Realisability on Dynamical Systems and Complexity

Thomas Seiller
CNRS, LIPN (Paris 13 Univ.)

Workshop on Realisability
June 12th-13th 2018, Marseille

A few definitions

Abstract Programs

Definition

An *abstract model of computation* (AMC) is defined as a monoid action $\alpha : M \curvearrowright \mathbf{X}$ of a monoid $M = \mathrm{M}\langle G, \mathrm{R}\rangle$ on a space $\mathbf{X}$. I.e. a morphism $\alpha : M \to \mathrm{End}(\mathbf{X})$.

Definition (Reductions)

If $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are AMCs, $\alpha \leqslant \beta$ iff there exists an automorphism $\phi : \mathbf{X} \to \mathbf{Y}$ s.t. for all $m \in M_\alpha$, $\phi(\alpha(m))$ is a glueing of a finite number of restrictions of elements $\beta(n_1), \beta(n_2), \ldots, \beta(n_k)$.

Remark

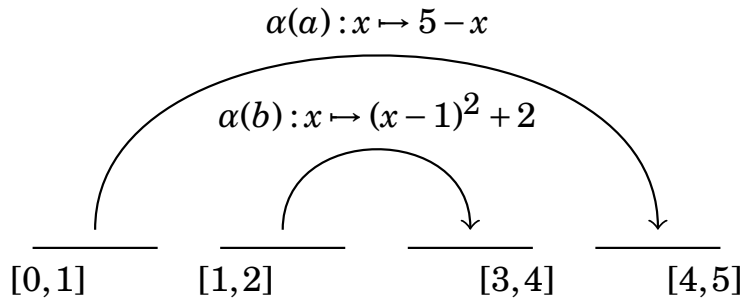
This induces an equivalence relation on AMCs (which is finer than Orbit Equivalence (OE) in the case of groups of m.p.m.).

Definition

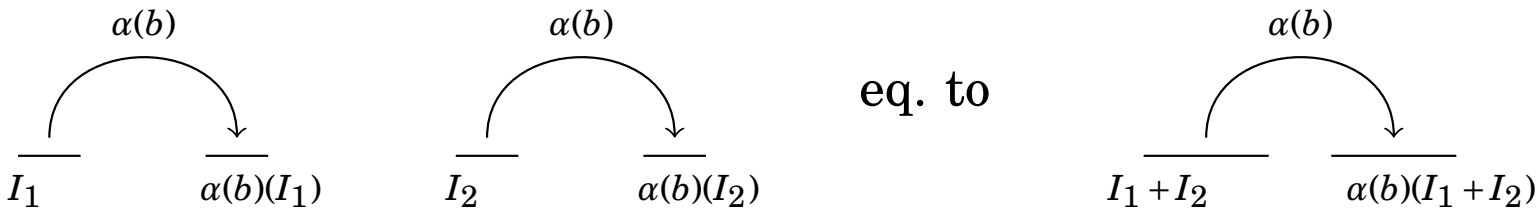
An *abstract program* is a α-graphing.

Wait. What's a graphing?

- Pick a directed graph.
- Replace vertices by (–, resp. open, resp. measurable) subsets of a fixed (discrete, resp. topological, resp. measured) space.
- Decide *how* (i.e. pick an element of M) the edges map sources to targets.



- Then quotient the set of such objects w.r.t. *refinement*:

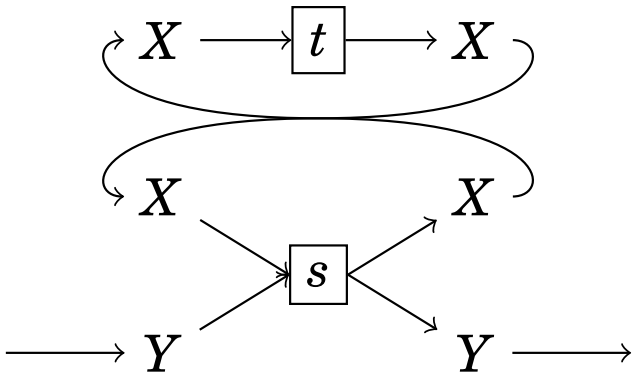


Graphings vs Lambda-Calculus

Lambda	IG	Discrete	Deterministic	Probabilistic
Grammar	AMC	(AMC)	(AMC)	(AMC)
Term	Graphing	Graph	Dyn. System	Markov P.*
Execution	"Paths"	Paths	Max. Finite Orbits	– –
Orthogonality	"Cycles"	Cycles	Infinite Orbits	– –

