The GCT chasm I

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.

The beginning of GCT

Theorem:[M., 1993] The MAXFLOW problem cannot be solved in the PRAM model without bit operations in polylog(N) time using poly(N) processors, where N denotes the total bit-length of the input.

The beginning of GCT

Theorem:[M., 1993] The MAXFLOW problem cannot be solved in the PRAM model without bit operations in polylog(N) time using poly(N) processors, where N denotes the total bit-length of the input.

The only known non-trivial implication of the fundamental uniform Boolean $P \neq NC$ conjecture that can be proved unconditionally in a model of computation in which the determinant can be computed efficiently.

The beginning of GCT

Theorem:[M., 1993] The MAXFLOW problem cannot be solved in the PRAM model without bit operations in polylog(N) time using poly(N) processors, where N denotes the total bit-length of the input.

The only known non-trivial implication of the fundamental uniform Boolean $P \neq NC$ conjecture that can be proved unconditionally in a model of computation in which the determinant can be computed efficiently.

The proof is geometric and goes via upper bound techniques [the flip].

The beginning of GCT

Theorem:[M., 1993] The MAXFLOW problem cannot be solved in the PRAM model without bit operations in polylog(N) time using poly(N) processors, where N denotes the total bit-length of the input.

The only known non-trivial implication of the fundamental uniform Boolean $P \neq NC$ conjecture that can be proved unconditionally in a model of computation in which the determinant can be computed efficiently.

The proof is geometric and goes via upper bound techniques [the flip].

Why is improving on this lower bound so difficult? This talk.

The permanent vs. determinant problem

Conjecture [Valiant 1979]: The permanent of an $n \times n$ variable matrix X cannot be expressed as a symbolic determinant of size m, i.e., as the determinant of an $m \times m$ matrix whose entries are linear functions of the entries of X, if $m = \text{poly}(n)$.

The permanent vs. determinant problem

Conjecture [Valiant 1979]: The permanent of an $n \times n$ variable matrix X cannot be expressed as a symbolic determinant of size m, i.e., as the determinant of an $m \times m$ matrix whose entries are linear functions of the entries of X, if $m = \text{poly}(n)$.

Almost equivalently: VP $\neq$ VNP.

The permanent vs. determinant problem

Conjecture [Valiant 1979]: The permanent of an $n \times n$ variable matrix X cannot be expressed as a symbolic determinant of size m, i.e., as the determinant of an $m \times m$ matrix whose entries are linear functions of the entries of X, if $m = \text{poly}(n)$.

Almost equivalently: VP $\neq$ VNP.

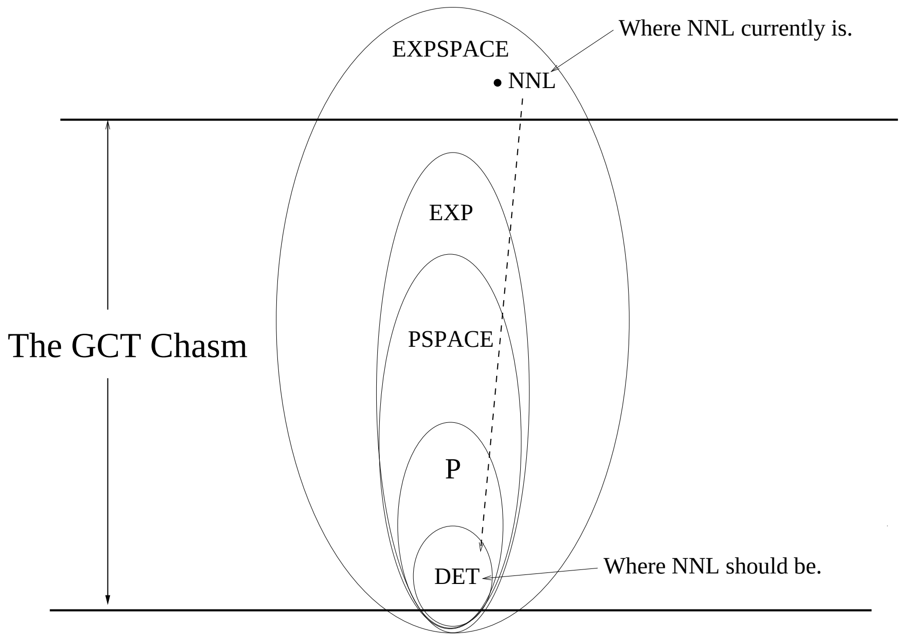
Stronger conjecture:[GCT1: M., Sohoni; 2001] The permanent of an $n \times n$ variable matrix X cannot be approximated infinitesimally closely by symbolic determinants of $O(\text{poly}(n))$ or even $O(2^{n^\epsilon})$ size, for some small enough constant $\epsilon > 0$.

