The GCT Program: Recent developments and concrete open problems

Ketan D. Mulmuley

The University of Chicago

November 30, 2018

The main reference for this talk

The main reference for this talk

[GCT5][M.]: Geometric Complexity Theory V: Efficient algorithms for Noether Normalization.

The main reference for this talk

[GCT5][M.]: Geometric Complexity Theory V: Efficient algorithms for Noether Normalization.

Extended abstract: FOCS 2012.

The main reference for this talk

[GCT5][M.]: Geometric Complexity Theory V: Efficient algorithms for Noether Normalization.

Extended abstract: FOCS 2012.

Journal version: JAMS 2017.

The basic set up

The basic set up

- K: An algebraically closed field of characteristic zero.

The basic set up

- K: An algebraically closed field of characteristic zero.
- VP: The class of families of polynomials that can be computed by algebraic circuits over K of polynomial degree and size.

The basic set up

- K: An algebraically closed field of characteristic zero.
- VP: The class of families of polynomials that can be computed by algebraic circuits over K of polynomial degree and size.
- $\mathrm{VP}_{\mathrm{ws}}$: The class of families of polynomials that can be computed by symbolic determinants over K of polynomial size.

The basic set up

- K: An algebraically closed field of characteristic zero.
- VP: The class of families of polynomials that can be computed by algebraic circuits over K of polynomial degree and size.
- $\mathrm{VP}_{\mathrm{ws}}$: The class of families of polynomials that can be computed by symbolic determinants over K of polynomial size.
- VNP: The class of families of p-definable polynomials (e.g. the permanent).

The basic set up

- K: An algebraically closed field of characteristic zero.
- VP: The class of families of polynomials that can be computed by algebraic circuits over K of polynomial degree and size.
- $\mathrm{VP}_{\mathrm{ws}}$: The class of families of polynomials that can be computed by symbolic determinants over K of polynomial size.
- VNP: The class of families of *p*-definable polynomials (e.g. the permanent).
- $\overline{\mathrm{VP}}$: The class of families of polynomials that can be approximated infinitesimally closely by algebraic circuits over K of polynomial degree and size.

The basic set up

- K: An algebraically closed field of characteristic zero.
- VP: The class of families of polynomials that can be computed by algebraic circuits over K of polynomial degree and size.
- $\mathrm{VP}_{\mathrm{ws}}$: The class of families of polynomials that can be computed by symbolic determinants over K of polynomial size.
- VNP: The class of families of p-definable polynomials (e.g. the permanent).
- $\overline{\mathrm{VP}}$: The class of families of polynomials that can be approximated infinitesimally closely by algebraic circuits over K of polynomial degree and size.
- $\overline{\mathrm{VP}_{\mathrm{ws}}}$: The class of families of polynomials that can be approximated infinitesimally closely by symbolic determinants over K of polynomial size.

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6].

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem,

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem, regardless of whether the answer to this question is affirmative or negative

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem, regardless of whether the answer to this question is affirmative or negative [GCT5]

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem, regardless of whether the answer to this question is affirmative or negative [GCT5] [This lecture].

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem, regardless of whether the answer to this question is affirmative or negative [GCT5] [This lecture].
- This difficulty has to be overcome by any approach to the VP vs. VNP problem that seeks to separate VNP from $\overline{\mathrm{VP}}$.

The battleground of GCT: The VP vs. $\overline{\mathrm{VP}}$ problem

Conjecture (Valiant: 1979): $\mathrm{VP} \neq \mathrm{VNP}$.

The hardness hypothesis of GCT (GCT1:MS2001): $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$.

Any realistic approach to the VP vs. VNP problem can be expected to prove this stronger form of Valiant's conjecture.

Question [GCT1,B,BLMW]: Is $\overline{\mathrm{VP}} = \mathrm{VP}$?

- Related to foundational issues in algebraic geometry and representation theory [GCT6]. [Not covered in this lecture].
- The cause of a deep difficulty at the interface of algebraic geometry, representation theory and complexity theory, called the GCT chasm, which arises in the context of the $\overline{\mathrm{VP}}$ vs. VNP problem, regardless of whether the answer to this question is affirmative or negative [GCT5] [This lecture].
- This difficulty has to be overcome by any approach to the VP vs. VNP problem that seeks to separate VNP from $\overline{\mathrm{VP}}$. We call any such approach a GCT approach in a broad sense.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y,

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices,

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices, whose entries are homogeneous linear functions of the entries of Y

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices, whose entries are homogeneous linear functions of the entries of Y (a constructible set).

