Simulation Complexity Classes

Ketan Mulmuley
U Chicago

1) The P vs. NP problem : (char 0) [GCT1]
2) #P vs. NC problem

The Basic Plan

The first step

non existence problem (-)

Perm vs. det ⟹

Existence Problem proving existence of a family $\{O_n\}$ of obstructions

Obstruction or "Proof-certificate" for hardness of perm(X)

Associate with:

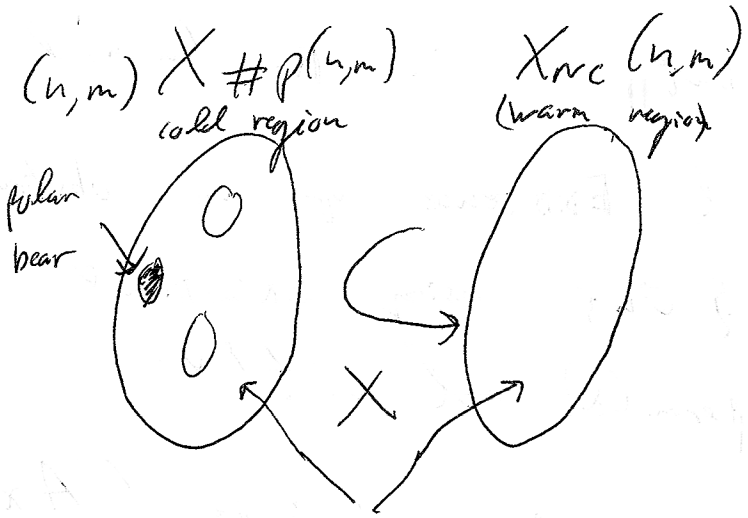
#p. A family $\{X_{\#p}(n,m)\}$ of class varieties (group-theoretic)

NC. ——— $\{X_{nc}(n,m)\}$

Such that:

If $perm(X^{n\times n})$ can be represented linearly on $det(Y^{m\times m})$, $m > n$, then

$X_{\#p}(n,m) \subseteq X_{nc}(n,m)$



Bricks are bimodule

Irreducible representations of $G = GL_\ell(\mathbb{C})$ $\overset{\text{Weyl}}{\longleftrightarrow}$ $\lambda : \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_\ell \geq 0$ integral

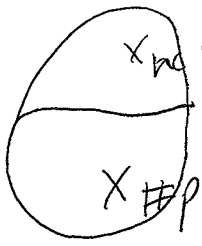
Weyl-module $V_\lambda(G) \longleftrightarrow \lambda$

Fix $\log^{a+1} n > 2$, $a > 1$ fixed

Suppose to the contrary, that $X_{\#p}(n,m) \subseteq X_{nc}(n,m)$

$R_{\#P}(n,m)_d \leftarrow R_{VC}(n,m)_d$

Suppose to the contrary, that



Homogeneous Coordinate ring

Defn An obstruction on is a Weyl-module $V_\lambda(\epsilon)$ that occurs in $R_{\#P}(n,m)_d$ but not in $R_{VC}(n,m)_d$ for some d

Goal Existence of an obstruction family $\{O_n\}$ using exceptional nature of perm(X) and det(Y).

Unique: $\text{perm}(X) = \text{perm}(A \times B)$ $\forall A, B$ diagonal or permutation matrices

$X^* = X$ or X^t

Unique: $\det(Y) = \det(A\, Y^* B)$ $\forall$ $A, B \in GL_{m^2}$ with $\det(A)\det(B) = 1$

& $Y^* = Y$ or Y^t

Exceptional: characterized by symmetries

<u>Proof:</u> Existence of an obstruction: On, $n \to \infty$ with $m = 2^{\log^a n}$, $a \geq 1$, implies that $\mathrm{perm}_{n\times n}(X)$ cannot be expressed linearly on $\det_{m\times m}(Y)$.