The main result

Theorem [GCT5]: The stronger GCT1-conjecture implies that the problem (NNL) of derandomizing Noether's Normalization Lemma for the orbit closure of the determinant can be brought down from EXPSPACE, where it currently is, to DET $\subseteq P$, up to quasi-prefix.

The main result

Theorem [GCT5]: The stronger GCT1-conjecture implies that the problem (NNL) of derandomizing Noether's Normalization Lemma for the orbit closure of the determinant can be brought down from EXPSPACE, where it currently is, to DET $\subseteq P$, up to quasi-prefix.



What if the GCT chasm cannot be crossed?

Theorem:
Suppose NNL is not in SUBEXP.

What if the GCT chasm cannot be crossed?

Theorem:
Suppose NNL is not in SUBEXP.

Then assuming GRH and robustness of Valiant's conjecture (i.e., $(VNP \neq VP) \Longrightarrow (VNP \not\subseteq \overline{VP})$):

What if the GCT chasm cannot be crossed?

Theorem:
Suppose NNL is not in SUBEXP.

Then assuming GRH and robustness of Valiant's conjecture (i.e., $(VNP \neq VP) \implies (VNP \not\subseteq \overline{VP})$):

(1) $NP \subseteq P/poly$.

What if the GCT chasm cannot be crossed?

Theorem:
Suppose NNL is not in SUBEXP.

Then assuming GRH and robustness of Valiant's conjecture (i.e., $(VNP \neq VP) \implies (VNP \not\subseteq \overline{VP})$):

(1) $NP \subseteq P/poly$.

(2) The polynomial hierarchy collapses to the second level.

What if the GCT chasm cannot be crossed?

Theorem:
Suppose NNL is not in SUBEXP.

Then assuming GRH and robustness of Valiant's conjecture (i.e., $(VNP \neq VP) \implies (VNP \not\subseteq \overline{VP})$):

(1) $NP \subseteq P/poly$.

(2) The polynomial hierarchy collapses to the second level.

[Under stronger assumptions, $P \neq BPP$.]

Outline of the talk

Outline of the talk

(1) Reformulation in terms of the orbit closures.

Outline of the talk

(1) Reformulation in terms of the orbit closures.

(2) The complexity theoretic and representation theoretic evidence for why the orbit closure of the determinant contains points that do not have small circuits.

Outline of the talk

(1) Reformulation in terms of the orbit closures.

(2) The complexity theoretic and representation theoretic evidence for why the orbit closure of the determinant contains points that do not have small circuits.

(3) The problem (NNL) of derandomizing Nother's Normalization Lemma for the orbit closure.

Outline of the talk

(1) Reformulation in terms of the orbit closures.

(2) The complexity theoretic and representation theoretic evidence for why the orbit closure of the determinant contains points that do not have small circuits.

(3) The problem (NNL) of derandomizing Nother's Normalization Lemma for the orbit closure.

(4) Why its current complexity is so high (EXPSPACE).

Outline of the talk

(1) Reformulation in terms of the orbit closures.

(2) The complexity theoretic and representation theoretic evidence for why the orbit closure of the determinant contains points that do not have small circuits.

(3) The problem (NNL) of derandomizing Nother’s Normalization Lemma for the orbit closure.

(4) Why its current complexity is so high (EXPSPACE).

(5) Why stengthened perm vs. det brings it to (quasi)-DET.

Outline of the talk

(1) Reformulation in terms of the orbit closures.

(2) The complexity theoretic and representation theoretic evidence for why the orbit closure of the determinant contains points that do not have small circuits.

(3) The problem (NNL) of derandomizing Nother's Normalization Lemma for the orbit closure.

(4) Why its current complexity is so high (EXPSPACE).

(5) Why stengthened perm vs. det brings it to (quasi)-DET.

(6) Evidence for it may not be possible to cross the chasm.

The orbit closures

Let $V = \mathbb{C}_m[Y]$ be the space of homogeneous polynomials of degree m in the entries of a variable $m \times m$ matrix Y with the action of $G = GL_{m^2}(\mathbb{C})$ that maps $f(Y) \in V$ to $f(\sigma^{-1}Y)$ for any $\sigma \in G$ (thinking of Y as an m^2-vector).

The orbit closures

Let $V = \mathbb{C}_m[Y]$ be the space of homogeneous polynomials of degree m in the entries of a variable $m \times m$ matrix Y with the action of $G = GL_{m^2}(\mathbb{C})$ that maps $f(Y) \in V$ to $f(\sigma^{-1}Y)$ for any $\sigma \in G$ (thinking of Y as an m^2-vector).

Let $P(V)$ be the projective space associated with V, and let $g = \det(Y) \in P(V)$. Define the orbit closure of the determinant as $\Delta[\det, m] = \overline{Gg} \subseteq P(V)$.