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices, whose entries are homogeneous linear functions of the entries of Y (a constructible set).
- $\Delta[\det, m] = \overline{\Sigma[\det, m]} \subseteq \mathbb{P}(V)$: The Zariski closure of $\Sigma[\det, m]$ in $\mathbb{P}(V)$

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices, whose entries are homogeneous linear functions of the entries of Y (a constructible set).
- $\Delta[\det, m] = \overline{\Sigma[\det, m]} \subseteq \mathbb{P}(V)$: The Zariski closure of $\Sigma[\det, m]$ in $\mathbb{P}(V)$ (a variety).

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem

- Let Y be an $m \times m$ variable matrix, X an $n \times n$ submatrix of Y, $n < m$, and z any entry of Y outside X.
- $V = K[Y]_m$: The space of homogeneous forms of degree m in the entries of Y.
- $\mathbb{P}(V)$: The projective space associated with V.
- $\Sigma[\det, m] \subseteq \mathbb{P}(V)$: The set of all points in $\mathbb{P}(V)$ corresponding to non-zero homogeneous polynomials in the entries of Y, which can be expressed as determinants of symbolic $m \times m$ matrices, whose entries are homogeneous linear functions of the entries of Y (a constructible set).
- $\Delta[\det, m] = \overline{\Sigma[\det, m]} \subseteq \mathbb{P}(V)$: The Zariski closure of $\Sigma[\det, m]$ in $\mathbb{P}(V)$ (a variety).
- $\Delta[det, m]$ also equals the $GL_{m^2}(K)$-orbit-closure of $\det(Y) \in \mathbb{P}(V)$ under the natural action of $GL_{m^2}(K)$ on $\mathbb{P}(V)$.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem (continued)

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem (continued)

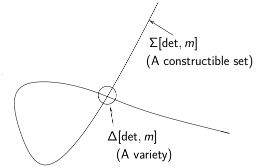
- The $\mathrm{VNP} \not\subseteq \mathrm{VP}_{\mathrm{ws}}$ conjecture [Valiant] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Sigma[\det, m]$.

Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem (continued)

- The $\mathrm{VNP} \not\subseteq \mathrm{VP}_{\mathrm{ws}}$ conjecture [Valiant] is equivalent to saying that $z^{m-n}\mathsf{perm}(X) \notin \Sigma[\det, m]$.
- The $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}_{\mathrm{ws}}}$ conjecture [GCT1] is equivalent to saying that $z^{m-n}\mathsf{perm}(X) \notin \Delta[\det, m]$.

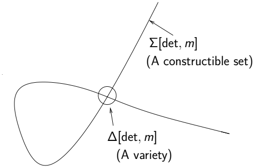
Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem (continued)

- The $\mathrm{VNP} \not\subseteq \mathrm{VP}_{\mathrm{ws}}$ conjecture [Valiant] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Sigma[\det, m]$.
- The $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}_{\mathrm{ws}}}$ conjecture [GCT1] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Delta[\det, m]$.



Reformulation of the $\overline{\mathrm{VP}_{\mathrm{ws}}}$ vs. VNP problem (continued)

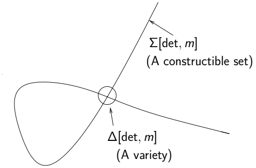
- The $\mathrm{VNP} \not\subseteq \mathrm{VP}_{\mathrm{ws}}$ conjecture [Valiant] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Sigma[\det, m]$.
- The $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}_{\mathrm{ws}}}$ conjecture [GCT1] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Delta[\det, m]$.



- The geometry of $\Sigma[\det, m]$ is controlled by the singularities of $\Delta[\det, m]$. Hence their structure is important in the context of the $\mathrm{VP}_{\mathrm{ws}}$ vs. $\overline{\mathrm{VP}_{\mathrm{ws}}}$ and $\mathrm{VP}_{\mathrm{ws}}$ vs. VNP problems.