$F_{\lambda,n,m}(k) = \#$ occurrences of $V_{k\lambda}(E)$ in $\otimes^m W$

$R_{\#P}(n,m)$

$G_{\lambda,n,m}(k) =$ ______________ in $R_{NC}(n,m)$

<u>Def:</u> A function $f(k)$ is called a quasi-polynomial if there are polynomials $f_i(x)$ for some $i \leq l_i$ such that

$$f(k) = f_i(k) \quad \text{if } k \equiv i \bmod p$$

$f_1(k)$
$\vdots$
$f_l(k)$

λ 2λ 3λ

Thm (GCT6):
$F_{\lambda,n,m}(k)$ and $G_{\lambda,n,m}(k)$ are quasi-polynomials

assuming that the singularities of the class varieties $X_{\#P}(n,m)$ and $X_{inc}(n,m)$ are rational.

Analogous result for P vs NP

Basic Idea:

Refs

P ← Polytope: $f_P(k) = \#(kP)$ — Ehrhart
↑ int points quasi-polynomials

PH (positive by hypothesis):

$\exists$ polytopes $P_{\ell,n,m}$ and $Q_{\ell,n,m}$ for given ℓ,n,m

such that

$F_{\ell,n,m}(k)$ and $G_{\ell,n,n}(k)$ have

positive convex representations

$$F_{\ell,n,m}(k) = \#(kP_{\ell,n,m})$$

$$G_{\ell,n,m}(k) = \#(kQ_{\ell,n,m})$$

The dimensions of $P_{z,y,m}$ and $Q_{z,y,m}$ are guaranteed to be polynomial in n and length (z)

$$z_1 \# z_2 \# \cdots \# z_s \# 0$$

length

Thm (GCTG)

There exists a family $\{a_n = V_{\lambda_m}(\epsilon)\}$ of obstructions, for $m = 2^{\log^a n}$ $a > 1$ fixed $n \to \infty$

assuming PH and

OH (Obstruction hypothesis)

$\forall n \to \infty$

$\exists z$ s.t. $P_{z,n,m} \neq \emptyset$ and $Q_{z,n,m} \neq \emptyset$

Strategies **Explicit constructions & Obstructions**

(1) Find explicit $P_{z,y,m}$, $Q_{z,y,m}$ satisfying PH

PH^+: membership in $P_{z,n,m}$ and $Q_{z,n,m} \in P$ & can be done in poly$(n, \langle z \rangle)$ time

↳ Bit length

(2) Find an explicit family $\{a_n = V_{f_n}(\epsilon)\}$ of obstruction satisfying OH

for each n, f_n can be constructed poly(n) time.

Why should PH and OH hold?

Evidence GCT 2, 6, 7, 8

How to prove PH:

GCT 6, 7, 4, 8. Basic Plan via theory of nonstandard quantum groups

– intricately related to Riemann Hypothesis over finite fields

What is Achieved? (P vs. NP char 0)

The original goal (#P vs. VC in char 0)

$\forall n$, $n = 2^{\log^a n}$, $a > 1$ fixed

$\downarrow$

$\forall c$ circuits of polylog(n) depth & poly(n) size

IOH (Infeasible Obstruction Hypothesis)

perm(x) $\neq f_c(x)$ — #P condition

(Infeasible) IOH: $\nearrow_2 \#P$

$\downarrow$ PH

OH: NP $[PH^+]$

(Positivity as means to eliminate quantifying variables)

$\downarrow \widetilde{PH}$

POH: P

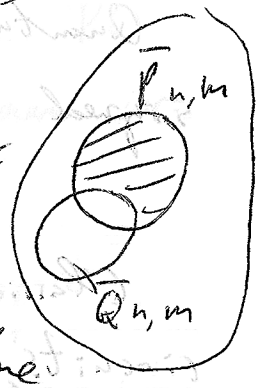
$\downarrow$ POH

tautology: trivial $O(1)$ proof — The Proof

Define $\dfrac{\text{length } s \le l}{\lambda_1 \succ \lambda_2 : \cdots \succ \lambda_s > 0} \le (n+1)^s$

