The GCT chasm II

Ketan D. Mulmuley

The University of Chicago

The main reference

GCT5 [M.]: Geometric Complexity Theory V: Equivalence between black-box derandomization of polynomial identity testing and derandomization of Noether's Normalization Lemma

Abstract: FOCS 2012.

Full version: Arxiv and the home page.

Summary of yesterday's tutorial

Summary of yesterday's tutorial

Negative conclusion (yesterday) If NNL is not in SUBEXP then under reasonable assumptions $VP = VNP$, $NP \subseteq P/poly$, and so on.

Summary of yesterday's tutorial

Negative conclusion (yesterday) If NNL is not in SUBEXP then under reasonable assumptions $VP = VNP$, $NP \subseteq P/poly$, and so on.

The positive view of GCT: The GCT chasm is not an evidence against these conjectures bur rather a measure of their difficulty.

Summary of yesterday's tutorial

Negative conclusion (yesterday) If NNL is not in SUBEXP then under reasonable assumptions $VP = VNP$, $NP \subseteq P/poly$, and so on.

The positive view of GCT: The GCT chasm is not an evidence against these conjectures bur rather a measure of their difficulty.

Positive conclusion: Under reasonable assumptions (including the robustness thesis), any proof of the $VP \neq VNP$ conjecture would need to produce a hitting set $\mathcal{B} = \{B_1, \ldots, B_l\}$ (a set of matrices) against the polynomials with exponential circuit size in the orbit closure $\Delta[\mathrm{det}, m]$ in sub-exponential time.

Intermediate questions: today

Question: To begin with, can we derandomize Noether's Normalization Lemma for some intermediate explicit varieties in which the border issues do not arise?

Intermediate questions: today

Question: To begin with, can we derandomize Noether's Normalization Lemma for some intermediate explicit varieties in which the border issues do not arise?

Yes (up to a quasi-prefix). This talk.

Intermediate questions: today

Question: To begin with, can we derandomize Noether's Normalization Lemma for some intermediate explicit varieties in which the border issues do not arise?

Yes (up to a quasi-prefix). This talk.

More basic question: Can the foundational Equivalence Problem of invariant theory (cf. Klein's Erlangen program) be solved explicitly?

Intermediate questions: today

Question: To begin with, can we derandomize Noether's Normalization Lemma for some intermediate explicit varieties in which the border issues do not arise?

Yes (up to a quasi-prefix). This talk.

More basic question: Can the foundational Equivalence Problem of invariant theory (cf. Klein's Erlangen program) be solved explicitly?

Yes, in some fundamental special cases, including the one that was the focus of Hilbert's paper. This talk.

The Equivalence Problem

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$.
Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V.

The Equivalence Problem

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V.

Call a polynomial $f(v) \in \mathbb{C}[V]$ invariant if $f(\sigma^{-1}v) = f(v)$ for all $\sigma \in G$. Let $\mathbb{C}[V]^G \subseteq \mathbb{C}[V]$ denote the sub-ring of invariants.

The Equivalence Problem

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V.

Call a polynomial $f(v) \in \mathbb{C}[V]$ invariant if $f(\sigma^{-1}v) = f(v)$ for all $\sigma \in G$. Let $\mathbb{C}[V]^G \subseteq \mathbb{C}[V]$ denote the sub-ring of invariants.

Call two points $v, w \in V$ equivalent if for every invariant $f \in \mathbb{C}[V]$, $f(v) = f(w)$, which is so iff $\overline{Gv} \cap \overline{Gw} \neq \emptyset$.

The Equivalence Problem

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V.

Call a polynomial $f(v) \in \mathbb{C}[V]$ invariant if $f(\sigma^{-1}v) = f(v)$ for all $\sigma \in G$. Let $\mathbb{C}[V]^G \subseteq \mathbb{C}[V]$ denote the sub-ring of invariants.

Call two points $v, w \in V$ equivalent if for every invariant $f \in \mathbb{C}[V]$, $f(v) = f(w)$, which is so iff $\overline{Gv} \cap \overline{Gw} \neq \emptyset$.

The Problem EQUIVALENCE: Given V and G, and two (rational) points v and w, decide if they are equivalent.

The Equivalence Problem

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V.

Call a polynomial $f(v) \in \mathbb{C}[V]$ invariant if $f(\sigma^{-1}v) = f(v)$ for all $\sigma \in G$. Let $\mathbb{C}[V]^G \subseteq \mathbb{C}[V]$ denote the sub-ring of invariants.

