Invariant theorya gentle introduction for computer scientists (optimization and complexity)

Avi Wigderson, IAS, Princeton

Ankit Garg, Rafael Oliveira

Zeyuan Allen-Zhu, Peter Burgisser, Cole Franks, Leonid Gurvits, Yuanzhi Li, Michael Walter

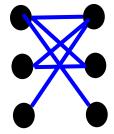
Prehistory

Linial, Samorodnitsky, W 2000 Cool algorithm Discovered many times before

Kruithof 1937 in telephone forecasting,
Deming-Stephan 1940 in transportation science,
Brown 1959 in engineering,
Wilkinson 1959 in numerical analysis,
Friedlander 1961, Sinkhorn 1964 in statistics.
Stone 1964 in economics,

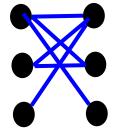
A non-negative matrix. Try making it doubly stochastic.

1	1	1
1	1	0
1	0	0



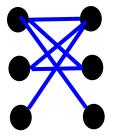
A non-negative matrix. Try making it doubly stochastic.

1/3	1/3	1/3
1/2	1/2	0
1	0	0



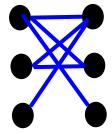
A non-negative matrix. Try making it doubly stochastic.

2/11	2/5	1
3/11	3/5	0
6/11	0	0



A non-negative matrix. Try making it doubly stochastic.

10/87	22/87	55/87
15/48	33/48	0
1	0	0



A non-negative matrix. Try making it doubly stochastic.

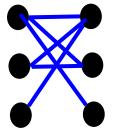
Alternating scaling rows and columns

A very different efficient Perfect matching algorithm

We'll understand it much better with Invariant Theory

0	0	1
0	1	0
1	0	0

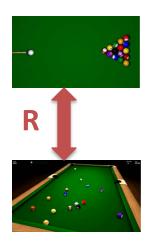
Converges (fast) iff Per(A) >0



Outline

Main motivations, questions, results, structure

- Algebraic Invariant theory
- Geometric invariant theory
- Optimization & Duality
- Moment polytopes
- Algorithms
- Conclusions & Open problems



- Energy
- Momentum

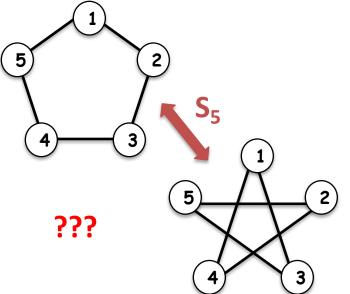
$\begin{array}{l} i,s:=0,0;\\ \mathbf{do}\ i\neq n\rightarrow\\ i,s:=i+1,s+b[i]\\ \mathbf{od} \end{array}$

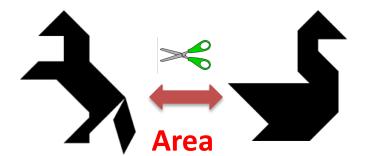
 ${\rm Precondition}\colon\, n\geq 0$

Postcondition: $s = (\sum j : 0 \le j < n : b[j])$

Invariant Theory

symmetries, group actions, orbits, invariants
Physics, Math, CS





Linear actions of groups

Group G acts linearly on vector space $V = F^d$. F = C

Action: Matrix-Vector multiplication G reductive.

G reductive. $g \rightarrow M_g$ rational.

 $M: G \to GL(V)$ ($d \times d$ matrices) group homomorphism.

 $M_g: V \to V$ invertible linear map $\forall g \in G$.

 $M_{g_1g_2} = M_{g_1}M_{g_2}$ and $M_{id} = id$.

Ex 1 $G = S_n$ acts on $V = \mathbb{C}^n$ by permuting coordinates. $M_{\sigma}(x_1, ..., x_n) = (x_{\sigma(1)}, ..., x_{\sigma(n)}).$

Ex 2 $G = GL_n(\mathbf{C})$ acts on $V = M_n(\mathbf{C})$ by conjugation. $M_A X = AXA^{-1}$ $(d = n^2)$ n variables).