Reformulation of the $\overline{\mathrm{VP}}_{\mathrm{ws}}$ vs. VNP problem (continued)

- The $\mathrm{VNP} \not\subseteq \mathrm{VP}_{\mathrm{ws}}$ conjecture [Valiant] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Sigma[\det, m]$.
- The $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}_{\mathrm{ws}}$ conjecture [GCT1] is equivalent to saying that $z^{m-n}\mathrm{perm}(X) \notin \Delta[\det, m]$.



- The geometry of $\Sigma[\det, m]$ is controlled by the singularities of $\Delta[\det, m]$. Hence their structure is important in the context of the $\mathrm{VP}_{\mathrm{ws}}$ vs. $\overline{\mathrm{VP}}_{\mathrm{ws}}$ and $\mathrm{VP}_{\mathrm{ws}}$ vs. VNP problems.
- Unfortunately, the singularities of $\Delta[\det, m]$ are not even normal [Kumar]. This is the beginning of difficulties [Next].

Noether's Normalization Lemma (NNL)

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Succinct means of $\text{poly}(m)$ size.

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Succinct means of poly(m) size. The usual specifications of $\Delta[\det, m] \subseteq \mathbb{P}(V)$ by its equations

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Succinct means of poly(m) size. The usual specifications of $\Delta[\det, m] \subseteq \mathbb{P}(V)$ by its equations or of ψ by its matrix

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Succinct means of $\text{poly}(m)$ size. The usual specifications of $\Delta[\det, m] \subseteq \mathbb{P}(V)$ by its equations or of ψ by its matrix are not succinct,

Noether's Normalization Lemma (NNL)

Hilbert: There exists a homogeneous linear map $\psi : V \to K^k$, for any $k > \dim(\Delta[\det, m])$, such that ψ does not vanish on any non-zero point in the affine cone $\hat{\Delta}[\det, m] \subseteq V$ of $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

This means the rational map $\hat{\psi} : \mathbb{P}(V) \dashrightarrow \mathbb{P}(K^k)$ is regular (well-defined) on $\Delta[\det, m] \subseteq \mathbb{P}(V)$.

We call such a homogeneous, linear map $\psi : V \to K^k$ a normalizing map for $\Delta[\det, m]$.

The Problem NNL:

Given $\Delta[\det, m]$, with a succinct specification, construct a normalizing map $\psi : V \to K^k$, with $k = \text{poly}(m)$, with a succinct specification.

Succinct means of $\text{poly}(m)$ size. The usual specifications of $\Delta[\det, m] \subseteq \mathbb{P}(V)$ by its equations or of ψ by its matrix are not succinct, since $\dim(V) = 2^{\text{poly}(m)}$.

The current complexity status of the problem NNL

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\det, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\det, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\mathsf{det}, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\mathrm{det}, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development [Forbes and Shpilka; Guo, Saxena, Sinhababu]:

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\det, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development [Forbes and Shpilka; Guo, Saxena, Sinhababu]: NNL is in PSPACE.

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\det, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development [Forbes and Shpilka; Guo, Saxena, Sinhababu]: NNL is in PSPACE.
- This is how far we can go without knowing the relationship between $\overline{\mathrm{VP}_{\mathrm{ws}}}$ and $\mathrm{VP}_{\mathrm{ws}}$.

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\det, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development [Forbes and Shpilka; Guo, Saxena, Sinhababu]: NNL is in PSPACE.
- This is how far we can go without knowing the relationship between $\overline{\mathrm{VP}_{\mathrm{ws}}}$ and $\mathrm{VP}_{\mathrm{ws}}$.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$, then NNL is in PH, assuming generalized Riemann hypothesis.

The current complexity status of the problem NNL

- The problem NNL for $\Delta[\mathrm{det}, m]$ is equivalent to the problem of constructing a hitting set for $\overline{\mathrm{VP}_{\mathrm{ws}}}$.
- This, in conjunction with Gröbner basis theory, implies that NNL is in EXPSPACE [GCT5].
- Recent development [Forbes and Shpilka; Guo, Saxena, Sinhababu]: NNL is in PSPACE.
- This is how far we can go without knowing the relationship between $\overline{\mathrm{VP}_{\mathrm{ws}}}$ and $\mathrm{VP}_{\mathrm{ws}}$.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$, then NNL is in PH, assuming generalized Riemann hypothesis.
- Where is NNL?

