- | E.g. Any finite group;  $SO(3)$

How to even define the model?

- | Need to add "noise" to a group element  $g_j$

**Answer:** Use **representation theory** to represent a group element as a matrix (and then add Gaussian noise)

- | A **representation** of  $G$  is a way to assign a matrix  $\rho(g)$  to each  $g \in G$
- | Formally, a homomorphism  $\rho: G \rightarrow GL(\mathbb{C}^d)$  =  $d \times d$  invertible matrices

**Frequencies** are replaced by **irreducible representations** of  $G$

- | Fourier theory for functions  $f: G \rightarrow \mathbb{C}$

For  $U(1)$ , 1D irreducible representation for each  $k \in \mathbb{Z}$  with  $\rho_k(g) = g^k$

## Part II: Orbit Recovery



# Back to cryo-EM

Image credit: [Singer, Shkolnisky '11]

# Back to cryo-EM

Image credit: [Singer, Shkolnisky '11]

Synchronization is not the ideal model for cryo-EM

# Back to cryo-EM

Image credit: [Singer, Shkolnisky '11]

Synchronization is not the ideal model for cryo-EM

- | The synchronization approach disregards the underlying signal (the molecule)

# Back to cryo-EM

Image credit: [Singer, Shkolnisky '11]

Synchronization is not the ideal model for cryo-EM

- | The synchronization approach disregards the underlying signal (the molecule)
- | Our Gaussian synchronization model assumes independent noise on each pair  $i, j$  of images, whereas actually there is independent noise on each image

# Back to cryo-EM

Image credit: [Singer, Shkolnisky '11]

Synchronization is not the ideal model for cryo-EM

- | The synchronization approach disregards the underlying signal (the molecule)
- | Our Gaussian synchronization model assumes independent noise on each pair  $i, j$  of images, whereas actually there is independent noise on each image
- | For high noise, it is impossible to reliably recover the rotations
  - | So we should not try to estimate the rotations!

## Orbit recovery problem

Let  $G$  be a **compact** group acting **linearly** and **continuously** on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

## Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

- | Compact: e.g. any finite group,  $SO(2)$ ,  $SO(3)$

# Orbit recovery problem

Let  $G$  be a **compact** group acting **linearly** and **continuously** on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

- | Compact: e.g. any finite group,  $SO(2)$ ,  $SO(3)$
- | Linear:  $\rho : G \rightarrow GL(V) = \text{invertible } p \times p \text{ matrices}$   
(homomorphism)



# Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

- | Compact: e.g. any finite group,  $SO(2)$ ,  $SO(3)$
- | Linear:  $\rho: G \rightarrow GL(V) = \text{invertible } p \times p \text{ matrices}$   
(homomorphism)
- | Action:  $g \cdot x = \rho(g)x$  for  $g \in G; x \in V$

# Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

- | Compact: e.g. any finite group,  $SO(2)$ ,  $SO(3)$
- | Linear:  $\rho : G \rightarrow GL(V) = \text{invertible } p \times p \text{ matrices}$   
(homomorphism)
- | Action:  $g \cdot x = \rho(g)x$  for  $g \in G; x \in V$
- | Continuous:  $\rho$  is continuous

## Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

## Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

Unknown signal  $x \in V$  (e.g. the molecule)

# Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

Unknown signal  $x \in V$  (e.g. the molecule)

For  $i = 1, \dots, n$  observe  $y_i = g_i x + \epsilon_i$  where:

- |  $g_i \sim \text{Haar}(G)$  ("uniform distribution" on  $G$ )
- |  $\epsilon_i \sim N(0; \sigma^2 I_p)$  (noise)

## Orbit recovery problem

Let  $G$  be a compact group acting linearly and continuously on a finite-dimensional real vector space  $V = \mathbb{R}^p$ .