Call two points $v, w \in V$ equivalent if for every invariant $f \in \mathbb{C}[V]$, $f(v) = f(w)$, which is so iff $\overline{Gv} \cap \overline{Gw} \neq \emptyset$.

The Problem EQUIVALENCE: Given V and G, and two (rational) points v and w, decide if they are equivalent.

The basic problem in Klein's Erlangen program.

The history of EQUIVALENCE

(1) Hilbert [1890]: $\mathbb{C}[V]^G$ is finitely generated (non-constructive proof). This implies that EQUIVALENCE has a finite (non-uniform) circuit. “Mythology” [Gordon].

The history of EQUIVALENCE

(1) Hilbert [1890]: $\mathbb{C}[V]^G$ is finitely generated (non-constructive proof). This implies that EQUIVALENCE has a finite (non-uniform) circuit. "Mythology" [Gordon].

(2) Hilbert [1893]: An algorithm for constructing a finite set of generators for $\mathbb{C}[V]^G$. This implies that EQUIVALENCE is decidable. This was not known before Hilbert even for $m = 3$.

The history of EQUIVALENCE

(1) Hilbert [1890]: $\mathbb{C}[V]^G$ is finitely generated (non-constructive proof). This implies that EQUIVALENCE has a finite (non-uniform) circuit. “Mythology” [Gordon].

(2) Hilbert [1893]: An algorithm for constructing a finite set of generators for $\mathbb{C}[V]^G$. This implies that EQUIVALENCE is decidable. This was not known before Hilbert even for $m = 3$.

(3) Popov [1982]: Explicit upper bound on the running time of Hilbert’s algorithm.

The history of EQUIVALENCE

(1) Hilbert [1890]: $\mathbb{C}[V]^G$ is finitely generated (non-constructive proof). This implies that EQUIVALENCE has a finite (non-uniform) circuit. “Mythology” [Gordon].

(2) Hilbert [1893]: An algorithm for constructing a finite set of generators for $\mathbb{C}[V]^G$. This implies that EQUIVALENCE is decidable. This was not known before Hilbert even for $m = 3$.

(3) Popov [1982]: Explicit upper bound on the running time of Hilbert’s algorithm.

(4) Derksen[2001]: EQUIVALENCE is in PSPACE. The bound is the same even for constant m.

EQUIVALENCE is in DET for constant m

Theorem [GCT5]: EQUIVALENCE is in $DET \subseteq NC \subseteq P$ if m is constant.

EQUIVALENCE is in DET for constant m

Theorem [GCT5]: EQUIVALENCE is in $DET \subseteq NC \subseteq P$ if m is constant.

History: m is constant

Hilbert[1890]: Finite non−uniform algorithm [Mythology: Gordon]

$\downarrow$

Hilbert[1893]: Decidable, without an explicit upper bound on the time

$\downarrow$

Popov[1982]: An explicit upper bound on the time

$\downarrow$

Derksen[2001]; Grobner basis theory [Mayr et al. 2011]: Belongs to PSPACE

$\downarrow$

GCT5[2012]: Belongs to DET.

Towards a high-level picture of the proof

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$, and $R = \mathbb{C}[V]^G$ the ring of invariants. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V. Let $f_1, \ldots, f_l \in R$ be a finite set of generators of R (which exists by Hilbert).

Towards a high-level picture of the proof

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$, and $R = \mathbb{C}[V]^G$ the ring of invariants. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V. Let $f_1, \ldots, f_l \in R$ be a finite set of generators of R (which exists by Hilbert).

Defn [GCT5]: We say that an explicit FFT (First Fundamental Theorem) holds for R if there exists a poly(n, m)-time computable circuit C (with rational constants) over the variables v and an auxiliary set $x = (x_1, \ldots, x_l)$, $l =$ poly(n), of variables such that the polynomial $C(v, x)$ computed by this circuit can be expressed as $C(v, x) = \sum_\alpha f_\alpha(v) x_\alpha$, where $f_\alpha(v)$'s generate the ring R.

Towards a high-level picture of the proof

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$, and $R = \mathbb{C}[V]^G$ the ring of invariants. Let $v = (v_1, \ldots, v_n)$ be the coordinate functions of V. Let $f_1, \ldots, f_l \in R$ be a finite set of generators of R (which exists by Hilbert).