Objects of study

Group G acts *linearly* on vector space $V = C^d$, and also on polynomials $C[V] = C[x_1, ..., x_d]$

- Invariant polynomials: under action of G: p s.t. $p(M_g v) = p(v)$ for all $g \in G$, $v \in V$.
- Orbits: Orbit of vector v, $O_v = \{M_g v : g \in G\}$
- Orbit-closures: An orbit \mathcal{O}_v may not be closed. Take its closure in Euclidean topology.

$$\overline{O_v} = \operatorname{cl} \{ M_g v : g \in G \}.$$

$$G = S_n$$
 acts on $V = \mathbb{C}^n$ by permuting coordinates. $M_{\sigma}(x_1, ..., x_n) \to (x_{\sigma(1)}, ..., x_{\sigma(n)}).$

- Invariants: symmetric polynomials.
- Orbits: x, y in same orbit iff they are of same type.

$$\forall c \in C, |\{i: x_i = c\}| = |\{i: y_i = c\}|.$$

Orbit-closures: same as orbits.

$$G=GL_n({m C})$$
 acts on $V=M_n({m C})={m C}^{n^2}$ by conjugation.
$$M_A \ X=AXA^{-1}.$$

- Invariants: trace of powers: $tr(X^i)$.
- Orbits: Characterized by *Jordan normal form*.
- Orbit-closures: differ from orbits.
- 1. $\overline{O_X} \neq O_X$ iff X is not diagonalizable.
- 2. $\overline{O_X}$ and $\overline{O_Y}$ intersect iff X, Y have the same eigenvalues.

Orbits and orbit-closures in TCS

- *Graph isomorphism*: Whether orbits of two graphs the same. Group action: permuting the vertices.
- Border rank: Whether a tensor lies in the orbit-closure of the diagonal unit 3-tensor. [Special case: Matrix Multi exponent] Group action: Natural action of $GL_n(\mathbf{C}) \times GL_n(\mathbf{C}) \times GL_n(\mathbf{C})$.
- PIT Does an $n \times n$ symbolic determinant on m variables vanish? Group action: Natural action of $GL_n(\mathbf{C}) \times GL_n(\mathbf{C}) \times GL_m(\mathbf{C})$.
- Property testing: Graphs Group action: Symmetric group,
 Codes Group action: Affine group
- Arithmetic circuits: The VP vs VNP question via GCT program:
 Whether permanent lies in the orbit-closure of the determinant.
 Group action = Reductions: Action on polynomials induced by linear transformation on variables.

Invariant ring

Group G acts *linearly* on vector space V.

 $C[V]^G$: ring of invariant polynomials.

[Hilbert 1890, 93]: $C[V]^G$ is finitely generated! Nullstellansatz, Finite Basis Theorem etc. proved in these papers as "lemmas"! Also origin of Grobner Basis Algorithm

- 1. $G = S_n$ acts on $V = \mathbb{C}^n$ by permuting coordinates. $\mathbb{C}[V]^G$ generated by *elementary symmetric* polynomials.
- 2. $G = GL_n(C)$ acts on $V = M_n(C)$ by conjugation. $C[V]^G$ generated by $tr(X^i)$, $1 \le i \le n$. Degree bound $\le n$

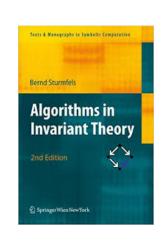
[Derksen 2000]: $C[V]^G$ is generated by degree exp(n)

Computational invariant theory

Highly algorithmic field.

Algorithms sought and well developed.

Polynomial eq sys solving, ideal bases, comp algebra, FFT, MM via groups,...