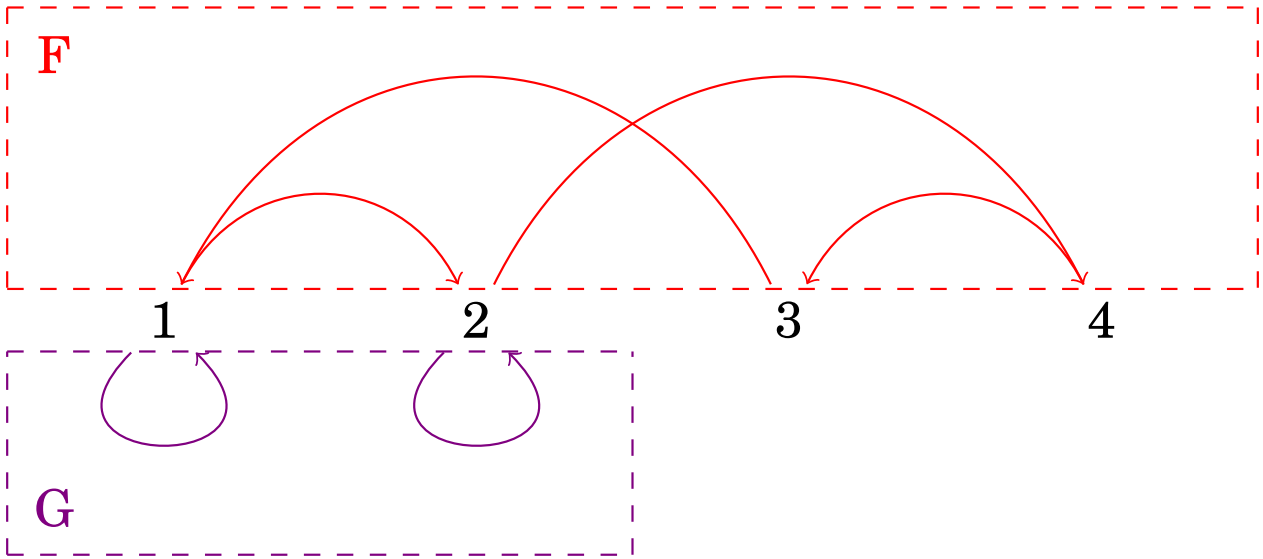
Execution

Execution is defined as follows. Given $s : X + Y \to X + Y$ and $t : X \to X$, we define $s :: t : Y \to Y$ as the fixpoint of:



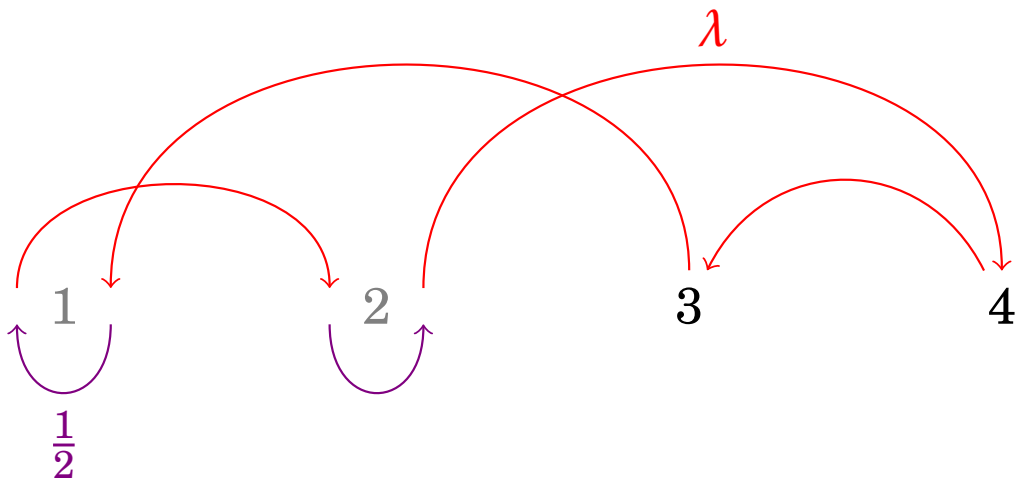
Execution as Paths

The execution $F :: G$ of two graphs F, G is the graph of alternating paths of source and target in $V^F \Delta V^G$.



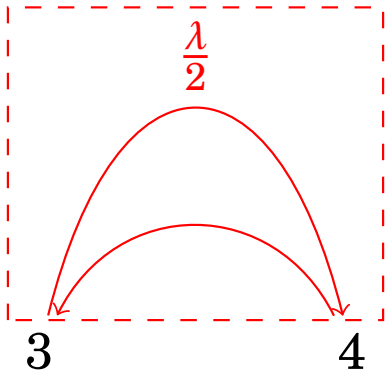
Execution as Paths

The execution $F :: G$ of two graphs F, G is the graph of alternating paths of source and target in $V^F \Delta V^G$.