The orbit closures

Let $V = \mathbb{C}_m[Y]$ be the space of homogeneous polynomials of degree m in the entries of a variable $m \times m$ matrix Y with the action of $G = GL_{m^2}(\mathbb{C})$ that maps $f(Y) \in V$ to $f(\sigma^{-1}Y)$ for any $\sigma \in G$ (thinking of Y as an m^2-vector).

Let $P(V)$ be the projective space associated with V, and let $g = \det(Y) \in P(V)$. Define the orbit closure of the determinant as $\Delta[\det, m] = \overline{Gg} \subseteq P(V)$.

Let X be the lower-right $n \times n$ sub-matrix of Y, and z any element of Y outside X. Let $f(Y) = z^{m-n}\text{perm}(X) \in P(V)$, and define the orbit closure of the permanent as $\Delta[\text{perm}, n, m] = \overline{Gf} \subseteq P(V)$.

The reformulation in terms of orbit closures

The stronger permanent vs. determinant conjecture is now equivalent to:

Conjecture [GCT1]: $\Delta[\text{perm}, n, m] \not\subseteq \Delta[\det, m]$ if $m = \text{poly}(n)$, or more generally, $O(2^{n^\epsilon})$, for a small enough $\epsilon > 0$.

The reformulation in terms of orbit closures

The stronger permanent vs. determinant conjecture is now equivalent to:

Conjecture [GCT1]: $\Delta[\text{perm}, n, m] \not\subseteq \Delta[\det, m]$ if $m = \text{poly}(n)$, or more generally, $O(2^{n^\epsilon})$, for a small enough $\epsilon > 0$.

The main difference between the original Valiant's conjecture and this conjecture: The original conjecture is a statement about the constructible set $M_{m^2}(\mathbb{C}) \cdot \det(Y) \subseteq V$, whereas this conjecture is a statement about the variety which is its closure.

The reformulation in terms of orbit closures

The stronger permanent vs. determinant conjecture is now equivalent to:

Conjecture [GCT1]: $\Delta[\text{perm}, n, m] \not\subseteq \Delta[\det, m]$ if $m = \text{poly}(n)$, or more generally, $O(2^{n^\epsilon})$, for a small enough $\epsilon > 0$.

The main difference between the original Valiant's conjecture and this conjecture: The original conjecture is a statement about the constructible set $M_{m^2}(\mathbb{C}) \cdot \det(Y) \subseteq V$, whereas this conjecture is a statement about the variety which is its closure.

The basic principle of algebraic geometry: The difficulty of a constructible set is controlled by what lies on its border.

What lies on the border of $G \cdot \det(Y)$?

Defn: A family of points $\{p_m\}$, $p_m \in \Delta[\det, m]$, is called a family of bad exterior points if $\{p_m\} \notin VP$ (i.e., p_m cannot be computed by a small circuit over $\mathbb{C}$).

What lies on the border of $G \cdot \det(Y)$?

Defn: A family of points $\{p_m\}$, $p_m \in \Delta[\det, m]$, is called a family of bad exterior points if $\{p_m\} \notin VP$ (i.e., p_m cannot be computed by a small circuit over $\mathbb{C}$).

Fact: Assuming GCT1-conjecture, such a family is VNP-intermediate. If there did not exist VNP-intermediate polynomials, such bad exterior points could not exist. But VNP-intermediate polynomials exist [Bürgisser] (failure of dichotomy).

What lies on the border of $G \cdot \det(Y)$?

Defn: A family of points $\{p_m\}$, $p_m \in \Delta[\det, m]$, is called a family of bad exterior points if $\{p_m\} \notin VP$ (i.e., p_m cannot be computed by a small circuit over $\mathbb{C}$).

Fact: Assuming GCT1-conjecture, such a family is VNP-intermediate. If there did not exist VNP-intermediate polynomials, such bad exterior points could not exist. But VNP-intermediate polynomials exist [Bürgisser] (failure of dichotomy).

Conjecture: $\Delta[\det, m]$ has bad exterior points.

What lies on the border of $G \cdot \det(Y)$?

Defn: A family of points $\{p_m\}$, $p_m \in \Delta[\det, m]$, is called a family of bad exterior points if $\{p_m\} \notin VP$ (i.e., p_m cannot be computed by a small circuit over $\mathbb{C}$).

Fact: Assuming GCT1-conjecture, such a family is VNP-intermediate. If there did not exist VNP-intermediate polynomials, such bad exterior points could not exist. But VNP-intermediate polynomials exist [Bürgisser] (failure of dichotomy).

Conjecture: $\Delta[\det, m]$ has bad exterior points.

Next: The complexity-theoretic evidence and natural (constructive) candidates from representation theory.