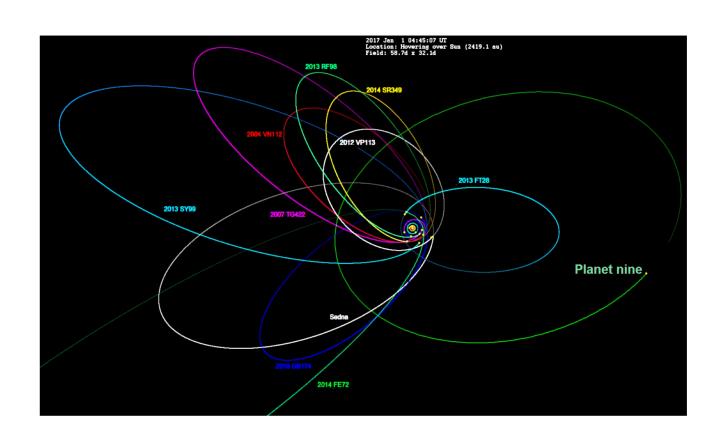




Main problems:

- Describe all invariants (generators, relations).
- Simpler: degree bounds for generating set.
- Isomorphism/Word problem: When are two objects the "same"?
- 1. Orbit intersection.
- 2. Orbit-closure intersection.
- 3. Noether normalization, Mulmuley's GCT5,...
- Orbit-closure containment.
- 5. Simpler: null cone. When is an object ``like" 0? Is $0 \in \overline{O_v}$?

Geometric invariant theory (GIT)



Null cone

Captures many interesting questions.

Group G acts *linearly* on vector space V.

Null cone: Vectors \boldsymbol{v} s.t. 0 lies in the orbit-closure of \boldsymbol{v} .

$$N_G(V) = \{v \colon 0 \in \overline{O_v}\}.$$

Sequence of group elements g_1, \dots, g_k, \dots s.t. $\lim_{k \to \infty} M_{g_k} v = 0$.

Problem: Given $v \in V$, decide if it is in the null cone.

Optimization/Analytic: Is $\inf_{g \in G} ||M_g v|| = 0$?

Algebraic:[Hilbert 1893; Mumford 1965]: v in null cone iff p(v) = 0 for *all* homogeneous invariant polynomials p.

- One direction clear (polynomials are continuous).
- Other direction uses *Nullstellansatz* and algebraic geometry.

analytic ↔ algebraic optimization ↔ complexity

 $G=S_n$ acts on $V=C^n$ by permuting coordinates. $M_{\sigma}(x_1,\ldots,x_n)\to \big(x_{\sigma(1)},\ldots,x_{\sigma(n)}\big).$ Null cone = $\{0\}$.

No closures (same for all finite group actions).

$$G = GL_n(\mathbf{C})$$
 acts on $V = M_n(\mathbf{C})$ by conjugation. $M_A X = AXA^{-1}$.

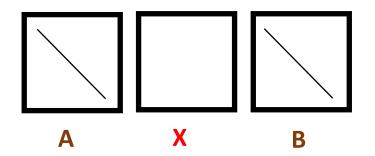
- Invariants: generated by $tr(X^i)$.
- Null cone: nilpotent matrices.

 $G = SL_n(\mathbf{C}) \times SL_n(\mathbf{C})$ acts on $V = M_n(\mathbf{C})$ by left-right multiplication.

$$M_{(A,B)} X = AXB.$$

- Invariants: generated by Det(X).
- Null cone: Singular matrices.

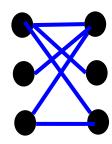
Example 4: Matrix Scaling



 ST_n : group of $n \times n$ diagonal matrices with determinant 1. $G = ST_n \times ST_n$ acts on $V = M_n(C)$ by left-right multiplication. $M_{(A,B)} X = AXB$.

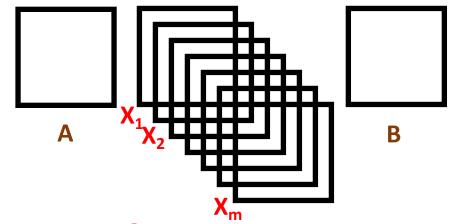
- Invariants: generated by matchings $X_{1,\sigma(1)}X_{2,\sigma(2)}\cdots X_{n,\sigma(n)}$.
- Null cone \leftrightarrow Per(X)=0
- A_H is in null cone \leftrightarrow H has no perfect matching.