$P_{n,m} = \{\lambda : P_{\lambda,n,m} \neq \emptyset\} \subseteq \mathbb{C}^s$

$\bar{Q}_{n,m} = \{\lambda : Q_{\lambda,n,m} \neq \emptyset\} \subseteq \mathbb{C}^s$

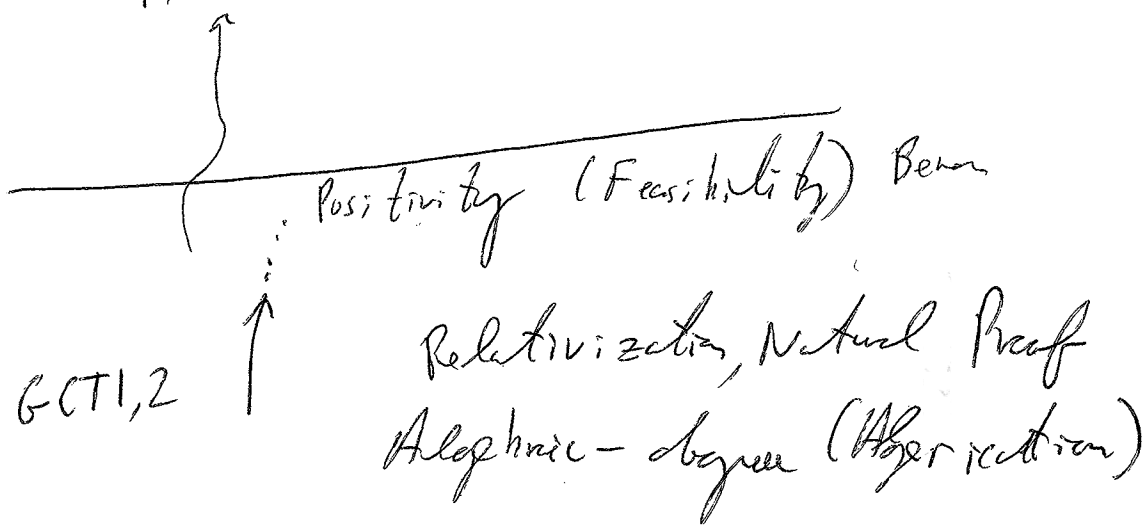


$\widetilde{PH}$: $\bar{P}_{n,m}$ and $\bar{Q}_{n,m}$ are convex cones in $\mathbb{C}^s = (n+1)^s$ $\xrightarrow{n}$

$\widetilde{PH}^+$: membership $\in P$ } can be done (containment $\in P$) } in $\text{poly}(n)$ time

POH: $\forall n \to \infty$ assuming $m = 2^{\log^a n}$ $a > 1$

$\text{vol}(\bar{P}_{n,m} \setminus \bar{Q}_{n,m}) > 0$ i.e. $\bar{P}_{n,m} \subseteq \bar{Q}_{n,m}$ fixed



What is PH

Class varieties

Obstruction

Mar. 11, 2009

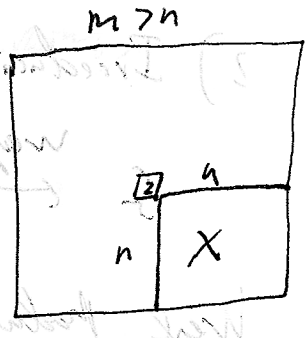
Quantum computing and quadratically-signed weight enumerators.

Knill, La flamme (2001)

Classical Ising model test for quantum circuits,

Geraci, Lidar (2009)

Perm vs. Det problem (Valiant)



Restatement: X: $n \times n$ variable matrix

Y: $m \times m$

Problem: $\nexists$ $A \in M_{m^2}(\mathbb{C})$ s.t.

$$\text{Perm}(X)\, 2^{m-n} = \det(AY)$$

(AY: $m^2 \times m^2$ matrix; m^2-vector)

Goal:

Basic Alg. Geom.