Unknown signal  $x \in V$  (e.g. the molecule)

For  $i = 1, \dots, n$  observe  $y_i = g_i x + \epsilon_i$  where:

- $g_i \sim \text{Haar}(G)$  ("uniform distribution" on  $G$ )
- $\epsilon_i \sim N(0; \sigma^2 I_p)$  (noise)

Goal: Recover some  $x$  in the orbit  $\{g x : g \in G\}$  of  $x$

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}/p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1, \dots, n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

Image credit: Jonathan Weed

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}_p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1, \dots, n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017



# Special case: multi-reference alignment (MRA)

$G = \mathbb{Z} = p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_i x_i$

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z} = p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\frac{1}{p} \sum_i x_i$  (mean)

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z} = p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\frac{1}{p} \sum_i x_i$  (mean)

Degree-2:

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0; \Sigma)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_i x_i$  (mean)

Degree-2:  $\sum_i x_i^2$

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1x_2 + x_2x_3 + \dots + x_px_1; \dots$

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0; \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1x_2 + x_2x_3 + \dots + x_px_1; \dots$  (autocorrelation)

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim N(0, \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1x_2 + x_2x_3 + \dots + x_px_1; \dots$  (autocorrelation)

Degree-3:

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017



## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1x_2 + x_2x_3 + \dots + x_px_1; \dots$  (autocorrelation)

Degree-3:  $x_1x_2x_3 + x_2x_3x_4 + \dots$

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

## Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}^p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1 x_2 + x_2 x_3 + \dots + x_p x_1; \dots$  (autocorrelation)

Degree-3:  $x_1 x_2 x_3 + x_2 x_3 x_4 + \dots$  (triple correlation)

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

# Special case: multi-reference alignment (MRA)

$G = \mathbb{Z}_p$  acts on  $\mathbb{R}^p$  via cyclic shifts

For  $i = 1; \dots; n$  observe  $y_i = g_i x + \epsilon_i$  with  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

**Method of invariants**[1,2]: measure features of the signal that are shift-invariant

Degree-1:  $\sum_{i=1}^p x_i$  (mean)

Degree-2:  $\sum_{i=1}^p x_i^2, x_1x_2 + x_2x_3 + \dots + x_px_1; \dots$  (autocorrelation)

Degree-3:  $x_1x_2x_3 + x_2x_3x_4 + \dots$  (triple correlation)

**Invariant features are easy to estimate from the samples**

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

[2] Perry, Weed, Bandeira, Rigollet, Singer, The sample complexity of multi-reference alignment, 2017

# Sample complexity

Theorem[1]:

(Upper bound) With noise level  $\epsilon$ , can estimate degree-invariants using  $n = O(\epsilon^{-2d})$  samples.

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

# Sample complexity

Theorem[1]:

(Upper bound) With noise level  $\epsilon$ , can estimate degree- $d$  invariants using  $n = O(\frac{1}{\epsilon^2} \binom{2d}{d})$  samples.

(Lower bound) If  $x^{(1)}, x^{(2)}$  agree on all invariants of degree  $d - 1$  then  $\binom{2d}{d}$  samples are required to distinguish them.

| **Method of invariants is optimal**

# Sample complexity

Theorem[1]:

(Upper bound) With noise level  $\epsilon$ , can estimate degree- $d$  invariants using  $n = O\left(\frac{1}{\epsilon^2} \binom{2d}{d}\right)$  samples.

(Lower bound) If  $x^{(1)}, x^{(2)}$  agree on all invariants of degree  $d - 1$  then  $\binom{2d}{d}$  samples are required to distinguish them.

| **Method of invariants is optimal**

**Question:** What degree  $d$  of invariants do we need to learn before we can recover (the orbit of)  $x$ ?

| Optimal sample complexity is  $n = \binom{2d}{d}$

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

# Sample complexity

Theorem[1]:

(Upper bound) With noise level  $\epsilon$ , can estimate degree- $d$  invariants using  $n = O\left(\frac{1}{\epsilon^2} \binom{2d}{d}\right)$  samples.

(Lower bound) If  $x^{(1)}, x^{(2)}$  agree on all invariants of degree  $d - 1$  then  $\binom{2d}{d}$  samples are required to distinguish them.

| **Method of invariants is optimal**

**Question:** What degree  $d$  of invariants do we need to learn before we can recover (the orbit of)  $x$ ?

| Optimal sample complexity is  $n = \binom{2d}{d}$

**Answer (for MRA)[1]:**

| For "generic"  $x$ , **degree 3** is sufficient, so sample complexity  $n = \binom{6}{3}$

# Sample complexity

Theorem[1]:

(Upper bound) With noise level  $\epsilon$ , can estimate degree- $d$  invariants using  $n = O(\frac{1}{\epsilon^2} \binom{2d}{d})$  samples.