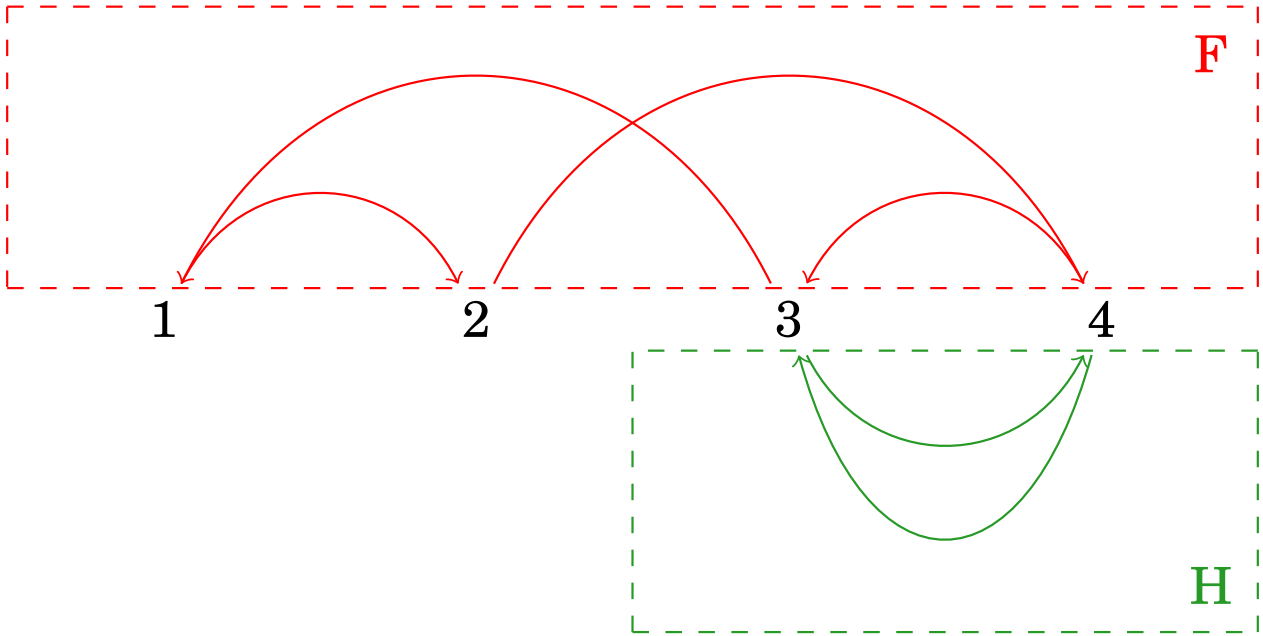
Execution as Paths

The execution $F :: G$ of two graphs F, G is the graph of alternating paths of source and target in $V^F \Delta V^G$.



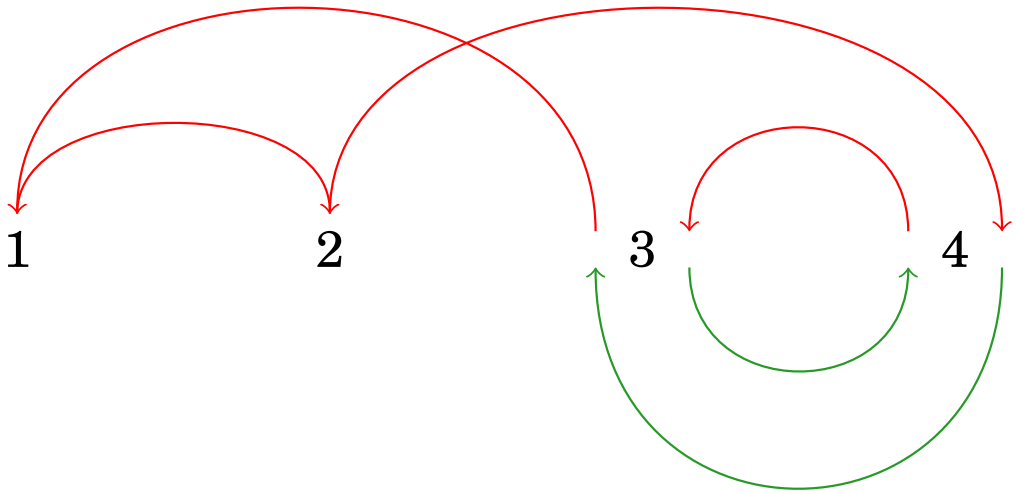
Cycles

In some cases, cycles appear during this operation.



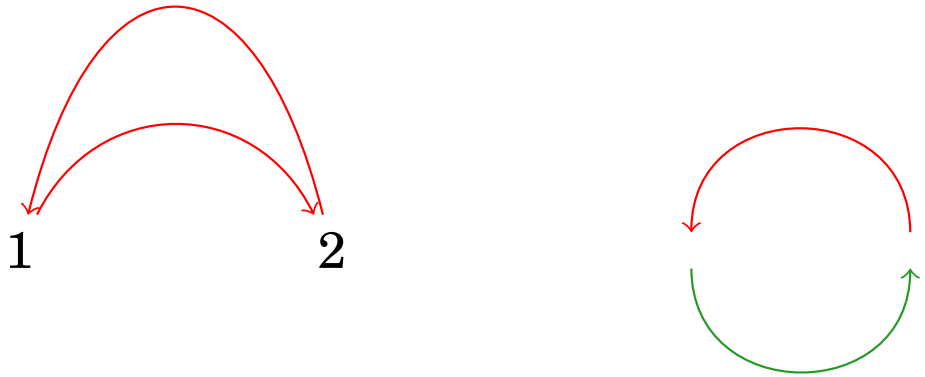
Cycles

In some cases, cycles appear during this operation.