Defn [GCT5]: We say that an explicit FFT (First Fundamental Theorem) holds for R if there exists a poly(n, m)-time computable circuit C (with rational constants) over the variables v and an auxiliary set $x = (x_1, \ldots, x_l)$, $l =$ poly(n), of variables such that the polynomial $C(v, x)$ computed by this circuit can be expressed as $C(v, x) = \sum_\alpha f_\alpha(v) x_\alpha$, where $f_\alpha(v)$'s generate the ring R.

The number of f_α's can be exponential.

Example 1: The ring of vector invariants

Let $V = (\mathbb{C}^m)^{\oplus r}$, with the left action of $G = SL_m(\mathbb{C})$. Let Z be a variable $m \times r$ matrix whose entries are coordinates of V.

Example 1: The ring of vector invariants

Let $V = (\mathbb{C}^m)^{\oplus r}$, with the left action of $G = SL_m(\mathbb{C})$. Let Z be a variable $m \times r$ matrix whose entries are coordinates of V.

First Fundamental Theorem (Weyl): The ring $\mathbb{C}[V]^G$ is generated by the principle $m \times m$ minors of Z.

Example 1: The ring of vector invariants

Let $V = (\mathbb{C}^m)^{\oplus r}$, with the left action of $G = SL_m(\mathbb{C})$. Let Z be a variable $m \times r$ matrix whose entries are coordinates of V.

First Fundamental Theorem (Weyl): The ring $\mathbb{C}[V]^G$ is generated by the principle $m \times m$ minors of Z.

Let $Z_1, \ldots, Z_r$ denote the columns of Z. Let $x = \{x_{ij}\}$, $1 \leq i \leq m$, $1 \leq j \leq r$, be a set of auxiliary variables. Let $F(Z, x) = \det([\sum_j x_{1,j} Z_j, \ldots, \sum_j x_{m,j} Z_j])$.

Example 1: The ring of vector invariants

Let $V = (\mathbb{C}^m)^{\oplus r}$, with the left action of $G = SL_m(\mathbb{C})$. Let Z be a variable $m \times r$ matrix whose entries are coordinates of V.

First Fundamental Theorem (Weyl): The ring $\mathbb{C}[V]^G$ is generated by the principle $m \times m$ minors of Z.

Let $Z_1, \ldots, Z_r$ denote the columns of Z. Let $x = \{x_{ij}\}$, $1 \leq i \leq m$, $1 \leq j \leq r$, be a set of auxiliary variables. Let $F(Z, x) = \det([\sum_j x_{1,j} Z_j, \ldots, \sum_j x_{m,j} Z_j])$.

Then the coefficients of $F(Z, x)$, considered as a polynomial in x, generate the ring $\mathbb{C}[V]^G$. Furthermore, the polynomial $F(Z, x)$ has a small poly(m, r)-time computable circuit.

Example 2: The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$, with the adjoint action of $G = SL_m(\mathbb{C})$. Let $U = (U_1, \ldots, U_r)$ be a tuple of $m \times m$ variable matrices whose entries are coordinate functions of V.

Example 2: The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$, with the adjoint action of $G = SL_m(\mathbb{C})$. Let $U = (U_1, \ldots, U_r)$ be a tuple of $m \times m$ variable matrices whose entries are coordinate functions of V.

First Fundamental Theorem [Procesi-Razmyslov]: The ring $\mathbb{C}[V]^G$ is generated by traces of the form trace$(U_{i_1} \cdots U_{i_l})$, $l \leq m^2$, $i_1, \ldots, i_l \in [r]$.

Example 2: The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$, with the adjoint action of $G = SL_m(\mathbb{C})$. Let $U = (U_1, \ldots, U_r)$ be a tuple of $m \times m$ variable matrices whose entries are coordinate functions of V.

First Fundamental Theorem [Procesi-Razmyslov]: The ring $\mathbb{C}[V]^G$ is generated by traces of the form trace$(U_{i_1} \cdots U_{i_l})$, $l \leq m^2$, $i_1, \ldots, i_l \in [r]$.

Let $y = (y_1, \ldots, y_l)$ be a set of auxiliary variables. Let $F_l(U, y) =$ trace$(\prod_{j=1}^{l} (\sum_{i=1}^{r} y_j^i U_i))$. It follows that the coefficients of $F_l(U, y)$'s, $1 \leq l \leq m^2$, considered as polynomials in y, generate $\mathbb{C}[V]^G$. Furthermore, $F_l(U, y)$'s have small poly(m, r)-time computable circuits.