(Lower bound) If  $x^{(1)}, x^{(2)}$  agree on all invariants of degree  $d - 1$  then  $\binom{2d}{d}$  samples are required to distinguish them.

| Method of invariants is optimal

Question: What degree  $d$  of invariants do we need to learn before we can recover (the orbit of)  $x$ ?

| Optimal sample complexity is  $n = \binom{2d}{d}$

Answer (for MRA)[1]:

| For "generic"  $x$ , degree 3 is sufficient, so sample complexity  $n = \binom{6}{3}$

| But for a measure-zero set of "bad" signals, need much higher degree (as high as  $d$ )

---

[1] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017



## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g x + \epsilon$  with  $g \sim G, \epsilon \sim N(0; \sigma^2 I)$

## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g \cdot x + \epsilon$  with  $g \in G$ ,  $\epsilon \sim N(0; \sigma^2 I)$

The distribution of  $y$  is a (uniform) mixture of  $|G|$  Gaussians centered at  $g \cdot x : g \in G$

## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g \cdot x + \epsilon$  with  $g \in G$ ,  $\epsilon \sim N(0; \sigma^2 I)$

The distribution of  $y$  is a (uniform) mixture of  $|G|$  Gaussians centered at  $g \cdot x : g \in G$

- | For infinite groups, a mixture of infinitely-many Gaussians

## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g \cdot x + \epsilon$  with  $g \in G$ ,  $\epsilon \sim N(0; \sigma^2 I)$

The distribution of  $y$  is a (uniform) mixture of  $|G|$  Gaussians centered at  $g \cdot x : g \in G$

- | For infinite groups, a mixture of infinitely-many Gaussians

**Method of moments:** Estimate moments  $E[y]$ ;  $E[y^2]$ ;  $\dots$ ;  $E[y^d]$

## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g \cdot x + \epsilon$  with  $g \in G$ ,  $\epsilon \sim N(0; \sigma^2 I)$

The distribution of  $y$  is a (uniform) mixture of  $|G|$  Gaussians centered at  $g \cdot x : g \in G$

- For infinite groups, a mixture of infinitely-many Gaussians

**Method of moments:** Estimate moments  $E[y]$ ;  $E[y^2]$ ;  $\dots$ ;  $E[y^d]$

$$E[y^k] = E_g[(g \cdot x)^k]$$

## Another viewpoint: mixtures of Gaussians

MRA sample:  $y = g \cdot x + \epsilon$  with  $g \in G$ ,  $\epsilon \sim N(0; \sigma^2)$

The distribution of  $y$  is a (uniform) mixture of  $|G|$  Gaussians centered at  $g \cdot x : g \in G$

- | For infinite groups, a mixture of infinitely-many Gaussians

**Method of moments:** Estimate moments  $E[y]$ ;  $E[y^2]$ ;  $\dots$ ;  $E[y^d]$

$$E[y^k] = E_g[(g \cdot x)^k]$$

**Fact:** Moments are equivalent to invariants

- |  $E_g[(g \cdot x)^k]$  contains the same information as the degree- $k$  invariant polynomials

# Our contributions

Joint work with Ben Blum-Smith, Afonso Bandeira, Amelia Perry,  
Jonathan Weed

# Our contributions

Joint work with Ben Blum-Smith, Afonso Bandeira, Amelia Perry, Jonathan Weed

- | We generalize from MRA to **any compact group**



# Our contributions

Joint work with Ben Blum-Smith, Afonso Bandeira, Amelia Perry, Jonathan Weed

- | We generalize from MRA to **any compact group**
- | Again, the method of invariants/moments is optimal

# Our contributions

Joint work with Ben Blum-Smith, Afonso Bandeira, Amelia Perry, Jonathan Weed

- | We generalize from MRA to **any compact group**
- | Again, the method of invariants/moments is optimal
- | We give an (inefficient) algorithm that achieves optimal sample complexity: solve polynomial system