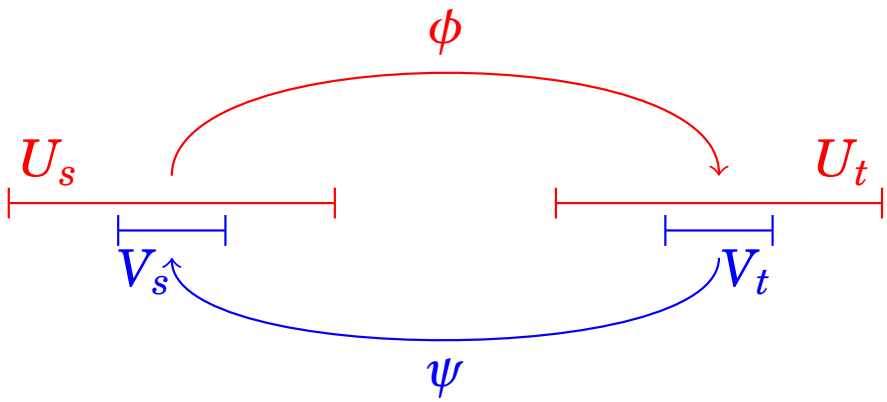


Cycles

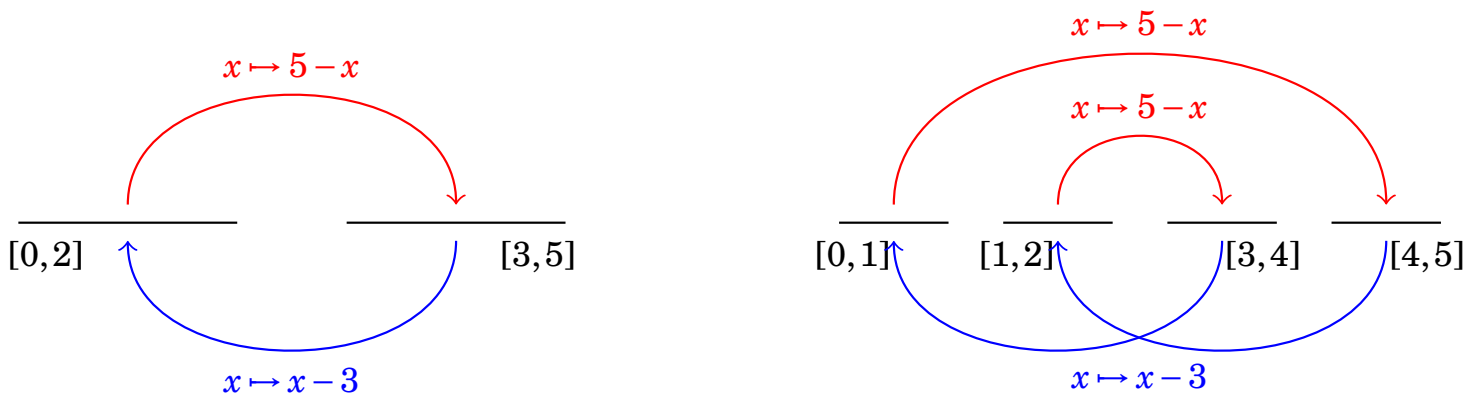
In some cases, cycles appear during this operation.



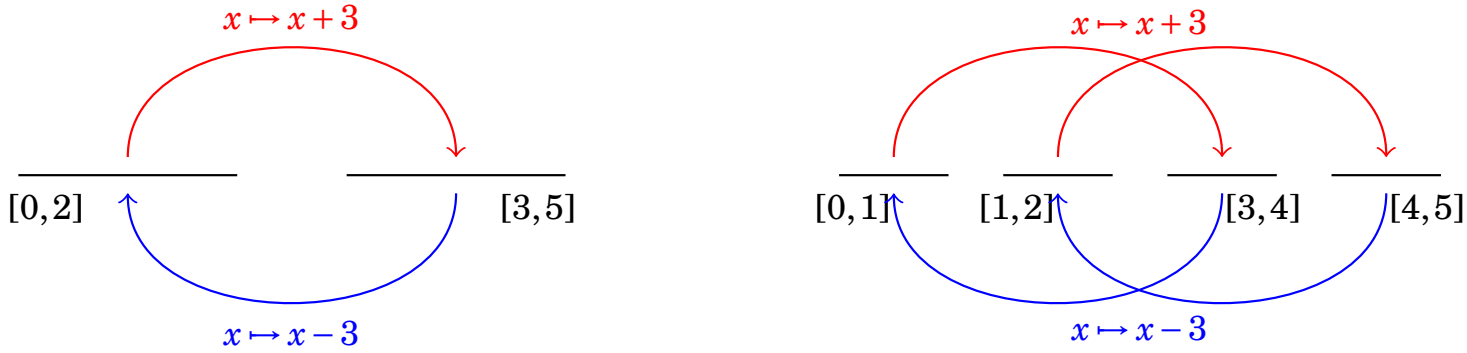
Execution in Graphings



Cycles in Graphings



(a) A cycle can become a longer cycle



(b) A cycle can become two (or more) cycles

Figure: Evolution of cycles through refinement

Orthogonality and Zeta

- Orthogonality in IG: defined by *measuring* cycles.
  - In the case of graphs:
$$[\![F,G]\!]_m = \sum_{\pi \in \mathscr{C}(F,G)} m(\pi)$$
  - In the case of dynamical systems:
$$[\![s,t]\!]_m = \sum_i m(\mathrm{Fix}((st)^i))$$
- This is related to Zeta functions of graphs (Ihara) and dynamical systems (Ruelle, Artin-Mazur):
$$\zeta_G(z) = \prod_{\pi \in \mathscr{C}(G)} (1 - z^{\omega(\pi)})^{-1}$$
$$\zeta_{f,\Phi}(z) = \exp\left(\sum_{m \geqslant 1} \frac{z^m}{m} \sum_{x \in \mathrm{Fix}(f^m)} \mathrm{tr}\left(\prod_{i=0}^{m-1} \phi(f^i(x)) \right) \right)$$

Realisability

- We want: $[\![s, t+t']\!]_m = [\![s::t, t']\!]_m$, but in fact $[\![s, t+t']\!]_m = [\![s::t, t']\!]_m + [\![s, t]\!]_m$. This can be corrected by keeping track of sets of cycles, i.e. t becomes (c, t) with c some term representing a set of cycles (can be the set of cycles itself or its measurement). We keep writing t in the following.
- From $[\![s, t+t']\!]_m = [\![s::t, t']\!]_m$, one can define orthogonality through a pole $\perp \subset \mathrm{Im}([\![\cdot, \cdot]\!]_m)$.
- Define types as sets $\mathbf{A} = \mathbf{A}^{\perp\perp}$, (eq. $\exists B$ s.t. $\mathbf{A} = B^{\perp}$);
- Define $\mathbf{A} \otimes \mathbf{B} = \{s + s' \mid s \in \mathbf{A}, s' \in \mathbf{B}\}^{\perp\perp}$;
- Define $\mathbf{A} \multimap \mathbf{B} = \{t \mid \forall s \in \mathbf{A}, t::s \in \mathbf{B}\}$.
- Check that $\mathbf{A} \multimap \mathbf{B} = (\mathbf{A} \otimes \mathbf{B}^{\perp]})^{\perp}$.