Example 2: The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$, with the adjoint action of $G = SL_m(\mathbb{C})$. Let $U = (U_1, \ldots, U_r)$ be a tuple of $m \times m$ variable matrices whose entries are coordinate functions of V.

First Fundamental Theorem [Procesi-Razmyslov]: The ring $\mathbb{C}[V]^G$ is generated by traces of the form trace$(U_{i_1} \cdots U_{i_l})$, $l \leq m^2$, $i_1, \ldots, i_l \in [r]$.

Let $y = (y_1, \ldots, y_l)$ be a set of auxiliary variables. Let $F_l(U, y) =$ trace$(\prod_{j=1}^{l} (\sum_{i=1}^{r} y_j^i U_i))$. It follows that the coefficients of $F_l(U, y)$'s, $1 \leq l \leq m^2$, considered as polynomials in y, generate $\mathbb{C}[V]^G$. Furthermore, $F_l(U, y)$'s have small poly(m, r)-time computable circuits. Such circuits are called ROABP's [FS2012].

Explicit FFT for constant m

Let V be any n-dimensional representation of $G = SL_m(\mathbb{C})$, m constant, with coordinate functions $v = (v_1, \ldots, v_n)$.

Explicit FFT for constant m

Let V be any n-dimensional representation of $G = SL_m(\mathbb{C})$, m constant, with coordinate functions $v = (v_1, \ldots, v_n)$.

Call a circuit $C(x)$, $x = (x_1, \ldots, x_l)$, a diagonal depth three circuit if it computes a polynomial of the form $\sum_{i=1}^{s} l_i(x)^{d_i}$, where $l_i(x)$ are linear functions in x.

Explicit FFT for constant m

Let V be any n-dimensional representation of $G = SL_m(\mathbb{C})$, m constant, with coordinate functions $v = (v_1, \ldots, v_n)$.

Call a circuit $C(x)$, $x = (x_1, \ldots, x_l)$, a diagonal depth three circuit if it computes a polynomial of the form $\sum_{i=1}^{s} l_i(x)^{d_i}$, where $l_i(x)$ are linear functions in x.

Theorem [GCT5]: Explicit FFT holds for $\mathbb{C}[V]^G$ if m is constant.

Explicit FFT for constant m

Let V be any n-dimensional representation of $G = SL_m(\mathbb{C})$, m constant, with coordinate functions $v = (v_1, \ldots, v_n)$.

Call a circuit $C(x)$, $x = (x_1, \ldots, x_l)$, a diagonal depth three circuit if it computes a polynomial of the form $\sum_{i=1}^{s} l_i(x)^{d_i}$, where $l_i(x)$ are linear functions in x.

Theorem [GCT5]: Explicit FFT holds for $\mathbb{C}[V]^G$ if m is constant.

More strongly, one can compute in poly(n, m) time a diagonal depth three circuit $C(v, x)$ (considered as a polynomial in x with coefficients in $\mathbb{C}[V]$), such that the coefficients of $C(v, x)$, considered as a polynomial in x as above, generate $\mathbb{C}[V]^G$.

Proof ingredients

Geometric invariant theory: Cayley; Hilbert; Mumford; Popov; Derksen.

Proof ingredients

Geometric invariant theory: Cayley; Hilbert; Mumford; Popov; Derksen.

Standard monomial theory: Doubillet, Rota, Stein; ...

Proof ingredients

Geometric invariant theory: Cayley; Hilbert; Mumford; Popov; Derksen.

Standard monomial theory: Doubillet, Rota, Stein; ...

Algebraic complexity theory: Strassen; Valiant et al.; Csanky; Malod, Portier; ..

Proof ingredients

Geometric invariant theory: Cayley; Hilbert; Mumford; Popov; Derksen.

Standard monomial theory: Doubillet, Rota, Stein; ...

Algebraic complexity theory: Strassen; Valiant et al.; Csanky; Malod, Portier; ..

Basic proof idea: Efficient implementation of the Raynold's operator (in the form of Cayley's Ω-process) and efficient implementation of standard monomial theory via algebraic complexity theory.

The high level proof

Theorem [recall]: EQUIVALENCE is in DET if m is constant

The high level proof

Theorem [recall]: EQUIVALENCE is in DET if m is constant

(1): By the explicit FFT for constant m, we can compute fast (using a DET-algorithm) a diagonal depth three circuit $C(v, x)$ such that the coefficients of $C(v, x)$, considered as a polynomial in x over the ring $\mathbb{C}[V]$, generate $\mathbb{C}[V]^G$.