1	1	1
1	0	0
1	0	1



H

Example 5: Operator Scaling



$$G = SL_n(\mathbf{C}) \times SL_n(\mathbf{C})$$
 acts on $V = M_n(\mathbf{C})^{\oplus m}$

by simultaneous left-right multiplication.

$$M_{(A,B)}(X_1,...,X_m) = (AX_1B,...,AX_mB).$$
PIT problem

- Invariants [DW 00, DZ 01, SdB 01]: generated by $\text{Det}(\sum_i D_i \otimes X_i)$.
- → Non-commutative rational identity testing
 → ...

[GGOW 16, IQS 16]: Deterministic polynomial time algorithms.



Example 6: Linear programming

```
G = T_n: (Abelian!) group of n \times n diagonal matrices.

V: Laurent polynomials. q \in V (poly w/some exponents negative).

G acts on V by scaling variables. t \in T_n, t = \operatorname{diag}(t_1, \dots, t_n).

M_t \ q(x_1, \dots, x_n) = q(t_1 x_1, \dots, t_n x_n).

q = \sum_{\alpha \in \Omega} c_\alpha x^\alpha. \sup \{q\} = \{\alpha \in \Omega : c_\alpha \neq 0\}.

Null cone \Leftrightarrow Linear Programming \sup \{q\} not in null cone \Leftrightarrow 0 \in \operatorname{conv}\{\sup \{q\}\}. (=Newton polytope \{q\})
```

In non-Abelian groups, the null cone (membership) problem is a non-commutative analogue of Linear Programming.

GIT: computational perspective

What is *complexity* of *null cone* membership? GIT puts it in $NP \cap coNP$ (morally).

- Hilbert-Mumford criterion: how to certify membership in null cone.
- Kempf-Ness theorem:
 how to certify non-membership in null cone.

Many mathematical characterizations have this flavor.

Begs for complexity theoretic quantification

(e.g proof complexity approach to Nullstellensatz, Positivstellensatz...)

Hilbert-Mumford

```
Group G acts linearly on vector space V.
How to certify v \in N_G(V) (null cone)?
Sequence of group elements g_1, \dots, g_k, \dots
such that \lim_{k \to \infty} M_{g_k} v = 0.
```

Compact description of the sequence? Given by one-parameter subgroups.

[Hilbert 1893; Mumford 1965]: $v \in N_G(V)$ iff \exists one-parameter subgroup λ : $C^* \to G$ s.t. $\lim_{t\to 0} M_{\lambda(t)}v = 0$.

One-parameter subgroups

One-parameter subgroup: Group homomorphism $\lambda: \mathbb{C}^* \to G$. Also this map is algebraic.

•
$$G = \mathbf{C}^*$$
: $\lambda(t) = t^a$, $a \in \mathbf{Z}$.

•
$$G = T_n = (\mathbf{C}^*)^{\times n}$$
: $\lambda(t) = \operatorname{diag}(t^{a_1}, \dots, t^{a_n}), \quad a_i \in \mathbf{Z}$.

•
$$G = ST_n$$
: $\lambda(t) = \operatorname{diag}(t^{a_1}, \dots, t^{a_n}), \quad a_i \in \mathbb{Z}, \sum_i a_i = 0$.

• $G = GL_n$: $\lambda(t) = S \operatorname{diag}(t^{a_1}, ..., t^{a_n})S^{-1}$, $S \in GL_n$, $a_i \in \mathbb{Z}$. (Abelian, up to a basis change S)

Example: Matrix Scaling & Perfect Matching

```
G = ST_n \times ST_n (ST_n : n \times n diagonal matrices with det 1) acts on V = M_n (X an n \times n matrix) M_{(A,B)} X = AXB.
```

```
X in null cone \Leftrightarrow \exists a_1, ..., a_n, b_1, ..., b_n \in \mathbf{Z}:
\sum_i a_i = \sum_j b_j = 0
s.t. a_i + b_j > 0 \quad \forall (i,j) \in \operatorname{supp}(X).
\Leftrightarrow \operatorname{Supp}(X) \text{ has no perfect matching (Hall's theorem)}
\operatorname{Supp}(X) = \{(i,j) \in [n] \times [n] : X_{i,j} \neq 0\} \text{ (adjacency matrix of } X)
```