# Our contributions

Joint work with Ben Blum-Smith, Afonso Bandeira, Amelia Perry, Jonathan Weed

- | We generalize from MRA to **any compact group**
- | Again, the method of invariants/moments is optimal
- | We give an (inefficient) algorithm that achieves optimal sample complexity: solve polynomial system
- | To determine what degree of invariants are required, we use **invariant theory** and **algebraic geometry**
  - | How to tell if polynomial equations have a unique solution

# Invariant theory

Variables  $x_1; \dots; x_p$  (corresponding to the coordinates  $\alpha$ )

# Invariant theory

Variables  $x_1; \dots; x_p$  (corresponding to the coordinates of)

The **invariant ring**  $R[x]^G$  is the subring of  $R[x] := R[x_1; \dots; x_p]$  consisting of polynomials  $f$  such that  $f(g \cdot x) = f(x) \quad \forall g \in G$ .

# Invariant theory

Variables  $x_1; \dots; x_p$  (corresponding to the coordinates of)

The **invariant ring**  $R[x]^G$  is the subring of  $R[x] := R[x_1; \dots; x_p]$  consisting of polynomials  $f$  such that  $f(g \cdot x) = f(x) \quad \forall g \in G$ .

- | Aside: A main result of invariant theory is that  $R[x]^G$  is finitely-generated

# Invariant theory

Variables  $x_1; \dots; x_p$  (corresponding to the coordinates of)

The **invariant ring**  $R[x]^G$  is the subring of  $R[x] := R[x_1; \dots; x_p]$  consisting of polynomials  $f$  such that  $f(g \cdot x) = f(x) \quad \forall g \in G$ .

- Aside: A main result of invariant theory is that  $R[x]^G$  is finitely-generated

$R[x]^G_d = \{ \text{invariants of degree } d \}$

# Invariant theory

Variables  $x_1; \dots; x_p$  (corresponding to the coordinates of)

The **invariant ring**  $R[x]^G$  is the subring of  $R[x] := R[x_1; \dots; x_p]$  consisting of polynomials  $f$  such that  $f(g \cdot x) = f(x) \forall g \in G$ .

- Aside: A main result of invariant theory is that  $R[x]^G$  is finitely-generated

$R[x]^G_d$  { invariants of degree  $d$

(Simple) algorithm:

- Pick  $d$  (to be chosen later)
- Using  $\binom{2d}{d}$  samples, estimate invariants up to degree: learn values  $f(x)$  for all  $f \in R[x]^G_d$
- Solve for  $ax$  that is consistent with those values:  
 $f(ax) = f(x) \forall f \in R[x]^G_d$  (polynomial system of equations)



# All invariants determine orbit

**Theorem**[1]: If  $G$  is compact, for every  $x \in V$ , the full invariant ring  $R[x]^G$  determines  $x$  up to orbit.

- | In the sense that if  $x, x^0$  do not lie in the same orbit, there exists  $f \in R[x]^G$  that separates them  $f(x) \neq f(x^0)$

---

[1] Katz, Invariant theory lecture notes, 1994

[2] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

# All invariants determine orbit

**Theorem**[1]: If  $G$  is compact, for every  $x \in V$ , the full invariant ring  $R[x]^G$  determines  $x$  up to orbit.

- | In the sense that if  $x, x^0$  do not lie in the same orbit, there exists  $f \in R[x]^G$  that separates them  $f(x) \neq f(x^0)$

**Corollary**: Suppose that for some  $d$ ,  $R[x]^G_d$  generates  $R[x]^G$  (as an  $R$ -algebra). Then  $R[x]^G_d$  determines  $x$  up to orbit and so sample complexity is  $\mathcal{O}(2^d)$ .

---

[1] Katz, Invariant theory lecture notes, 1994

[2] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

# All invariants determine orbit

**Theorem**[1]: If  $G$  is compact, for every  $x \in V$ , the full invariant ring  $R[x]^G$  determines  $x$  up to orbit.

- | In the sense that if  $x, x^0$  do not lie in the same orbit, there exists  $f \in R[x]^G$  that separates them  $f(x) \neq f(x^0)$

**Corollary:** Suppose that for some  $d$ ,  $R[x]^G_d$  generates  $R[x]^G$  (as an  $R$ -algebra). Then  $R[x]^G_d$  determines  $x$  up to orbit and so sample complexity is  $\mathcal{O}(2^d)$ .