Hierarchies of models

Complexity Constraints

Quantitative Aspects
(e.g. probabilities, effects)

Theorem (Seiller, APAL 2017)

For every monoid of measurable maps $\mathfrak{m}$ *(and every monoid* Ω *, and every measurable map* $g : \Omega \to \mathbf{R}_{\geqslant 0} \cup \{\infty\}$ *), the set of α-graphings defines a non-degenerate model of Multiplicative-Additive Linear Logic .*

Geometric Measurement
(Ihara/Ruelle Zeta Functions)

AT LEAST!

Constraints on Graphings
(e.g. deterministic: (partial) measured dynamical systems,
probabilistic: (discrete time) Markov processes)

Hierarchies of models

Complexity Constraints

Theorem (Seiller, APAL 2017)

For every monoid of measurable maps $\mathfrak{m}$ *(and every monoid* Ω *, and every measurable map* $g : \Omega \to \mathbf{R}_{\geqslant 0} \cup \{\infty\}$ *), the set of* $\mathfrak{m}$*-graphings defines a non-degenerate model of Multiplicative-Additive Linear Logic .*

All Geometry of Interaction constructions are recovered as specific cases

Operators in C* / von Neumann algebras (1989,1990,2011)

Unification/Resolution clauses / Prefix Rewriting (1995,2016)

Complexity

Previous Results

AMC	det. model	non-det. model		prob. model
α_1	REGULAR	REGULAR	REGULAR	STOCHASTIC
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_k	D_k	N_k	co-N_k	P_k
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_∞	LOGSPACE	NLOGSPACE	coNLOGSPACE	PLOGSPACE
β	PTIME	PTIME	PTIME	PTIME?
γ	PTIME	NPTIME	coNPTIME	PP?

Refines and generalises both:

- a series of characterisations of complexity classes (e.g. LOGSPACE, PTIME) by sets of operators (with Aubert), logic programs (with Aubert, Bagnol and Pistone);
- the result where relating the expressivity of GoI models with a classification of *inclusions of maximal abelian sub-algebras*:

$$\ell^\infty(\mathbf{X}) \subseteq \ell^\infty(\mathbf{X}) \rtimes \mathfrak{m}$$

Previous Results

AMC	det. model	non-det. model		prob. model
α_1	REGULAR	REGULAR	REGULAR	STOCHASTIC
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_k	D_k	N_k	co-N_k	P_k
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_∞	LOGSPACE	NLOGSPACE	coNLOGSPACE	PLOGSPACE
β	PTIME	PTIME	PTIME	PTIME?
γ	PTIME	NPTIME	coNPTIME	PP?

- Only known correspondence between infinite hierarchies of mathematical objects and complexity classes.
- Indicates a strong connection between *geometry* and complexity: cf. AMC generalise *group actions*, use of (generalised) Zeta functions, (homotopy) equivalence between microcosms implies equality of the classes.

Previous Results

AMC	det. model	non-det. model		prob. model
α_1	REGULAR	REGULAR	REGULAR	STOCHASTIC
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_k	D_k	N_k	co-N_k	P_k
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_∞	LOGSPACE	NLOGSPACE	coNLOGSPACE	PLOGSPACE
β	PTIME	PTIME	PTIME	PTIME?
γ	PTIME	NPTIME	coNPTIME	PP?

Conjecture

If $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are *separable* (by e.g. ℓ^2-Betti numbers), they characterise different complexity classes.

- Can be checked on classical separation results and the computation of the invariants on the AMCs $\alpha_1, \ldots, \alpha_k, \ldots, \alpha_\infty$.

Dynamic complexity

Definition

An *abstract model of computation* (AMC) is defined as a monoid action $\alpha : M \curvearrowright \mathbf{X}$ of a monoid M on a space $\mathbf{X}$. I.e. $\alpha : M \to \mathscr{M}(\mathbf{X} \to \mathbf{X})$.

Definition

An *abstract program* is a $\alpha(M)$-graphing.

Definition

Define(!) the *dynamic complexity* of a program as the *smallest* (equivalence class of) monoid action $\alpha : M \curvearrowright \mathbf{X}$ needed to interpret it as an abstract program.