NNL vs. the Hardness Hypothesis of GCT

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant:

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof:

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] +

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof),

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr,

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo,

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety,

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety, we mean any variety

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety, we mean any variety whose coordinate ring has a set of generators

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety, we mean any variety whose coordinate ring has a set of generators that can be encoded succinctly and uniformly

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety, we mean any variety whose coordinate ring has a set of generators that can be encoded succinctly and uniformly by algebraic circuits

NNL vs. the Hardness Hypothesis of GCT

Theorem (GCT5)

NNL is P (ignoring a quasi prefix) iff a variant of the hardness hypothesis of GCT holds.

- The variant: Some exponential-time computable multilinear polynomial cannot be approximated infinitesimally closely by sub-exponential-size algebraic circuits.
- The proof: Classical algebraic geometry [Hilbert, ...] + algebraic complexity theory [Kaltofen and Trager (the crux of the proof), Heintz and Schnorr, Kabanets and Impagliazzo, Nisan and Wigderson].
- Analogous result holds, in general, for any explicit variety in place of $\Delta[\det, m]$.
- By an explicit variety, we mean any variety whose coordinate ring has a set of generators that can be encoded succinctly and uniformly by algebraic circuits of size polynomial in the dimension of the variety.

An Algorithmic Challenge

An Algorithmic Challenge

An Intermediate Problem:

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.
- If not, the task gets even harder.

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.
- If not, the task gets even harder.
- Hence bringing down NNL from PSPACE to PH would need overcoming the VP vs. $\overline{\mathrm{VP}}$ problem [the battleground of GCT], one way or the other.

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.
- If not, the task gets even harder.
- Hence bringing down NNL from PSPACE to PH would need overcoming the VP vs. $\overline{\mathrm{VP}}$ problem [the battleground of GCT], one way or the other.
- [GCT6]:

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.
- If not, the task gets even harder.
- Hence bringing down NNL from PSPACE to PH would need overcoming the VP vs. $\overline{\mathrm{VP}}$ problem [the battleground of GCT], one way or the other.
- [GCT6]: The $\mathrm{VP}_{\mathrm{ws}}$ vs. $\overline{\mathrm{VP}_{\mathrm{ws}}}$ problem is related to foundational issues in algebraic geometry and representation theory.

An Algorithmic Challenge

An Intermediate Problem:

Show that NNL is in PH (assuming only GRH).

- This is a challenge regardless of whether $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}_{\mathrm{ws}}$ or not.
- If $\overline{\mathrm{VP}_{\mathrm{ws}}} = \mathrm{VP}$, the challenge is to show this equality.
- If not, the task gets even harder.
- Hence bringing down NNL from PSPACE to PH would need overcoming the VP vs. $\overline{\mathrm{VP}}$ problem [the battleground of GCT], one way or the other.
- [GCT6]: The $\mathrm{VP}_{\mathrm{ws}}$ vs. $\overline{\mathrm{VP}_{\mathrm{ws}}}$ problem is related to foundational issues in algebraic geometry and representation theory.
- Hence bringing NNL to PH may need a deep synthesis and extension of the existing techniques of algebraic geometry, representation theory, and complexity theory.

The GCT chasm

The GCT chasm

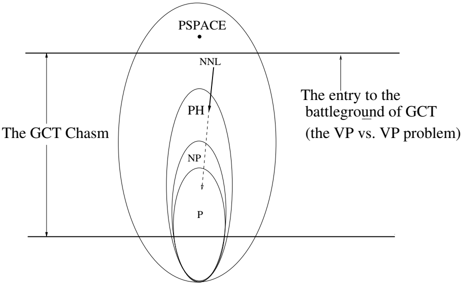
We call the existing PSPACE vs. P gap in the complexity of NNL
the GCT chasm

The GCT chasm

We call the existing PSPACE vs. P gap in the complexity of NNL the GCT chasm (revising the earlier definition in GCT5, thanks to [FS,GSS]).

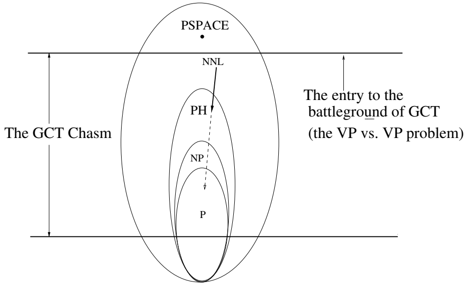
The GCT chasm

We call the existing PSPACE vs. P gap in the complexity of NNL the GCT chasm (revising the earlier definition in GCT5, thanks to [FS,GSS]).