1-parameter subgroups:
$$\lambda(t) = \left((t^{a_1}, \dots, t^{a_n}), (t^{b_1}, \dots, t^{b_n}) \right)$$

$$a_i, b_j \in \mathbf{Z}: \quad \sum_i a_i = \sum_j b_j = 0.$$

$$\lambda(t) \text{ sends } \mathbf{X} \text{ to } \mathbf{0} \iff a_i + b_j > 0 \quad \forall \ (i,j) \in \operatorname{supp}(\mathbf{X})$$

Kempf-Ness

Group G acts linearly on vector space V. How to certify v is not in null cone?

Algebraic: Exhibit *invariant* polynomial p s.t. $p(v) \neq 0$. Typically doubly exponential time...

Invariants hard to find, high degree, high complexity etc.

Analytic: Kempf-Ness provides a more efficient way.

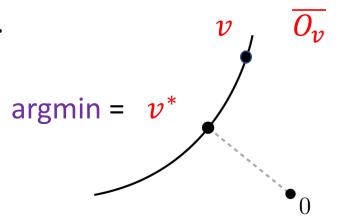
An optimization perspective (+ duality!)

Finding minimal norm elements in orbit-closures!

Group G acts linearly on vector space V.

$$\operatorname{cap}(v) = \inf_{g \in G} \left\| M_g \ v \right\|_2^2.$$

$$cap(v) = 0 \leftrightarrow v \in Null cone$$



$$cap(v) > 0 \leftrightarrow v \notin Null cone$$
 $\leftrightarrow \mu_G(v^*) = 0 \qquad \mu_G \text{ moment map (gradient)}$
 $\leftrightarrow v \text{ can be ``scaled''}$

Minimizing μ_G is a dual optimization problem.

Moment map

Group G acts linearly on vector space V.

Moment map $\mu_G(v)$: gradient of $\|M_g v\|_2^2$ at g = id.

How much *norm* of v decreases by *infinitesimal action* near id.

 $\mu_G(v)$: a linear function (like the familiar gradient), on a linear space called the Lie algebra of the group G.

 μ_G can be defined in more general contexts.

Moment \rightarrow *momentum*.

Fundamental in symplectic geometry and physics.

Minimizing $\mu_G(v)=0$ (finding $\mu_G(v^*)=0$) is a scaling problem!

Example 1: Matrix Scaling

$$G = ST_n \times ST_n$$
 acts on $V = M_n$. $M_{(A,B)} X = AXB$.

Consider only
$$w$$
:
$$\sum_{j} w(j) = 0$$

$$A(s) = \text{diag exp}(s \ q_1), \quad B(s) = \text{diag exp}(s \ q_2)$$
Directional derivative: action of $(A(s), B(s))$ on $X, s \approx 0$.
$$\mu_G(X) = (p_1, p_2), \quad \sum_{i} p_1(i) = \sum_{j} p_2(j) = 0 \text{ s.t.}$$

$$\langle p_1, q_1 \rangle + \langle p_2, q_2 \rangle = \frac{d}{ds} \left[\left\| M_{(A,B)} X \right\|_F^2 \right]_{s=0}^s$$

$$= \langle r_X, q_1 \rangle + \langle c_X, q_2 \rangle$$

$$= \langle r_X - \alpha \mathbf{1}, q_1 \rangle + \langle c_X - \alpha \mathbf{1}, q_2 \rangle$$

 $\mu_G(X) = (r_X - \alpha \mathbf{1}, c_X - \alpha \mathbf{1}), \qquad (\alpha = \langle r_X, \mathbf{1} \rangle = \langle c_X, \mathbf{1} \rangle)$ r_X, c_X vectors of row and $column \ell_2^2$ norms of X.