Conjecture

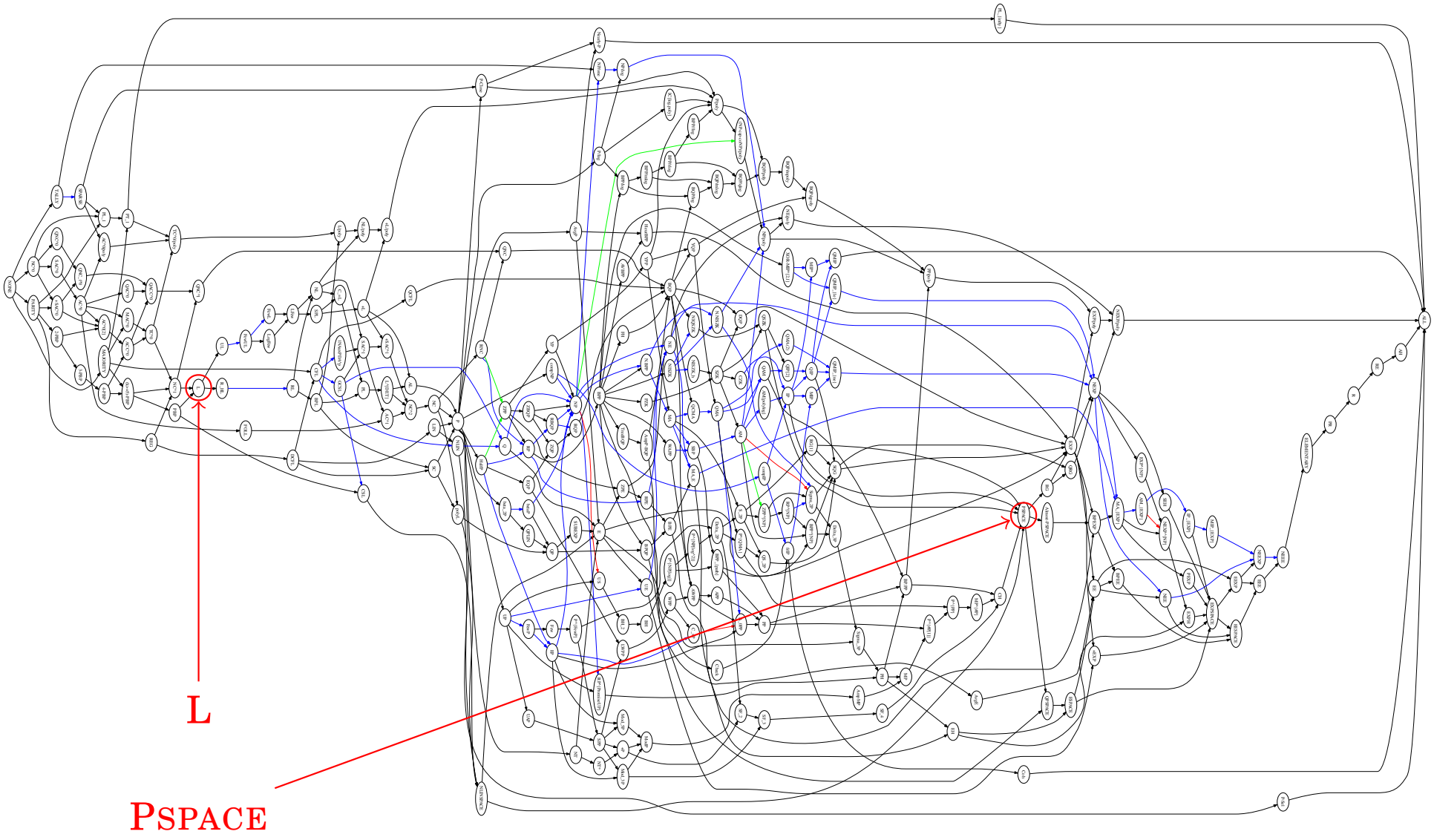
Dynamic complexity of programs coincide* with computational complexity.

Lower Bounds and Barriers

Complexity Theory, Today

- Separation results were obtained, most of them in the 70s, but a lot of questions remain open. E.g. we know $\textsc{Logspace} \subsetneq \textsc{Pspace}$, but not which of these are strict: $\textsc{Logspace} \subset \textsc{NLogspace} \subset \textsc{NC} \subset \textsc{P} \subset \textsc{NP} \subset \textsc{Pspace}$.

Complexity Theory, Today (well, in 2006)



Complexity Theory, Today

- Separation results were obtained, most of them in the 70s, but a lot of questions remain open. E.g. we know $\textsc{Logspace} \subsetneq \textsc{Pspace}$, but not which of these are strict: $\textsc{Logspace} \subset \textsc{NLogspace} \subset \mathrm{NC} \subset \mathrm{P} \subset \mathrm{NP} \subset \textsc{Pspace}$.
- In fact, the three more important results are *negative results* (called *barriers*) showing that known proof methods for separation of complexity classes are inefficient w.r.t. currently open problems. They are: relativisation (1975), natural proofs (1995), and algebrization (2008).
- **Thus: no proof methods for (new) separation results exist today.**
- (Proviso) A single research program is considered as viable for obtaining new results: Mulmuley's *Geometric Complexity Theory* (GCT). According to Mulmuley, **if** GCT produces results, it will not be during our lifetimes (and maybe not our children's lifetime either*). Recent ...

*Well, this depends on the children ages and how long they live, but it is quite unlikely.

Requiem for a Dream

State of the Art in Complexity (Separation Problem): Barriers.

- Relativization/Algebrization (SIAM J. Comp. 1975 / STOC 2008): Proof methods that are oblivious to the use/disuse of oracles are ineffective.

- Natural Proofs (J. Comp. Sys. Sci. 1997): Proof methods expressible as (**Large**, Constructible) predicates on boolean functions are ineffective.

Conclusion: Lack of proof methods for separation.

Geometric Complexity Theory

- GCT is a research program whose aim is to prove PTIME $\neq$ NPTIME using techniques from algebraic geometry (Mulmuley and Sohoni).
- Basically, the goal is to prove that the permanent cannot be embedded in the determinant[†]
- Mulmuley does not expect results within the next 100 years. Recently several drawbacks, in particular closing the easiest path to GCT.

[†]More details: tomorrow's CALIN seminar and subsequent working groups (June 12th and 19th).