The high level proof

Theorem [recall]: EQUIVALENCE is in DET if m is constant

(1): By the explicit FFT for constant m, we can compute fast (using a DET-algorithm) a diagonal depth three circuit $C(v, x)$ such that the coefficients of $C(v, x)$, considered as a polynomial in x over the ring $\mathbb{C}[V]$, generate $\mathbb{C}[V]^G$.

(2): [The basic connection between EQUIVALENCE and Polynomial Identity Testing (PIT)]: This implies that, given two points $a, b \in V$, a and b are equivalent iff $C(a, x) - C(b, x)$ is identically zero as a polynomial.

The high level proof

Theorem [recall]: EQUIVALENCE is in DET if m is constant

(1): By the explicit FFT for constant m, we can compute fast (using a DET-algorithm) a diagonal depth three circuit $C(v, x)$ such that the coefficients of $C(v, x)$, considered as a polynomial in x over the ring $\mathbb{C}[V]$, generate $\mathbb{C}[V]^G$.

(2): [The basic connection between EQUIVALENCE and Polynomial Identity Testing (PIT)]: This implies that, given two points $a, b \in V$, a and b are equivalent iff $C(a, x) - C(b, x)$ is identically zero as a polynomial.

(3): Polynomial identity testing (white-box) for diagonal depth three circuits is in DET: Arvind, Joglekar, Srinivasan [2009].

The problem NNL for invariant rings

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$.
Let $R = \mathbb{C}[V]^G$ be the invariant ring.

The problem NNL for invariant rings

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $R = \mathbb{C}[V]^G$ be the invariant ring.

Noether's Normalization Lemma: There exists a small homogeneous $S \subseteq R$ of poly(n) cardinality such that R is integral over the subring generated by S. (A random small S works).

The problem NNL for invariant rings

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$. Let $R = \mathbb{C}[V]^G$ be the invariant ring.

Noether's Normalization Lemma: There exists a small homogeneous $S \subseteq R$ of poly(n) cardinality such that R is integral over the subring generated by S. (A random small S works).

The problem NNL for R: Construct such a small S, given V and G in the standard specification.

The problem NNL for invariant rings

Let V be an n-dimensional representation of $G = SL_m(\mathbb{C})$.
Let $R = \mathbb{C}[V]^G$ be the invariant ring.

Noether's Normalization Lemma: There exists a small homogeneous $S \subseteq R$ of poly(n) cardinality such that R is integral over the subring generated by S. (A random small S works).

The problem NNL for R: Construct such a small S, given V and G in the standard specification.

We say that NNL for R is derandomized if such a small S can be constructed explicitly (in poly(n, m) time) given V and G in the standard representation.

The significance of derandomizing NNL: I

The wild problem of representation theory: Classify G-orbits in V “explicitly”.

The significance of derandomizing NNL: I

The wild problem of representation theory: Classify G-orbits in V "explicitly".

Given $v \in V$, let $[v]$ denote the class of points equivalent to v.

The significance of derandomizing NNL: I

The wild problem of representation theory: Classify G-orbits in V “explicitly”.

Given $v \in V$, let $[v]$ denote the class of points equivalent to v.

Coarser Moduli problem [cf. Mumford] (cf. Klein’s program): Classify the equivalence classes $[v]$ “explicitly”.

The significance of derandomizing NNL: I

The wild problem of representation theory: Classify G-orbits in V "explicitly".

Given $v \in V$, let $[v]$ denote the class of points equivalent to v.

Coarser Moduli problem [cf. Mumford] (cf. Klein's program): Classify the equivalence classes $[v]$ "explicitly".

Derandomization of NNL implies an explicit solution to this problem.

The significance of derandomizing NNL: I

The wild problem of representation theory: Classify G-orbits in V "explicitly".

Given $v \in V$, let $[v]$ denote the class of points equivalent to v.

Coarser Moduli problem [cf. Mumford] (cf. Klein's program): Classify the equivalence classes $[v]$ "explicitly".

Derandomization of NNL implies an explicit solution to this problem.

How?: Next.

The significance of derandomizing NNL: II

Suppose NNL for $R = \mathbb{C}[V]^G$ can be derandomized.