Scaling = Minimizing $\mu_G(X) = DS G$ -scaling Y of the matrix X.

Example 2: Scaling polynomials

 T_n : (Abelian!) group of $n \times n$ diagonal matrices.

V: Laurent polynomials (with negative exponents).

G acts on V by scaling variables. $t \in T_n$, $t = \text{diag}(t_1, ..., t_n)$.

$$M_t q(x_1, ..., x_n) = q(t_1 x_1, ..., t_n x_n).$$

$$T(s) = \operatorname{diag} \exp(sw)$$
, $w \in \mathbb{R}^n$
Directional derivative: action of $T(s)$ on $q, s \approx 0$.
 $\mu_G(q) = u, \quad u \in \mathbb{R}^n$ s.t.
 $\langle u, w \rangle = \frac{d}{ds} \left[\left\| M_{T(s)} q \right\|_2^2 \right]_{s=0} = \langle \operatorname{grad} \hat{q}(\mathbf{1}), w \rangle$

$$\mu_G(q) = \operatorname{grad} \hat{q}(\mathbf{1})$$
 (the usual gradient)
 $q = \sum_{\alpha \in \Omega} c_{\alpha} x^{\alpha}$ $\hat{q} = \sum_{\alpha \in \Omega} |c_{\alpha}|^2 x^{\alpha}$

Scaling = Minimizing $\mu_G(q)$ = finding extrema of \hat{q}

Kempf-Ness

Group G acts linearly on vector space V.

[Kempf, Ness 79]: \boldsymbol{v} not in null cone iff there exist a non-zero \boldsymbol{w} in orbit-closure of \boldsymbol{v} s.t. $\mu_G(\boldsymbol{w}) = 0$. \boldsymbol{w} certifies \boldsymbol{v} not in null cone.

Easy direction.

- v not in null cone. Take w vector of minimal norm in the orbit-closure of v. w non-zero.
- w minimal norm in its orbit. \Rightarrow Norm does not decrease by infinitesimal action around id. $\Rightarrow \mu_G(w) = 0$.
- *global* minimum \Rightarrow *local* minimum.

Kempf-Ness

Hard direction: *local* minimum \Rightarrow *global* minimum. Some "*convexity*".

• Commutative group actions — Euclidean convexity. (change of variables) [exercise].

Non-commutative group actions: geodesic convexity.

Example: Matrix Scaling

$$G = ST_n \times ST_n$$
 acts on $V = M_n$.
 $M_{(A,B)} X = AXB$.

[Hilbert-Mumford]: X in null cone iff bipartite graph defined by supp(X) does not have a perfect matching.

```
[Kempf-Ness]: X not in null cone \Leftrightarrow \Leftrightarrow non-zero Y in orbit-closure s.t. \mu_G(Y) = 0 \Leftrightarrow \Leftrightarrow X is scalable to ``Doubly Stochastic'' Why only DS?
```

Matrix scaling theorem [Rothblum, Schneider 89].

Moment polytopes

Moment polytopes

Group G acts linearly on vector space V.

```
\Delta= {all gradients} = {\mu_G(w) : w \in V}

\Delta_v= {all gradients in the orbit closure of v} = {\mu_G(w) : w \in \overline{O_v}}

[Atiyah, Hilbert, Mumford]: All "such" are convex polytopes

(\mu_G needs to be normalized, standardized)
```

Uniform Scaling: Given v, does $0 \in \Delta_v$? (null cone problem)

Non-uniform Scaling: Given $v \in V$, r, does $r \in \Delta_v$?

We have algorithms! Polyhedral combinatorics!!

Non-uniform matrix scaling

```
(r,c): probability distributions over \{1,\ldots,n\}.

Non-negative n\times n matrix X.

Scaling of X with row sums r_1,\ldots,r_n

and column sums c_1,\ldots,c_n?

\Delta_X = \{(r,c)\colon r = Y1,c = Y^t1\}.
```

[...; Rothblum, Schneider 89]: Δ_X convex polytope!