Newton degeneration

Given any symbolic matrix Z of size $m = \text{poly}(n)$ over the variables $z_1, \ldots, z_n$, let $Newton(Z)$ be the Newton polytope of $\det(Z) = \sum_\alpha c_\alpha z^\alpha$. Given any face $F \subseteq Newton(Z)$, let $\det_F(Z) = \sum_{\alpha \in F} c_\alpha z^\alpha$. Call it the Newton degeneration of $\det(Z)$ associated with the face F.

Newton degeneration

Given any symbolic matrix Z of size $m = \text{poly}(n)$ over the variables $z_1, \ldots, z_n$, let $Newton(Z)$ be the Newton polytope of $\det(Z) = \sum_\alpha c_\alpha z^\alpha$. Given any face $F \subseteq Newton(Z)$, let $\det_F(Z) = \sum_{\alpha \in F} c_\alpha z^\alpha$. Call it the Newton degeneration of $\det(Z)$ associated with the face F.

Fact: $\det_F(Z) \in \Delta[\det, m]$ for any F and Z as above.

Newton degeneration

Given any symbolic matrix Z of size $m = \text{poly}(n)$ over the variables $z_1, \ldots, z_n$, let $Newton(Z)$ be the Newton polytope of $\det(Z) = \sum_\alpha c_\alpha z^\alpha$. Given any face $F \subseteq Newton(Z)$, let $\det_F(Z) = \sum_{\alpha \in F} c_\alpha z^\alpha$. Call it the Newton degeneration of $\det(Z)$ associated with the face F.

Fact: $\det_F(Z) \in \Delta[\det, m]$ for any F and Z as above.

(1) Qiao: Every Newton degeneration of the Tutte polynomial associated with the Edmonds perfect matching polytope of any non-bipartite graph has a small circuit.

Newton degeneration

Given any symbolic matrix Z of size $m = \text{poly}(n)$ over the variables $z_1, \ldots, z_n$, let $Newton(Z)$ be the Newton polytope of $\det(Z) = \sum_\alpha c_\alpha z^\alpha$. Given any face $F \subseteq Newton(Z)$, let $\det_F(Z) = \sum_{\alpha \in F} c_\alpha z^\alpha$. Call it the Newton degeneration of $\det(Z)$ associated with the face F.

Fact: $\det_F(Z) \in \Delta[\det, m]$ for any F and Z as above.

(1) Qiao: Every Newton degeneration of the Tutte polynomial associated with the Edmonds perfect matching polytope of any non-bipartite graph has a small circuit.
(1) Fournier, Malod: The problem of deciding if x^α occurs in $\det(Z)$, given Z and α, is hard ($C_= P$-complete).

Newton degeneration

Given any symbolic matrix Z of size $m = \text{poly}(n)$ over the variables $z_1, \ldots, z_n$, let $Newton(Z)$ be the Newton polytope of $\det(Z) = \sum_\alpha c_\alpha z^\alpha$. Given any face $F \subseteq Newton(Z)$, let $\det_F(Z) = \sum_{\alpha \in F} c_\alpha z^\alpha$. Call it the Newton degeneration of $\det(Z)$ associated with the face F.

Fact: $\det_F(Z) \in \Delta[\det, m]$ for any F and Z as above.

(1) Qiao: Every Newton degeneration of the Tutte polynomial associated with the Edmonds perfect matching polytope of any non-bipartite graph has a small circuit.
(1) Fournier, Malod: The problem of deciding if x^α occurs in $\det(Z)$, given Z and α, is hard ($C_= P$-complete).
(2) Qiao: The membership problem for $Newton(Z)$ is P-hard.

Newton degeneration of VP

Given any family $\{\det(Z_n)\} \in VP_s$ and any sequence $\{F_n \subseteq Newton(Z_n)\}$, the family $\{\det_{F_n}(Z_n)\}$ is called a Newton degeneration of $\{\det(Z_n)\}$. Let $Newton(VP_s) \subseteq \overline{VP_s} \cap VNP$ be the set of all Newton degenerations of the elements in VP_s.

Newton degeneration of VP

Given any family $\{\det(Z_n)\} \in VP_s$ and any sequence $\{F_n \subseteq Newton(Z_n)\}$, the family $\{\det_{F_n}(Z_n)\}$ is called a Newton degeneration of $\{\det(Z_n)\}$. Let $Newton(VP_s) \subseteq \overline{VP_s} \cap VNP$ be the set of all Newton degenerations of the elements in VP_s.

Conjecture: $Newton(VP_s) \not\subseteq VP$. Implies existence of bad exterior points, and is supported by complexity theory (Edmonds, Qiao, Fournier, Malod).

Newton degeneration of VP

Given any family $\{\det(Z_n)\} \in VP_s$ and any sequence $\{F_n \subseteq Newton(Z_n)\}$, the family $\{\det_{F_n}(Z_n)\}$ is called a Newton degeneration of $\{\det(Z_n)\}$. Let $Newton(VP_s) \subseteq \overline{VP_s} \cap VNP$ be the set of all Newton degenerations of the elements in VP_s.