**Problem:** This is for **worst-case**  $x \in V$ . For MRA (cyclic shifts) this requires  $d = p$  whereas generic  $x$  only requires  $d = 3$  [2].

---

[1] Katz, Invariant theory lecture notes, 1994

[2] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

# All invariants determine orbit

**Theorem**[1]: If  $G$  is compact, for every  $x \in V$ , the full invariant ring  $\mathbb{R}[x]^G$  determines  $x$  up to orbit.

- In the sense that if  $x, x^0$  do not lie in the same orbit, there exists  $f \in \mathbb{R}[x]^G$  that separates them  $f(x) \neq f(x^0)$

**Corollary:** Suppose that for some  $d$ ,  $\mathbb{R}[x]^G_d$  generates  $\mathbb{R}[x]^G$  (as an  $\mathbb{R}$ -algebra). Then  $\mathbb{R}[x]^G_d$  determines  $x$  up to orbit and so sample complexity is  $\mathcal{O}(2^d)$ .

**Problem:** This is for **worst-case**  $x \in V$ . For MRA (cyclic shifts) this requires  $d = p$  whereas generically only requires  $d = 3$  [2].

Actually care about whether  $\mathbb{R}[x]^G_d$  **generically** determine  $\mathbb{R}[x]^G$

---

[1] Katz, Invariant theory lecture notes, 1994

[2] Bandeira, Rigollet, Weed, Optimal rates of estimation for multi-reference alignment, 2017

## Do polynomials generically determine other polynomials?

Say we have  $A, B \in R[x]$

- | (Technically need to assume  $B$  is finitely generated)

## Do polynomials generically determine other polynomials?

Say we have  $A \subseteq B \subseteq R[x]$

- (Technically need to assume  $B$  is finitely generated)

**Question:** Do the values  $\{a(x) : a \in A\}$  generically determine the values  $\{b(x) : b \in B\}$ ?

# Do polynomials generically determine other polynomials?

Say we have  $A \subseteq B \subseteq R[x]$

| (Technically need to assume  $B$  is finitely generated)

**Question:** Do the values  $\{a(x) : a \in A\}$  generically determine the values  $\{b(x) : b \in B\}$ ?

**Definition:** Polynomials  $f_1, \dots, f_m$  are **algebraically independent** if there is no  $P \in R[y_1, \dots, y_m]$  with  $P(f_1, \dots, f_m) = 0$ .

# Do polynomials generically determine other polynomials?

Say we have  $A \subseteq B \subseteq R[x]$

| (Technically need to assume  $B$  is finitely generated)

**Question:** Do the values  $\{a(x) : a \in A\}$  generically determine the values  $\{b(x) : b \in B\}$ ?

**Definition:** Polynomials  $f_1, \dots, f_m$  are **algebraically independent** if there is no  $P \in R[y_1, \dots, y_m]$  with  $P(f_1, \dots, f_m) = 0$ .

**Definition:** For  $U \subseteq R[x]$ , the **transcendence degree** ~~trdeg~~ is the number of algebraically independent polynomials in  $U$ .



# Do polynomials generically determine other polynomials?

Say we have  $A \subseteq B \subseteq \mathbb{R}[x]$

- (Technically need to assume  $B$  is finitely generated)

**Question:** Do the values  $\{a(x) : a \in A\}$  generically determine the values  $\{b(x) : b \in B\}$ ?

**Definition:** Polynomials  $f_1, \dots, f_m$  are **algebraically independent** if there is no  $P \in \mathbb{R}[y_1, \dots, y_m]$  with  $P(f_1, \dots, f_m) = 0$ .

**Definition:** For  $U \subseteq \mathbb{R}[x]$ , the **transcendence degree**  $\text{trdeg}(U)$  is the number of algebraically independent polynomials in  $U$ .

**Answer:** Suppose  $\text{trdeg}(A) = \text{trdeg}(B)$ . If  $x$  is "generic" then the values  $\{a(x) : a \in A\}$  determine a **finite number** of possibilities for the entire collection  $\{b(x) : b \in B\}$ .

- "Generic":  $x$  lies in a particular full-measure set

# How to test algebraic independence?

# How to test algebraic independence?

This is actually easy!

# How to test algebraic independence?

This is actually easy!