The GCT chasm

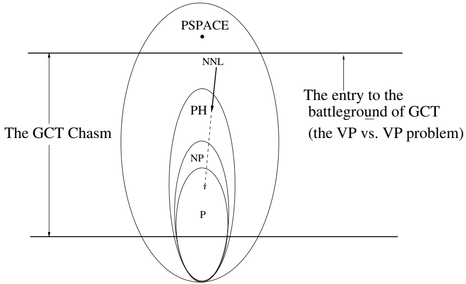
We call the existing PSPACE vs. P gap in the complexity of NNL the GCT chasm (revising the earlier definition in GCT5, thanks to [FS,GSS]).



- This GCT chasm will have to be crossed by any approach to the VP vs. VNP which also separates VNP from $\overline{\mathrm{VP}}$ in the process.

The GCT chasm

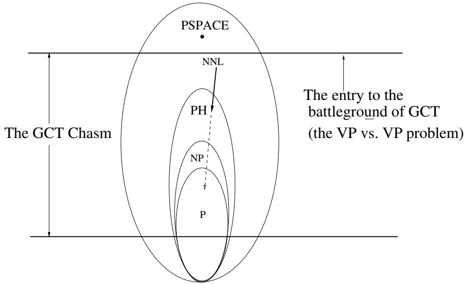
We call the existing PSPACE vs. P gap in the complexity of NNL the GCT chasm (revising the earlier definition in GCT5, thanks to [FS,GSS]).



- This GCT chasm will have to be crossed by any approach to the VP vs. VNP which also separates VNP from $\overline{\mathrm{VP}}$ in the process. Recall: By definition, any such approach is a GCT approach in a broad sense.

The GCT chasm

We call the existing PSPACE vs. P gap in the complexity of NNL the GCT chasm (revising the earlier definition in GCT5, thanks to [FS,GSS]).



- This GCT chasm will have to be crossed by any approach to the VP vs. VNP which also separates VNP from $\overline{\mathrm{VP}}$ in the process. Recall: By definition, any such approach is a GCT approach in a broad sense.
- GCT5,GCT6, and GCT7 provide a concrete GCT program to cross the GCT chasm.

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

This the first step of the GCT program [GCT5,GCT6,GCT7] to cross the GCT chasm.

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

This the first step of the GCT program [GCT5,GCT6,GCT7] to cross the GCT chasm.

A null-cone membership problem for V is a special case of this problem, which results when w is the origin.

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

This the first step of the GCT program [GCT5,GCT6,GCT7] to cross the GCT chasm.

A null-cone membership problem for V is a special case of this problem, which results when w is the origin.

Theorem (GCT5)

The orbit-closure intersection problem is in P, for any finite-dimensional representation V of a reductive group G, if

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

This the first step of the GCT program [GCT5,GCT6,GCT7] to cross the GCT chasm.

A null-cone membership problem for V is a special case of this problem, which results when w is the origin.

Theorem (GCT5)

The orbit-closure intersection problem is in P, for any finite-dimensional representation V of a reductive group G, if (1) the categorical quotient $V//G = spec(K[V]^G)$ is explicit,

The first step of the GCT program to cross the GCT chasm (The Orbit Closure Intersection Problem)

Let V be a finite-dimensional representation of a reductive group G (such as $SL_m(K)$).

Problem (The orbit closure intersection problem)

Given (V, G), and rational points $v, w \in V$, decide if the G-orbit-closures of v and w intersect.

This the first step of the GCT program [GCT5,GCT6,GCT7] to cross the GCT chasm.

A null-cone membership problem for V is a special case of this problem, which results when w is the origin.

Theorem (GCT5)

The orbit-closure intersection problem is in P, for any finite-dimensional representation V of a reductive group G, if (1) the categorical quotient $V//G = spec(K[V]^G)$ is explicit, and (2) the white-box PIT is in P.

The Orbit-Closure-Intersection Hypothesis

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].
  A concrete application of GCT:

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].
  A concrete application of GCT: This special case of the GCT hypothesis above implies a polynomial time algorithm for non-commutative rational identity testing.