Conjecture: $Newton(VP_s) \not\subseteq VP$. Implies existence of bad exterior points, and is supported by complexity theory (Edmonds, Qiao, Fournier, Malod). Also supported by representation theory of quivers (Drozd (tame-wild dichotomy); Gabriel; Schofield; Derksen-Weyman).

Newton degeneration of VP

Given any family $\{\det(Z_n)\} \in VP_s$ and any sequence $\{F_n \subseteq Newton(Z_n)\}$, the family $\{\det_{F_n}(Z_n)\}$ is called a Newton degeneration of $\{\det(Z_n)\}$. Let $Newton(VP_s) \subseteq \overline{VP_s} \cap VNP$ be the set of all Newton degenerations of the elements in VP_s.

Conjecture: $Newton(VP_s) \not\subseteq VP$. Implies existence of bad exterior points, and is supported by complexity theory (Edmonds, Qiao, Fournier, Malod). Also supported by representation theory of quivers (Drozd (tame-wild dichotomy); Gabriel; Schofield; Derksen-Weyman).

To each quiver Q without oriented cycles, one can associate using the representation theory of quivers a subclass $VP_s[Q] \subseteq VP_s$.

Newton degeneration of VP

Given any family $\{\det(Z_n)\} \in VP_s$ and any sequence $\{F_n \subseteq Newton(Z_n)\}$, the family $\{\det_{F_n}(Z_n)\}$ is called a Newton degeneration of $\{\det(Z_n)\}$. Let $Newton(VP_s) \subseteq \overline{VP_s} \cap VNP$ be the set of all Newton degenerations of the elements in VP_s.

Conjecture: $Newton(VP_s) \not\subseteq VP$. Implies existence of bad exterior points, and is supported by complexity theory (Edmonds, Qiao, Fournier, Malod). Also supported by representation theory of quivers (Drozd (tame-wild dichotomy); Gabriel; Schofield; Derksen-Weyman).

To each quiver Q without oriented cycles, one can associate using the representation theory of quivers a subclass $VP_s[Q] \subseteq VP_s$. Conjecturally $Newton(VP_s[Q]) \not\subseteq VP$, Q wild.

Tame vs. wild quivers

(1) Q is $\rightarrow$ (tame): $VP_s[Q]$ consists of the single family $\{\det(X_n)\}$, where X_n is an $n \times n$ variable matrix.

Tame vs. wild quivers

(1) Q is $\rightarrow$ (tame): $VP_s[Q]$ consists of the single family $\{\det(X_n)\}$, where X_n is an $n \times n$ variable matrix.

(2) Q is $\overset{\frown}{\rightarrow}$ (tame symmetric): $VP_s[Q]$ consists of the single family $\{\det(X_n)\}$, where X_n is a $2n \times 2n$ variable skew-symmetric matrix. This quiver corresponds to Edmonds' P-theory, and $Newton(VP_s[Q]) \subseteq VP$ [Qiao].

Tame vs. wild quivers

(1) Q is $\rightarrow$ (tame): $VP_s[Q]$ consists of the single family $\{\det(X_n)\}$, where X_n is an $n \times n$ variable matrix.

(2) Q is $\widehat{\rightarrow}$ (tame symmetric): $VP_s[Q]$ consists of the single family $\{\det(X_n)\}$, where X_n is a $2n \times 2n$ variable skew-symmetric matrix. This quiver corresponds to Edmonds' P-theory, and $Newton(VP_s[Q]) \subseteq VP$ [Qiao].

(3) Q is $\overrightarrow{\Longrightarrow}$ (wild): $VP_s[Q]$ consists of the families $\{\det(Z_n)\}$, where Z_n is a $d \times d$ block matrix, with $d = p(n)$ (a fixed polynomial), and its (i,j)-th block is the symbolic sum $x_{ij}^1 Z_1 + x_{ij}^2 Z_2 + x_{ij}^3 Z_3$, where Z_1, Z_2 and Z_3 are $n \times n$ variable matrices, and x_{ij}^k's are variables. $Newton(VP_s[Q]) \subseteq \overline{VP_s}$, and conjecturally it is not in VP.

Noether's Normalization Lemma [Hilbert]

Lemma [NNL]: Given any projective variety $X \subseteq P(\mathbb{C}^k)$ of dimension n, there exists a homogeneous linear map $\psi : \mathbb{C}^k \to \mathbb{C}^m$, $m =$ poly(n), that induces a regular (well defined) map on X, called a normalizing map.

Noether's Normalization Lemma [Hilbert]

Lemma [NNL]: Given any projective variety $X \subseteq P(\mathbb{C}^k)$ of dimension n, there exists a homogeneous linear map $\psi : \mathbb{C}^k \to \mathbb{C}^m$, $m =$ poly(n), that induces a regular (well defined) map on X, called a normalizing map.