Geometric Complexity Theory

- GCT is a research program whose aim is to prove PTIME $\neq$ NPTIME using techniques from algebraic geometry (Mulmuley and Sohoni).
- Basically, the goal is to prove that the permanent cannot be embedded in the determinant[†]
- Mulmuley does not expect results within the next 100 years. Recently several drawbacks, in particular closing the easiest path to GCT.
- Somehow builds on *Algebraic Complexity* (AC) which studies models of computation over arbitrary structures (e.g. the real numbers). Advantages of AC: lower bounds are easier, some successes in proving some bounds on specific computations (e.g. matrix multiplication).

[†]More details: tomorrow's CALIN seminar and subsequent working groups (June 12th and 19th).

Geometric Complexity Theory

- GCT is a research program whose aim is to prove PTIME $\neq$ NPTIME using techniques from algebraic geometry (Mulmuley and Sohoni).
- Basically, the goal is to prove that the permanent cannot be embedded in the determinant[†]
- Mulmuley does not expect results within the next 100 years. Recently several drawbacks, in particular closing the easiest path to GCT.
- Somehow builds on *Algebraic Complexity* (AC) which studies models of computation over arbitrary structures (e.g. the real numbers). Advantages of AC: lower bounds are easier, some successes in proving some bounds on specific computations (e.g. matrix multiplication).
- Initiated after a proof of lower bound for a restricted algebraic PRAM model, which we note PRAM$^-$. This model defines a class NC$^-$ lying within NC (still quite large) and shows it is strictly contained within PTIME.
  This is sometimes considered as the strongest lower bounds result obtained so far.

[†]More details: tomorrow's CALIN seminar and subsequent working groups (June 12th and 19th).

Barriers as Guidelines

State of the Art in Complexity (Separation Problem): Barriers.

- Relativization/Algebrization: Proof methods that are oblivious to the use/disuse of oracles are ineffective.

- Natural Proofs: Proof methods expressible as (**Constructible**, Large) predicates on boolean functions are ineffective.

Barriers as Guidelines

State of the Art in Complexity (Separation Problem): Barriers.

- Relativization/Algebrization: Proof methods that are oblivious to the use/disuse of oracles are ineffective.
  - Separation proof methods should depend on the computational principles allowed in the model.
- Natural Proofs: Proof methods expressible as (**Constructible**, Large) predicates on boolean functions are ineffective.
  - Separation proof methods should not "quotient" the set of programs too much. (by definition, complexity classes are non-decidable predicates on boolean functions)

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?
  - It has to be defined *explicitly*, i.e. extend the AMC by adding a new computational principle as a measurable map $o : \mathbf{O} \to \mathbf{O}$;

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?
  - It has to be defined *explicitly*, i.e. extend the AMC by adding a new computational principle as a measurable map $o : \mathbf{O} \to \mathbf{O}$;
  - Impact the invariants: if $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are separable, there are no reasons to believe that $\alpha + o : M \curvearrowright \mathbf{X}$ and $\beta + o : N \curvearrowright \mathbf{Y}$ are separable.

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?
  - It has to be defined *explicitly*, i.e. extend the AMC by adding a new computational principle as a measurable map $o : \mathbf{O} \to \mathbf{O}$;
  - Impact the invariants: if $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are separable, there are no reasons to believe that $\alpha + o : M \curvearrowright \mathbf{X}$ and $\beta + o : N \curvearrowright \mathbf{Y}$ are separable.
- (Natural Proofs)

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?
  - It has to be defined *explicitly*, i.e. extend the AMC by adding a new computational principle as a measurable map $o : \mathbf{O} \to \mathbf{O}$;
  - Impact the invariants: if $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are separable, there are no reasons to believe that $\alpha + o : M \curvearrowright \mathbf{X}$ and $\beta + o : N \curvearrowright \mathbf{Y}$ are separable.
- (Natural Proofs)
  - The Natural Proofs barrier applies to non-uniform classes.
  - As explained above, the approach should violate the constructivity axiom of the Natural Proof barrier.

Can we jump the barriers?

Why barriers do not apply to this approach:

- (Relativisation/Algebrization)
  - How to describe oracles in this setting?
  - It has to be defined *explicitly*, i.e. extend the AMC by adding a new computational principle as a measurable map $o : \mathbf{O} \to \mathbf{O}$;
  - Impact the invariants: if $\alpha : M \curvearrowright \mathbf{X}$ and $\beta : N \curvearrowright \mathbf{Y}$ are separable, there are no reasons to believe that $\alpha + o : M \curvearrowright \mathbf{X}$ and $\beta + o : N \curvearrowright \mathbf{Y}$ are separable.
- (Natural Proofs)
  - The Natural Proofs barrier applies to non-uniform classes.
  - As explained above, the approach should violate the constructivity axiom of the Natural Proof barrier.
  - More importantly, we can argue that if barriers exists in this setting then the separation problem is undecidable.

Entropy and Lower Bounds

Deterministic graphings

In this work, we only consider *deterministic topological graphings*.

Definition

A graphing on a space $\mathbf{X}$ is deterministic if for all $x \in \mathbf{X}$, x belongs to at most one source. (In measurable case, replace "for all" by "for almost all".)

Proposition

The set of all (–, resp. topological, resp. measurable) graphings over a space $\mathbf{X}$ *is equal to the set of all partial (discrete, resp. topological, resp. measurable) dynamical systems over* $\mathbf{X}$.

Goal

Convince you that invariants of the dynamical systems are relevant tools for the study of computational complexity.