**Theorem (Jacobian criterion):**

Polynomials  $f_1, \dots, f_m \in \mathbb{R}[x_1, \dots, x_p]$  are algebraically independent if and only if the  $m \times p$  Jacobian matrix  $J_{ij} = \frac{\partial f_i}{\partial x_j}$  has full row rank. (Still true if you evaluate at a generic point.)

# How to test algebraic independence?

This is actually easy!

**Theorem (Jacobian criterion):**

Polynomials  $f_1, \dots, f_m \in \mathbb{R}[x_1, \dots, x_p]$  are algebraically independent if and only if the  $m \times p$  Jacobian matrix  $J_{ij} = \frac{\partial f_i}{\partial x_j}$  has full row rank. (Still true if you evaluate at a generic point.)

- | Why: Tests whether map  $x_1, \dots, x_p \mapsto (f_1(x), \dots, f_m(x))$  is locally surjective

## Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$

## Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

Procedure:



# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Procedure:

- | Need to test whether  $\mathbb{R}[x]_d^G$  determines  $\mathbb{R}[x]^G$  (generically)

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Procedure:

- | Need to test whether  $R[x]_d^G$  determines  $R[x]^G$  (generically)
- | So need to check if  $\text{trdeg}(R[x]_d^G) = \text{trdeg}(R[x]^G)$

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Procedure:

- | Need to test whether  $R[x]_d^G$  determines  $R[x]^G$  (generically)
- | So need to check if  $\text{trdeg}(R[x]_d^G) = \text{trdeg}(R[x]^G)$
- |  $\text{trdeg}(R[x]^G)$  is easy:  $\dim(x) - \dim(\text{orbit})$

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Procedure:

- | Need to test whether  $R[x]_{G_d}^G$  determines  $R[x]^G$  (generically)
- | So need to check if  $\text{trdeg}(R[x]_{G_d}^G) = \text{trdeg}(R[x]^G)$
- |  $\text{trdeg}(R[x]^G)$  is easy:  $\dim(x) - \dim(\text{orbit})$
- |  $\text{trdeg}(R[x]_{G_d}^G)$  via Jacobian criterion

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

Comments:

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Comments:

- | For e.g. MRA (cyclic shifts), need to test each  $\phi$  separately on a computer

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Comments:

- | For e.g. MRA (cyclic shifts), need to test each  $\phi$  separately on a computer
- | Not an efficient algorithm to solve any particular instance

# Generic list recovery

Our **main result** is an efficient procedure that takes the problem setup as input (group  $G$  and action on  $V$ ) and outputs the degree  $d$  of invariants required for **generic list recovery**.

- | List recovery: output a finite list  $x^{(1)}; x^{(2)}; \dots$ , one of which (approximately) lies in the orbit of the true  $x$
- | List recovery may be good enough in practice?

## Comments:

- | For e.g. MRA (cyclic shifts), need to test each  $\phi$  separately on a computer
- | Not an efficient algorithm to solve any particular instance
- | There is also an algorithm to bound the size of the list (or test for **unique recovery**), but it is not efficient (Gröbner bases)



# Generalized orbit recovery problem

Extensions:

# Generalized orbit recovery problem

Extensions:

- | Projection (e.g. cryo-EM):
  - |  $\text{Observe } y_i = (g_i x) + \epsilon_i$
  - |  $g_i : V \rightarrow W$  linear
  - |  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$

# Generalized orbit recovery problem

Extensions:

| Projection (e.g. cryo-EM):

- | Observe  $y_i = (g_i x) + \epsilon_i$
- |  $g_i : V \rightarrow W$  linear
- |  $\epsilon_i \sim N(0, \sigma^2 I)$

| Heterogeneity:

- |  $K$  signals  $x^{(1)}; \dots; x^{(K)}$
- | Mixing weights  $(w_1; \dots; w_K) \in \mathbb{R}^K$
- | Observe  $y_i = (g_i x^{(k_i)}) + \epsilon_i$
- |  $k_i \in \{1; \dots; K\}$  according to  $w$

# Generalized orbit recovery problem

Extensions:

| Projection (e.g. cryo-EM):

- | Observe  $y_i = (g_i x) + \epsilon_i$
- |  $g_i : V \rightarrow W$  linear
- |  $\epsilon_i \sim N(0, \sigma^2 I)$

| Heterogeneity:

- |  $K$  signals  $x^{(1)}; \dots; x^{(K)}$
- | Mixing weights  $(w_1; \dots; w_K) \in \mathbb{R}^K$
- | Observe  $y_i = (g_i x^{(k_i)}) + \epsilon_i$
- |  $k_i \in \{1; \dots; K\}$  according to  $w$

Same methods apply!