Any random ψ has this property for $m \geq n + 1$. But deterministic construction of ψ (the problem NNL) is hard.

Noether's Normalization Lemma [Hilbert]

Lemma [NNL]: Given any projective variety $X \subseteq P(\mathbb{C}^k)$ of dimension n, there exists a homogeneous linear map $\psi : \mathbb{C}^k \to \mathbb{C}^m$, $m =$ poly(n), that induces a regular (well defined) map on X, called a normalizing map.

Any random ψ has this property for $m \geq n + 1$. But deterministic construction of ψ (the problem NNL) is hard.

If we use the standard representations of ψ and X, then the specification of ψ itself requires exponential space in n.

Noether's Normalization Lemma [Hilbert]

Lemma [NNL]: Given any projective variety $X \subseteq P(\mathbb{C}^k)$ of dimension n, there exists a homogeneous linear map $\psi : \mathbb{C}^k \rightarrow \mathbb{C}^m$, $m =$ poly(n), that induces a regular (well defined) map on X, called a normalizing map.

Any random ψ has this property for $m \geq n + 1$. But deterministic construction of ψ (the problem NNL) is hard.

If we use the standard representations of ψ and X, then the specification of ψ itself requires exponential space in n. So we only consider the case when X is an explicit variety, such as $\Delta[\det, m]$, that has a specification of bit-length polynomial in its dimension (a circuit for the determinant).

The problem NNL for $\Delta[\det, m]$

Let $X = \Delta[\det, m] \subseteq P(V)$, $V = \mathbb{C}_m[Y]$.

The problem NNL for $\Delta[\det, m]$

Let $X = \Delta[\det, m] \subseteq P(V)$, $V = \mathbb{C}_m[Y]$.

Given an $m \times m$ matrix B, let $\psi_B : V \to \mathbb{C}$ denote the linear evaluation map that maps $f(Y) \in V$ to $f(B)$. Given a set $\mathcal{B} = \{B_1, \ldots, B_l\}$ of $m \times m$ matrices, let $\psi_{\mathcal{B}} : V \to \mathbb{C}^l$ denote the map $(\psi_{B_1}, \ldots, \psi_{B_l})$.

The problem NNL for $\Delta[\det, m]$

Let $X = \Delta[\det, m] \subseteq P(V)$, $V = \mathbb{C}_m[Y]$.

Given an $m \times m$ matrix B, let $\psi_B : V \to \mathbb{C}$ denote the linear evaluation map that maps $f(Y) \in V$ to $f(B)$. Given a set $\mathcal{B} = \{B_1, \ldots, B_l\}$ of $m \times m$ matrices, let $\psi_{\mathcal{B}} : V \to \mathbb{C}^l$ denote the map $(\psi_{B_1}, \ldots, \psi_{B_l})$.

Lemma: There exists a small set $\mathcal{B}$ of integer matrices of poly(m) total bit-size such that $\psi_{\mathcal{B}} : V \to \mathbb{C}^l$ induces a regular (normalizing) map on $\Delta[\det, m] \subseteq P(V)$.

The problem NNL for $\Delta[\det, m]$

Let $X = \Delta[\det, m] \subseteq P(V)$, $V = \mathbb{C}_m[Y]$.

Given an $m \times m$ matrix B, let $\psi_B : V \to \mathbb{C}$ denote the linear evaluation map that maps $f(Y) \in V$ to $f(B)$. Given a set $\mathcal{B} = \{B_1, \ldots, B_l\}$ of $m \times m$ matrices, let $\psi_{\mathcal{B}} : V \to \mathbb{C}^l$ denote the map $(\psi_{B_1}, \ldots, \psi_{B_l})$.

Lemma: There exists a small set $\mathcal{B}$ of integer matrices of poly(m) total bit-size such that $\psi_{\mathcal{B}} : V \to \mathbb{C}^l$ induces a regular (normalizing) map on $\Delta[\det, m] \subseteq P(V)$.

The problem NNL: Given m (specified in unary), construct a small set $\mathcal{B}$ such that $\psi_{\mathcal{B}}$ is a normalizing map on $\Delta[\det, m]$.

The current complexity of NNL

Theorem: NNL is in EXPSPACE (Gröbner basis theory).

The current complexity of NNL

Theorem: NNL is in EXPSPACE (Gröbner basis theory).

The space complexity is exponential because the dimension of the ambient space $P(V)$ containing $\Delta[\det, m]$ is exponential in m.

The current complexity of NNL

Theorem: NNL is in EXPSPACE (Gröbner basis theory).

The space complexity is exponential because the dimension of the ambient space $P(V)$ containing $\Delta[\mathrm{det}, m]$ is exponential in m.

If we could prove that every point in $\Delta[\mathrm{det}, m]$ has a small circuit over $\mathbb{C}$ then it would follow from the existing techniques (Heintz and Schnorr, Koiran,...) that NNL is in PSPACE.