The significance of derandomizing NNL: II

Suppose NNL for $R = \mathbb{C}[V]^G$ can be derandomized.

Let $S = \{s_1, \ldots, s_l\} \subseteq R$, $l =$ poly(m,n), be an explicit small poly(n,m)-time computable subset such that R is integral over the subring generated by S.

The significance of derandomizing NNL: II

Suppose NNL for $R = \mathbb{C}[V]^G$ can be derandomized.

Let $S = \{s_1, \ldots, s_l\} \subseteq R$, $l =$ poly(m, n), be an explicit small poly(n, m)-time computable subset such that R is integral over the subring generated by S.

We assume that each element s_i of S is represented by a circuit (with rational constants) over the coordinates $v = (v_1, \ldots, v_n)$ of V.

The significance of derandomizing NNL: II

Suppose NNL for $R = \mathbb{C}[V]^G$ can be derandomized.

Let $S = \{s_1, \ldots, s_l\} \subseteq R$, $l =$ poly(m, n), be an explicit small poly(n, m)-time computable subset such that R is integral over the subring generated by S.

We assume that each element s_i of S is represented by a circuit (with rational constants) over the coordinates $v = (v_1, \ldots, v_n)$ of V.

Let $\pi_S : V \to \mathbb{C}^l$ denote the map $v \to (s_1(v), \ldots, s_l(v))$.

The significance of derandomizing NNL: II

Suppose NNL for $R = \mathbb{C}[V]^G$ can be derandomized.

Let $S = \{s_1, \ldots, s_l\} \subseteq R$, $l =$ poly(m, n), be an explicit small poly(n, m)-time computable subset such that R is integral over the subring generated by S.

We assume that each element s_i of S is represented by a circuit (with rational constants) over the coordinates $v = (v_1, \ldots, v_n)$ of V.

Let $\pi_S : V \to \mathbb{C}^l$ denote the map $v \to (s_1(v), \ldots, s_l(v))$.

If S is explicit, then the map π_S is also explicit (i.e., can be computed in polynomial time on rational v's).

The significance of derandomizing NNL: III

FACT: (1): The image of $\pi_S : V \to \mathbb{C}^l$ is a closed subvariety of $\mathbb{C}^l$.

The significance of derandomizing NNL: III

FACT: (1): The image of $\pi_S : V \to \mathbb{C}^l$ is a closed subvariety of $\mathbb{C}^l$.

(2): The points of $V/G[S] :=$ Image(π_S) are in one-to-one correspondence with the equivalences classes $[v]$.

The significance of derandomizing NNL: III

FACT: (1): The image of $\pi_S : V \to \mathbb{C}^l$ is a closed subvariety of $\mathbb{C}^l$.

(2): The points of $V/G[S] :=$ Image(π_S) are in one-to-one correspondence with the equivalences classes $[v]$.

(3): This implies explicit classification (parametrization) of $[v]$'s because the map π_S is polynomial-time-computable on rational points.

The significance of derandomizing NNL: III

FACT: (1): The image of $\pi_S : V \to \mathbb{C}^l$ is a closed subvariety of $\mathbb{C}^l$.

(2): The points of $V/G[S] :=$ Image(π_S) are in one-to-one correspondence with the equivalences classes $[v]$.

(3): This implies explicit classification (parametrization) of $[v]$'s because the map π_S is polynomial-time-computable on rational points.

In contrast, the Hilbert-Mumford map $\pi_{V/G} : V \to \mathbb{C}^k$ given by $v \to (f_1(v), \ldots, f_k(v))$, where $F = \{f_1, \ldots, f_k\}$ is a generating set of $\mathbb{C}[V]^G$, is not explicit.

The NNL for V/G for constant m

Theorem 2 [GCT5]: The NNL for V/G is in quasi-DET if m is constant.

The NNL for V/G for constant m

Theorem 2 [GCT5]: The NNL for V/G is in quasi-DET if m is constant.

Follows from geometric invariant theory, explicit FFT for constant m (the earlier theorem), and quasi-black-box derandomization of PIT for diagonal depth three circuits [Shpilka-Volkovitch 2009; Agrawal-Saha-Saxena 2012].

The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$ with the adjoint action of $G = SL_m(\mathbb{C})$.

The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$ with the adjoint action of $G = SL_m(\mathbb{C})$.

Theorem1 [GCT5] The NNL for V/G can be derandomized if Symbolic Determinant Identity Testing has black-box derandomization.