# Generalized orbit recovery problem

Extensions:

- | Projection (e.g. cryo-EM):
  - | Observe  $y_i = \Pi(g_i x) + \epsilon_i$
  - |  $\Pi : V \rightarrow W$  linear
  - |  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 I)$
- | Heterogeneity:
  - |  $K$  signals  $x^{(1)}, \dots, x^{(K)}$
  - | Mixing weights  $(w_1, \dots, w_K) \succeq \Delta_K$
  - | Observe  $y_i = \Pi(g_i x^{(k_i)}) + \epsilon_i$
  - |  $k_i \in \{1, \dots, K\}$  according to  $w$

Same methods apply!

- | Order- $d$  moments now only give access to a particular subspace of  $\mathbb{R}[\mathbf{x}]^G$

# Generalized orbit recovery problem

Extensions:

- | Projection (e.g. cryo-EM):
  - | Observe  $y_i = \Pi(g_i x) + \epsilon_i$
  - |  $\Pi : V \rightarrow W$  linear
  - |  $\epsilon_i \sim \mathcal{N}(0, \sigma^2 \mathbf{I})$
- | Heterogeneity:
  - |  $K$  signals  $x^{(1)}; \dots; x^{(K)}$
  - | Mixing weights  $(w_1; \dots; w_K) \in \Delta_K$
  - | Observe  $y_i = \Pi(g_i x^{(k_i)}) + \epsilon_i$
  - |  $k_i \in \{1; \dots; K\}$  according to  $w$

Same methods apply!

- | Order- $d$  moments now only give access to a particular subspace of  $\mathbb{R}[\mathbf{x}]^G$
- | For heterogeneity, work over a bigger group  $G^K$  acting on  $(x^{(1)}; \dots; x^{(K)}) \in V^K$

## Results: cryo-EM

Our methods show that for cryo-EM, generic list recovery is possible at **degree 3**

## Results: cryo-EM

Our methods show that for cryo-EM, generic list recovery is possible at **degree 3**

So information-theoretic sample complexity is  $\Theta(n^6)$



## Results: cryo-EM

Our methods show that for cryo-EM, generic list recovery is possible at **degree 3**

So information-theoretic sample complexity is  $\Theta(n^6)$

Ongoing work: **polynomial time** algorithm for cryo-EM

# Efficient recovery: tensor decomposition

Restrict to finite group

Recall: with  $O(n^6)$  samples, can estimate the third moment:

$$T_3(x) = \frac{1}{|G|} \sum_{g \in G} (g \cdot x)^{\otimes 3}$$

# Efficient recovery: tensor decomposition

Restrict to finite group

Recall: with  $O(n^6)$  samples, can estimate the third moment:

$$T_3(x) = \sum_{g \in G} (g \cdot x)^{\otimes 3}$$

This is an instance of **tensor decomposition**: Given  $\sum_{i=1}^m a_i^{\otimes 3}$  for some  $a_1, \dots, a_m \in \mathbb{R}^p$ , recover  $\{a_i\}$

# Efficient recovery: tensor decomposition

Restrict to finite group

Recall: with  $O(n^6)$  samples, can estimate the third moment:

$$T_3(x) = \sum_{g \in G} (g \cdot x)^{\otimes 3}$$

This is an instance of **tensor decomposition**: Given  $\sum_{i=1}^m a_i^{\otimes 3}$  for some  $a_1, \dots, a_m \in \mathbb{R}^p$ , recover  $\{a_i\}$

For MRA: since  $m \ll p$  (“undercomplete”) can apply **Jennrich’s algorithm** to decompose tensor efficiently [1]

---

[1] Perry, Weed, Bandeira, Rigollet, Singer, *The sample complexity of multi-reference alignment*, 2017