The current complexity of NNL

Theorem: NNL is in EXPSPACE (Gröbner basis theory).

The space complexity is exponential because the dimension of the ambient space $P(V)$ containing $\Delta[\det, m]$ is exponential in m.

If we could prove that every point in $\Delta[\det, m]$ has a small circuit over $\mathbb{C}$ then it would follow from the existing techniques (Heintz and Schnorr, Koiran,...) that NNL is in PSPACE.

The main obstacle to the existing techniques: the existence of bad exterior (including wild) points in $\Delta[\det, m]$.

The main results

Theorem: The stronger GCT1-conjecture implies that NNL for $\Delta[\mathrm{det}, m]$ is in quasi-DET $\subseteq$ quasi-P.

The main results

Theorem: The stronger GCT1-conjecture implies that NNL for $\Delta[\mathrm{det}, m]$ is in quasi-DET $\subseteq$ quasi-P.

Equivalence Theorem: There exists an exponential time computable multilinear polynomial in n variables which cannot be approximated infinitesimally closely by symbolic determinants of size $m = O(2^{n^\epsilon})$ iff (ignoring a quasi-prefix) NNL for $\Delta[\mathrm{det}, m]$ is in P.

The main results

Theorem: The stronger GCT1-conjecture implies that NNL for $\Delta[\mathrm{det}, m]$ is in quasi-DET $\subseteq$ quasi-P.

Equivalence Theorem: There exists an exponential time computable multilinear polynomial in n variables which cannot be approximated infinitesimally closely by symbolic determinants of size $m = O(2^{n^\epsilon})$ iff (ignoring a quasi-prefix) NNL for $\Delta[\mathrm{det}, m]$ is in P.

Theorem [Shallow circuits]: If there exists an exponential time computable multilinear polynomial in n variables that cannot be approximated infinitesimally closely by depth three (or depth four homogeneous) circuits of size $O(2^{n^{1/2+\epsilon}})$, for some $\epsilon > 0$, then NNL for $\Delta[\mathrm{det}, m]$ is in quasi-DET.

Basic proof idea

Step 1: Polynomial time Monte-Carlo algorithm: Hilbert et al. + Heintz and Schnorr.

Basic proof idea

Step 1: Polynomial time Monte-Carlo algorithm: Hilbert et al. + Heintz and Schnorr.

Step 2: Derandomize this algorithm using the GCT1-conjecture in conjunction with:

Basic proof idea

Step 1: Polynomial time Monte-Carlo algorithm: Hilbert et al. + Heintz and Schnorr.

Step 2: Derandomize this algorithm using the GCT1-conjecture in conjunction with:

(a) the Hardness vs. randomness principle: Nisan-Wigderson and Kabanets-Impagliazzo, and

Basic proof idea

Step 1: Polynomial time Monte-Carlo algorithm: Hilbert et al. + Heintz and Schnorr.

Step 2: Derandomize this algorithm using the GCT1-conjecture in conjunction with:

(a) the Hardness vs. randomness principle: Nisan-Wigderson and Kabanets-Impagliazzo, and

(b) efficient factorization of Multi-variate polynomials: Kaltofen. This lies at the heart of the proof.

Basic proof idea

Step 1: Polynomial time Monte-Carlo algorithm: Hilbert et al. + Heintz and Schnorr.