$V = \mathbb{C}^m$ $P(V)$: projective space,

$\mathbb{C}[V]$: coordinate ring of V

Projective algebraic variety Y in $P(V)$:

= zero-set of a set homogeneous forms in $x_1, \dots, x_m$ (irreducible)

Basic Reg Thm:

$G = GL_n(\mathbb{C})$

$I(Y)$: ideal of Y = space of forms that vanish on Y.

$R(Y)$: homogeneous coordinate ring of Y = $\mathbb{C}[V]/I(Y)$

Weyl: 1) Every finite dimensional representation W of G is completely reducible:

$$W = \bigoplus_i m_i W_i$$

(W_i: irreducible representation; m_i: multiplicity; i: primes)

2) Irreducible representations of

$G \overset{\text{Weyl}}{\longleftrightarrow} \lambda: \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$

Weyl Module $V_\lambda(G) \longleftrightarrow \lambda$

Basic GIT:

V = a finite dimensional representation

of $G = Gl_n(\mathbb{C})$

The $\mathbb{C}[V]$ — Homogeneous coordinate ring of $P(V)$

— is G-module coordinate ring of V

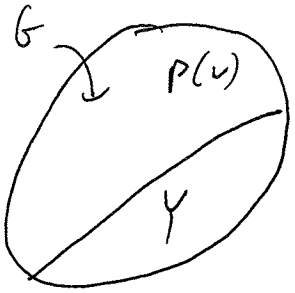
$$\begin{array}{ccc} f(v) & \longrightarrow & f(\sigma^{-1}v) \\ \uparrow & & \uparrow \\ \mathbb{C}[V] & & G = Gl_n(\mathbb{C}) \\ f(x_1, \ldots, x_n) & \longrightarrow & f(\sigma^{-1}x) \end{array}$$

σ acts on V; $\rho(\sigma)$ acts on $\mathbb{C}[V]$

X

Basic Fact: $\Delta_V[V]$ is a projective G-subvariety of $P(V)$. In general alg. geometry $\Delta_V[V]$ is hopeless

Defn: A projective variety $Y \subseteq P(V)$ is called a G-variety if the ideal $I(Y)$ is a G-module of $\mathbb{C}[V]$



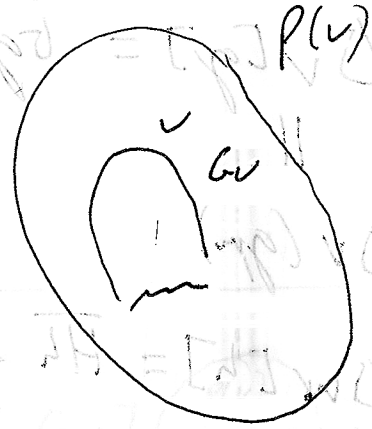
Let $v \in P(V)$ be a point,

G_v the orbit of v:

$$G_v = \{ gv \mid g \in G \}$$

The orbit-closure $\Delta_V[v]$ of v:

$$\Delta_V[v] : \overline{G_v} \subset P(V)$$



Class Varieties

$V = Sym^m(Y)$: space of forms in Y of degree m

$= $ representation of $G = GL(Y) = GL_{m^2}(\mathbb{C})$

$$\begin{array}{ccc} g & \longrightarrow & g(D^{-1}Y) \\ \uparrow & & \downarrow \\ G & & m^2 \times m^2 \text{ matrix} \end{array}$$