## Example: heterogeneous MRA

MRA with multiple signals  $x^{(1)}; \dots; x^{(K)}$

$$T_d(x) = \prod_{k=1}^K \prod_{g \in G} (g \cdot x^{(k)})^d$$

---

[1] Perry, Weed, Bandeira, Rigollet, Singer '17

[2] Boumal, Bendory, Lederman, Singer '17

[3] Ma, Shi, Steurer '16

## Example: heterogeneous MRA

MRA with multiple signals  $x^{(1)}; \dots; x^{(K)}$

$$T_d(x) = \prod_{k=1}^K \prod_{g \in G} (g \cdot x^{(k)})^d$$

Jennrich's algorithm works if given 5th moment  $n = O(10^5)$  [1]

---

[1] Perry, Weed, Bandeira, Rigollet, Singer '17

[2] Boumal, Bendory, Lederman, Singer '17

[3] Ma, Shi, Steurer '16

## Example: heterogeneous MRA

MRA with multiple signals  $x^{(1)}; \dots; x^{(K)}$

$$T_d(x) = \prod_{k=1}^K \prod_{g \in G} (g \cdot x^{(k)})^d$$

Jennrich's algorithm works if given 5th moment  $n = O(K^{10})$  [1]

**Information-theoretically**, 3rd moment suffices if  $K \leq p-6$

---

[1] Perry, Weed, Bandeira, Rigollet, Singer '17

[2] Boumal, Bendory, Lederman, Singer '17

[3] Ma, Shi, Steurer '16

## Example: heterogeneous MRA

MRA with multiple signals  $x^{(1)}; \dots; x^{(K)}$

$$T_d(x) = \prod_{k=1}^K \prod_{g \in G} (g \cdot x^{(k)})^d$$

Jennrich's algorithm works if given 5th moment  $n = O(10^6)$  [1]

**Information-theoretically**, 3rd moment suffices if  $K \geq \frac{1}{\epsilon} \log \frac{1}{\epsilon}$

If signals  $x^{(k)}$  are random (i.i.d. Gaussian), conjectured that **efficient** recovery is possible from 3rd moment iff  $K \geq \frac{1}{\epsilon} \log \frac{1}{\epsilon}$  [2]

---

[1] Perry, Weed, Bandeira, Rigollet, Singer '17

[2] Boumal, Bendory, Lederman, Singer '17

[3] Ma, Shi, Steurer '16



## Example: heterogeneous MRA

MRA with multiple signals  $x^{(1)}; \dots; x^{(K)}$

$$T_d(x) = \prod_{k=1}^K \sum_{g \in G} (g \cdot x^{(k)})^d$$

Jennrich's algorithm works if given 5th moment  $n = O(p^{10})$  [1]

**Information-theoretically**, 3rd moment suffices if  $K \geq p^6$

If signals  $x^{(k)}$  are random (i.i.d. Gaussian), conjectured that **efficient** recovery is possible from 3rd moment iff  $K \geq p^{\bar{p}}$  [2]

New result (with A. Moitra): if  $K \geq p^{\bar{p} = \text{polylog}(p)}$  then for random signals, efficient recovery is possible from 3rd moment

- | Based on random overcomplete 3-tensor decomposition [3]

---

[1] Perry, Weed, Bandeira, Rigollet, Singer '17

[2] Boumal, Bendory, Lederman, Singer '17

[3] Ma, Shi, Steurer '16

# Acknowledgements

# Acknowledgements

- | Ankur Moitra

# Acknowledgements

- | Ankur Moitra
- | Michel Goemans

# Acknowledgements

- | Ankur Moitra
- | Michel Goemans
- | Philippe Rigollet

# Acknowledgements

- | Ankur Moitra
- | Michel Goemans
- | Philippe Rigollet
- | Afonso Bandeira

# Acknowledgements

- | Ankur Moitra
- | Michel Goemans
- | Philippe Rigollet
- | Afonso Bandeira
- | Collaborators

# Acknowledgements

- | Ankur Moitra
- | Michel Goemans
- | Philippe Rigollet
- | Afonso Bandeira
- | Collaborators
- | Family



# Acknowledgements

- | Ankur Moitra
- | Michel Goemans
- | Philippe Rigollet
- | Afonso Bandeira
- | Collaborators
- | Family
- | Thank you!