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].
  A concrete application of GCT: This special case of the GCT hypothesis above implies a polynomial time algorithm for non-commutative rational identity testing.
- Holds if $V = K^{\binom{n}{2}}$ with the natural action of S_n

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].
  A concrete application of GCT: This special case of the GCT hypothesis above implies a polynomial time algorithm for non-commutative rational identity testing.
- Holds if $V = K^{\binom{n}{2}}$ with the natural action of S_n (Weighted Graph Isomorphism):

The Orbit-Closure-Intersection Hypothesis

Hypothesis (GCT5: M2012; M2017)

The orbit-closure intersection problem is in P, for any finite dimensional representation V of a reductive group G (possibly disconnected).

Expected to be an inherent difficulty underneath white-box PIT.

The status of the hypothesis:

- Holds if G is connected and $\dim(G)$ is constant [GCT5].
- Holds if $V = M_m(K)^n$, with the adjoint action of $G = SL_m(K)$ [GCT5 + Forbes and Shpilka][2012].
- Holds if $V = M_m(K)^n$, with the left-right action of $G = SL_m(K) \times SL_m(K)$ [GGOW; DM; IQS][2016].
  A concrete application of GCT: This special case of the GCT hypothesis above implies a polynomial time algorithm for non-commutative rational identity testing.
- Holds if $V = K^{\binom{n}{2}}$ with the natural action of S_n (Weighted Graph Isomorphism): [Babai][2017].

A special case of the hypothesis for finite groups

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles:

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1)

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1) Classification of all finite groups (not just finite simple groups) is not yet known.

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1) Classification of all finite groups (not just finite simple groups) is not yet known. In fact, this is the most outstanding open problem of finite group theory.

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1) Classification of all finite groups (not just finite simple groups) is not yet known. In fact, this is the most outstanding open problem of finite group theory. (2)

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1) Classification of all finite groups (not just finite simple groups) is not yet known. In fact, this is the most outstanding open problem of finite group theory. (2) the complexity of constructing irreducible representations of finite simple groups of Lie type (using the l-adic cohomology as per Grothendieck) is very high.

A special case of the hypothesis for finite groups

The Orbit Equality Problem:

Show that the problem of deciding, given any representation V of a finite group G and two rational points $v, w \in V$, whether v and w lie in the same G-orbit belongs to P.

- This is a special case of the orbit-closure-intersection problem for finite groups.
- The main obstacles: (1) Classification of all finite groups (not just finite simple groups) is not yet known. In fact, this is the most outstanding open problem of finite group theory. (2) the complexity of constructing irreducible representations of finite simple groups of Lie type (using the l-adic cohomology as per Grothendick) is very high.
- This is why the techniques such as operator scaling and optimization are unlikely to work for white-box PIT.

An overview of the GCT program

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT),

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008].

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]).

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier:

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P.

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5]

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk]

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]:

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]: Show that the problem NNL for the categorical quotient $V//G$ is in P, for any finite dimensional representation V of any reductive group G.

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]: Show that the problem NNL for the categorical quotient $V//G$ is in P, for any finite dimensional representation V of any reductive group G.
- Easiest [GCT5]

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]: Show that the problem NNL for the categorical quotient $V//G$ is in P, for any finite dimensional representation V of any reductive group G.
- Easiest [GCT5] [Covered in this talk]

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]: Show that the problem NNL for the categorical quotient $V//G$ is in P, for any finite dimensional representation V of any reductive group G.
- Easiest [GCT5] [Covered in this talk] [An inherent difficulty underneath white-box PIT]:

An overview of the GCT program

- Hardest: Prove that $\mathrm{VNP} \not\subseteq \overline{\mathrm{VP}}$ (the hardness hypothesis of GCT), using obstructions [GCT2:MS2008]. (Occurence obstructions do not exist [Bürgisser, Ikenmeyer, Panova]). GCT7: a systematic program to prove existence of multiplicity obstructions.
- Easier: Show that the problem NNL for general explicit varieties is in P. GCT5,6,7: a systematic program for this.
- Much easier [GCT5] [Not covered in this talk] [An inherent difficulty underneath black-box PIT]: Show that the problem NNL for the categorical quotient $V//G$ is in P, for any finite dimensional representation V of any reductive group G.
- Easiest [GCT5] [Covered in this talk] [An inherent difficulty underneath white-box PIT]: Show that the orbit-closure intersection problem is in P, for any finite dimensional representation V of any reductive group G (possibly disconnected).

Thank you.