Membership: Linear programming

 $\Delta_X = \{(r, c): \exists Z, \text{supp}(Z) \subseteq \text{supp}(X), Z \text{ marginals } (r, c)\}.$ Commutative group actions: classical marginal problems. Also related to maximum entropy distributions.

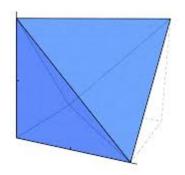
Quantum marginals

Pure quantum state $|\psi\rangle_{S_1,...,S_d}$ (d quantum systems): ψ is a d -tensor

Underlying group action: Products of GL's on d—tensors. (``local'' basis changes in each system)

Characterize marginals $\rho_{S_1}, \dots, \rho_{S_d}$ (marginal states on systems)? Only the spectra of ρ_{S_i} matter (local rotations for free).

- Collection of such spectra Δ_{ψ} convex polytope!
- Follows from theory of *moment polytopes*.
- [BFGOWW 18]: Membership via non-uniform tensor scaling.



More examples of moment polytopes

Schur-Horn: $A n \times n$ symmetric matrix.

$$\Delta_A = \{ \operatorname{diag}(B) : B \text{ similar to } A \} \subseteq \mathbb{R}^n$$

Horn:
$$\Delta = \{(\lambda_A, \lambda_B, \lambda_C): A + B = C\} \subseteq \mathbb{R}^{3n}$$

Brascamp-Lieb: Feasibility of analytic inequalities

Newton: $q = \sum_{\alpha \in \Omega} c_{\alpha} x^{\alpha} \in C[x_1, ..., x_n]$, homogeneous polynomial

$$\Delta_q = \operatorname{conv}\{\alpha : \alpha \in \Omega\} \subseteq \mathbb{R}^n$$

Edmonds: M, M' matroids on [n] (over the Reals).

$$\Delta_{M,M'} = \text{conv}\{ 1_S : S \text{ basis for } M, M' \} \subseteq \mathbb{R}^n$$

Algorithms: membership in moment polytopes

Group G acts linearly on vector space V. $v \in V \leftrightarrow \Delta_v \subseteq \mathbb{R}^n$ moment polytope.

Non-uniform scaling: Given
$$v \in V$$
, $r \in \mathbb{R}^n$, $\epsilon > 0$ does $r \in \Delta_v$ or ϵ —far from Δ_v

For general settings we have efficient:

- Alternating minimization: convergence poly(1/ ϵ)
- Geodesic optimization: convergence polylog(1/ ϵ)

Conclusions & Open problems

Summary: Invariant Theory + ToC

Lots of similar type questions, notions, results

- Algorithms are important, sought and discovered
- Has both an algebraic and analytic nature
- Quantitative, with many asymptotic notions
- Studies families of objects
- Needs comp theory structure, reductions, completeness
- Symmetry is becoming more central in ToC

Summary: Consequences

New efficient algorithmic techniques, solving classes of:

- non-convex optimization problems
- systems of quadratic equations
- linear programs of exponential size

Applicable (or potentially applicable) in:

- Derandomization (PIT)
- Analysis (Brascamp-Lieb inequalities)
- Non-commutative algebra (word problem)
- Quantum information theory (distillation, marginals, SLOCC)
- Representation theory (asymptotic Kronecker coefficients)
- Operator theory (Paulsen problem)
- Combinatorial optimization (moment polytopes)

Open problems

- PIT in **P** ?
- Is PIT a null cone problem?
- Polynomial time algorithms for
- 1. Null cone membership.
- Moment polytopes membership, separation, optimization.
- Extend algorithmic theory to group actions on algebraic varieties, Riemannian/symplectic manifolds

Learn more?

EATCS survey [Garg,Oliveira]

https://arxiv.org/abs/1808.09669

My CCC'17 tutorial:

http://www.computationalcomplexity.org/Archive/2017/tutorial.php

STOC 2018 tutorial:

https://staff.fnwi.uva.nl/m.walter/focs2018scaling/

A week of tutorials:

https://www.math.ias.edu/ocit2018

Mathematics and Computation
New book on my website