The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$ with the adjoint action of $G = SL_m(\mathbb{C})$.

Theorem1 [GCT5] The NNL for V/G can be derandomized if Symbolic Determinant Identity Testing has black-box derandomization.

Theorem2 [Forbes and Shpilka 2012] PIT for ROABP has black-box derandomization.

The ring of matrix invariants

Let $V = M_m(\mathbb{C})^r$ with the adjoint action of $G = SL_m(\mathbb{C})$.

Theorem1 [GCT5] The NNL for V/G can be derandomized if Symbolic Determinant Identity Testing has black-box derandomization.

Theorem2 [Forbes and Shpilka 2012] PIT for ROABP has black-box derandomization.

Variant of Theorem 1 for ROABP's, in conjunction with Theorem 2, implies:

Theorem: NNL for V/G can be quasi-derandomized unconditionally.

Consequence in the context of wild problems

Theorem: The equivalence classes $[v]$, $v \in M_m(\mathbb{C})$, can be parametrized quasi-explicitly.

Consequence in the context of wild problems

Theorem: The equivalence classes $[v]$, $v \in M_m(\mathbb{C})$, can be parametrized quasi-explicitly.

In contrast, classifying the G-orbits Gv's, $G = SL_m(\mathbb{C})$, is the wild problem of representation theory.

Consequence in the context of wild problems

Theorem: The equivalence classes $[v]$, $v \in M_m(\mathbb{C})$, can be parametrized quasi-explicitly.

In contrast, classifying the G-orbits Gv's, $G = SL_m(\mathbb{C})$, is the wild problem of representation theory.

Conjecture [GCT5]: Explicit FFT holds for arbitrary V/G, and NNL can also be derandomized for any V/G.

Consequence in the context of wild problems

Theorem: The equivalence classes $[v]$, $v \in M_m(\mathbb{C})$, can be parametrized quasi-explicitly.

In contrast, classifying the G-orbits Gv's, $G = SL_m(\mathbb{C})$, is the wild problem of representation theory.

Conjecture [GCT5]: Explicit FFT holds for arbitrary V/G, and NNL can also be derandomized for any V/G.

The fundamental difference between V/G and $\Delta[\det, m]$:

Consequence in the context of wild problems

Theorem: The equivalence classes $[v]$, $v \in M_m(\mathbb{C})$, can be parametrized quasi-explicitly.

In contrast, classifying the G-orbits Gv's, $G = SL_m(\mathbb{C})$, is the wild problem of representation theory.

Conjecture [GCT5]: Explicit FFT holds for arbitrary V/G, and NNL can also be derandomized for any V/G.

The fundamental difference between V/G and $\Delta[\det, m]$: $\Delta[\det, m]$ has conjecturally bad exterior points. In contrast, by Hilbert-Mumford, the map $\pi_{V/G} : V \to V/G$ is surjective. So provably it has no exterior points.

The GCT program

GCT6: An approach to cross the GCT chasm via a series of intermediate upper bound problems in algebraic geometry and representation theory, such as:

The GCT program

GCT6: An approach to cross the GCT chasm via a series of intermediate upper bound problems in algebraic geometry and representation theory, such as:

The KRONECKER problem: Given three partitions α, β, λ decide if the Kronecker coefficient $k^{\lambda}_{\alpha,\beta}$ is non-zero.

The GCT program

GCT6: An approach to cross the GCT chasm via a series of intermediate upper bound problems in algebraic geometry and representation theory, such as:

The KRONECKER problem: Given three partitions α, β, λ decide if the Kronecker coefficient $k_{\alpha,\beta}^{\lambda}$ is non-zero.

Conjecture [GCT6]: KRONECKER is in P, if α, β and λ are given in binary, and in DET if they are given in unary. Furthermore, $k_{\alpha,\beta}^{\lambda}$ has a positive ($\#P$-) formula.

The GCT program

GCT6: An approach to cross the GCT chasm via a series of intermediate upper bound problems in algebraic geometry and representation theory, such as:

The KRONECKER problem: Given three partitions α, β, λ decide if the Kronecker coefficient $k^{\lambda}_{\alpha,\beta}$ is non-zero.

Conjecture [GCT6]: KRONECKER is in P, if α, β and λ are given in binary, and in DET if they are given in unary. Furthermore, $k^{\lambda}_{\alpha,\beta}$ has a positive ($\#P$-) formula.

The next session on Kronecker coefficients and positivity.

Thank you.