g: m^2 vector; $g(D^{-1}Y)$: m^2-vector

$W = Sym^n(X)$: representation of $H = GL_{n^2}(\mathbb{C}) \supset GL(X)$

$$W \xrightarrow{\phi} V$$

$$h(x) \longrightarrow h^\phi(Y) = 2^{m-n} h(x)$$

$g = det(Y) \in V, P(V)$

$h = perm(X) \in W, P(W)$

$f = h^{\phi} \in V, P(V)$

$\| perm^{\phi}$

$\Delta_V[g] = \overline{G \cdot g} \subseteq P(V)$ — class variety of NC

$\| \qquad\qquad X_{NC}^{(n,m)}$

$\Delta_V(g_{m^2})$

$\Delta_W[h] = \overline{H \cdot h} \subseteq P(W)$ — Bar class varieties & #P

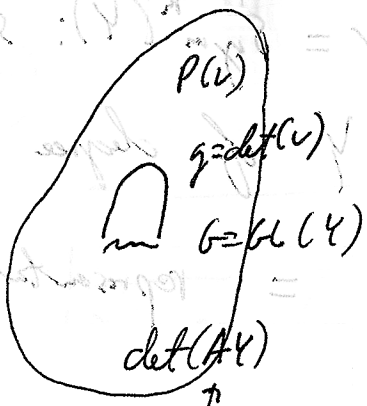
$\| \qquad\qquad$

$\Delta_W[h_{n^2}]$

$\Delta_V[f] = \overline{G \cdot f} \subseteq P(V)$

$\|$ (class variety for #P $(X_{\#P}^{(n,m)})$)

$\Delta_V[f_{n,m}]$



Prop: If $h = perm_n(X)$ can be expressed linearly as $det(AY)$ then $A \in M_{m^2}(\mathbb{C})$

$f \in \Delta_v[g, m] = \Delta v[g]$

$\hookrightarrow \Delta_v(g) \subseteq \Delta v(g)$

& ~~Conversely, convex. by~~ if

$f \in \Delta v[g, m]$ then

f can be approximately infinitesimally closely by

$$\det(AY)$$
$$\cap$$
$$Gl_{m^2}(\nabla)$$

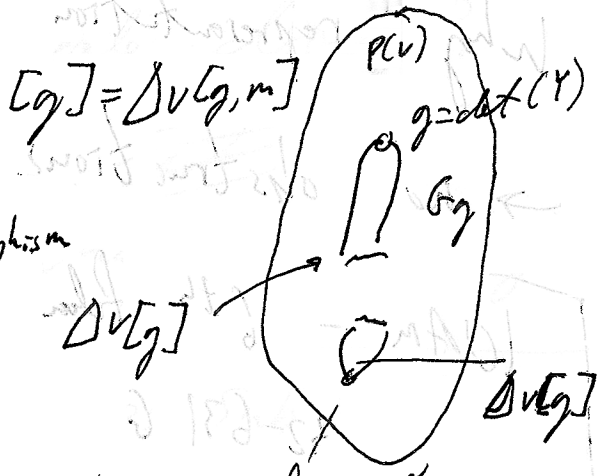
Suppose to the contrary that

$\Delta v[f, n, m] = \Delta v[f] \subsetneq \Delta v[g] = \Delta v[g, m]$

$R_v[f, n, m] = R_v[f]$ surjective G-homomorphism

$R_v[g]_d = R_v[g, m]_d$

Hom. coordinate ring of $\Delta v[g]$



$R_v[f, n, m]_2^* = R_v[f]_d^* \hookrightarrow R_v[g]_a^* = R_v[g, m]_d^*$

injective G-homomorphism

G-module

Defn: A Weyl module $V_\chi(G)$ is an *obstruction* if $G = GL_{m^2}(\mathbb{C})$

$V_\chi(G)$ occurs as a G-subrepresentation

but not... $\mathbb{C}[R_u[f, u, m]]_d^*$

... $\mathbb{C}[R_u[\det_m]]_d^*$ for some d.

[GCT2]

Symmetries b/w [Perm & Det]

Why representation theory

→ no obstructions.

[IAM – 6th floor conference room
32-6316
Why obstruction should exist.]

END