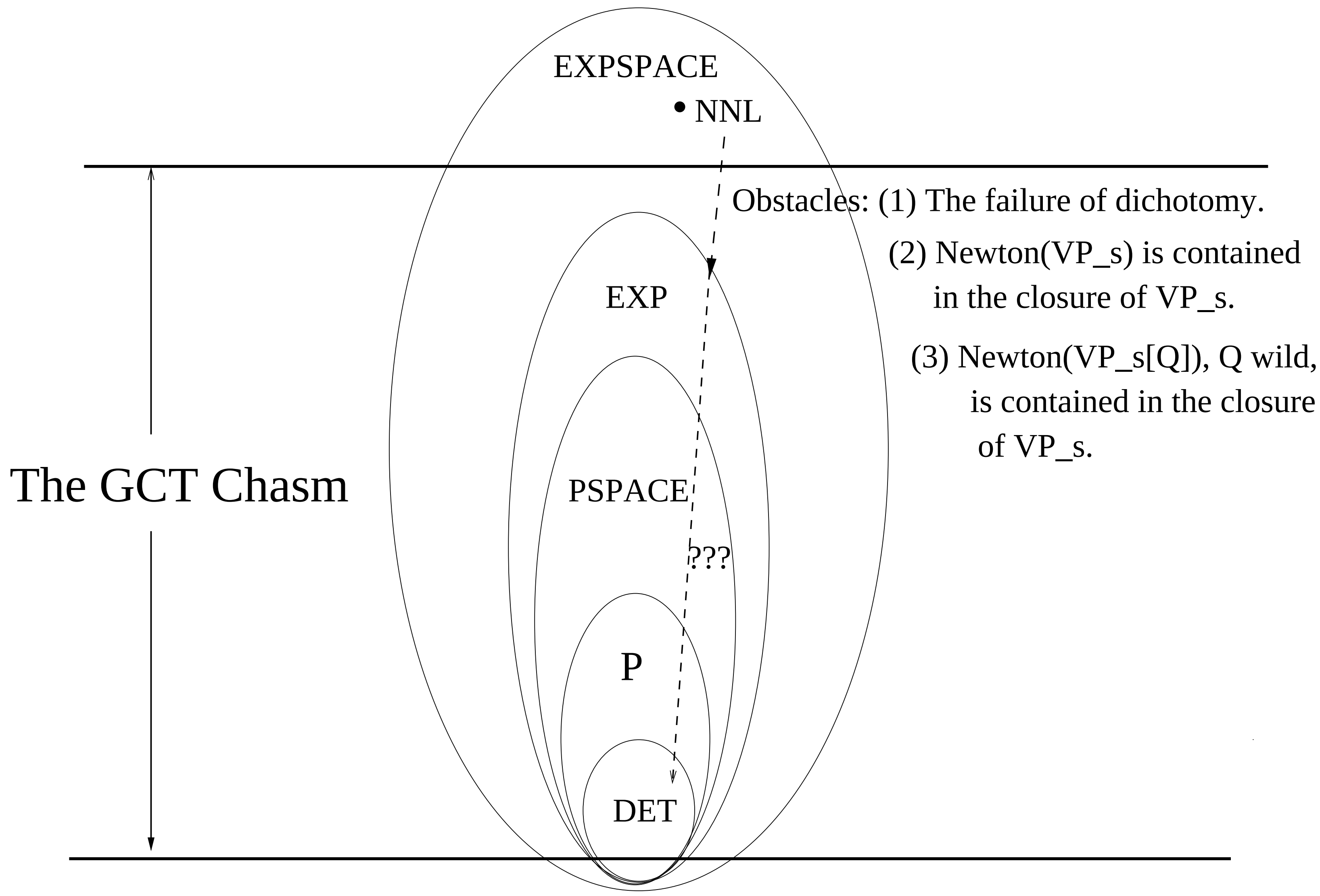
Step 2: Derandomize this algorithm using the GCT1-conjecture in conjunction with:

(a) the Hardness vs. randomness principle: Nisan-Wigderson and Kabanets-Impagliazzo, and

(b) efficient factorization of Multi-variate polynomials: Kaltofen. This lies at the heart of the proof.

All this works only in the models in which the determinant and multi-variate factorization can be computed efficiently.

The GCT chasm



Can the chasm be crossed? (contd.)

All the evidence supports that: (1) $Newton(VP_s) \not\subseteq VP$ (or even its subexponential analogue), as conjectured, and (2) the size of the circuit may not be beaten by the derandomization procedures. Hence, NNL for $\Delta[\mathrm{det}, m]$ may not be in SUBEXP.

Can the chasm be crossed? (contd.)

All the evidence supports that: (1) $Newton(VP_s) \not\subseteq VP$ (or even its subexponential analogue), as conjectured, and (2) the size of the circuit may not be beaten by the derandomization procedures. Hence, NNL for $\Delta[\det, m]$ may not be in SUBEXP.

Theorem [Recall] Then, assuming GRH and robustness of Valiant's conjecture, $NP \subseteq P/poly$ and hence the polynomial hierarchy collapses to the second level.

Can the chasm be crossed? (contd.)

All the evidence supports that: (1) $Newton(VP_s) \not\subseteq VP$ (or even its subexponential analogue), as conjectured, and (2) the size of the circuit may not be beaten by the derandomization procedures. Hence, NNL for $\Delta[\mathrm{det}, m]$ may not be in SUBEXP.

Theorem [Recall] Then, assuming GRH and robustness of Valiant's conjecture, $NP \subseteq P/poly$ and hence the polynomial hierarchy collapses to the second level.

Can NNL be derandomized for intemediate explicit varieties?

Can the chasm be crossed? (contd.)

All the evidence supports that: (1) $Newton(VP_s) \not\subseteq VP$ (or even its subexponential analogue), as conjectured, and (2) the size of the circuit may not be beaten by the derandomization procedures. Hence, NNL for $\Delta[\det, m]$ may not be in SUBEXP.

Theorem [Recall] Then, assuming GRH and robustness of Valiant's conjecture, $NP \subseteq P/poly$ and hence the polynomial hierarchy collapses to the second level.

Can NNL be derandomized for intemediate explicit varieties?

Yes, with implications in Klein's Erlangen program. Tomorrow.