Entropy and Cells

Definition

Let $\mathbf{X}$ be a topological space and $f : \mathbf{X} \to \mathbf{X}$ be a continuous partial map. For any finite open cover $\mathscr{U}$ of $\mathbf{X}$, we define:

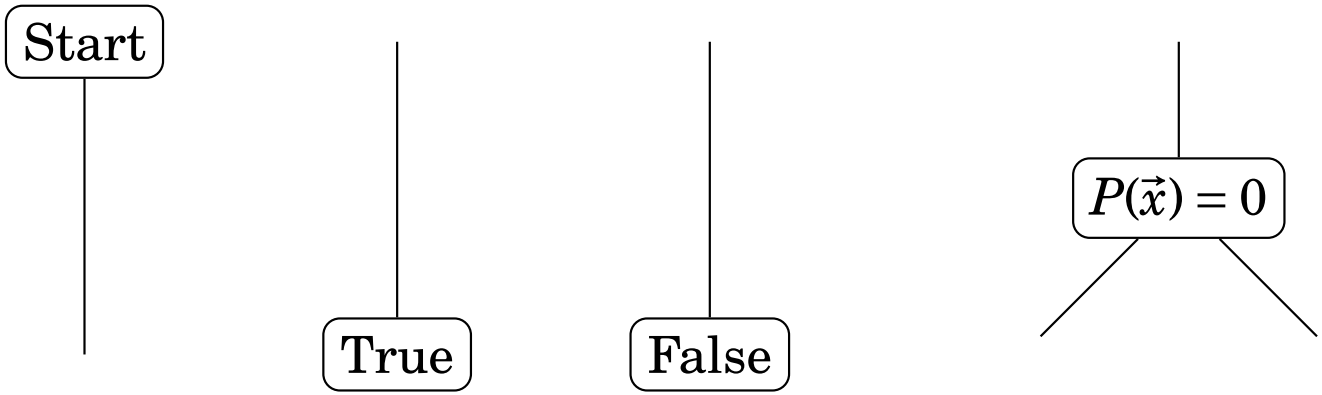
$$H^k_{\mathbf{X}}(f, \mathscr{U}) = \frac{1}{k} H^0_{f^{-k+1}(\mathbf{X})}(\mathscr{U} \vee f^{-1}(\mathscr{U}) \vee \cdots \vee f^{-(k-1)}(\mathscr{U})).$$

The *entropy* of f is then defined as $h(f) = \sup_{\mathscr{U} \in \mathrm{FCov}(\mathbf{X})} h(f, \mathscr{U})$, where $h(f, \mathscr{U})$ is again defined as the limit $\lim_{n \to \infty} H^n_{\mathbf{X}}(f, \mathscr{U})$.

Proposition

Let G be a deterministic graphing, with entropy $h(G)$. The cardinality of the k-th cell decomposition of $\mathbf{X}$ w.r.t. G, as a function $c(k)$ of k, is asymptotically bounded by $g(k) = 2^k 2^{h([G])}$, i.e. $c(k) = O(g(k))$.

Lower Bounds results I: Algebraic Decision Trees



Lemma

Let G be a regular deterministic graphing interpreting an algebraic decision tree of max degree d. The k-th cell decomposition of $\mathbf{X}$ w.r.t. G is determined by at most 2^k algebraic varieties of degrees bounded by d.

The Milnor-Thom theorem

Theorem (Milnor, Thom)

Let V be an algebraic variety $\subset \mathbf{R}^m$, defined by a polynomial of degree at most d. The sum of the Betti numbers of V is not greater than $d(2d-1)^{m-1}$.

Corollary

Let (S) be a system of s polynomial equations and inequalities in k variables, of degrees at most $d \geqslant 2$. The number of connected components of the set of solutions of (S) in $\mathbf{R}^n$ is not greater than $d(2d-1)^{k+s-1}$.

Remark

There are better bounds, e.g. Roy ($s^k O(d)^k$).

Lower Bounds results I: Algebraic Decision Trees

Lemma

Let G be a regular deterministic graphing interpreting an algebraic decision tree of max degree d. The k-th cell decomposition of $\mathbf{X}$ w.r.t. G is determined by at most 2^k algebraic varieties of degrees bounded by d.

- This gives lower bounds for deciding (semi-)algebraic sets. E.g.

Example 3. Set Disjointness. *Given two sets $A = \{x_1, \ldots, x_n\}$ and $B = \{y_1, \ldots, y_n\}$, determine whether or not $A \cap B = \emptyset$.*

For this problem set

$$W = \left\{ (x_1, \ldots, x_n, y_1, \ldots, y_n) \,\middle|\, \prod_{i,j} (x_i - y_j) \neq 0 \right\}$$

It is easy to see that $\#W \geq (n!)^2$, so again we know that $C(W), M(W), C_d(W) = \Omega(n \log n)$.

A second separation result

Lower Bounds results II: Algebraic circuits

Proposition

Let $f_n \in \mathbf{R}[X_1,\ldots,X_n], n \in \mathbf{Z}$, be a family of nonconstant irreducible polynomials such that for each n, the zero set $\mathcal{Z}(f_n)$ is a variety of dimension $n-1$. Let $d(n) = \deg(f_n)$. Then any parallel machine deciding the set $S = \{x \in \mathbf{R}^\infty \mid f_{\mathrm{size}(x)}(x) = 0\}$ has running time greater than $\log d(n)$.

Proposition

The same problem with the family of polynomials $X_1 - X_2^{2^n}$ is computable in polynomial (even linear) time in the real BSS model.

Theorem

$$\mathrm{NC}_{\mathbf{R}} \subsetneq \mathrm{Ptime}_{\mathbf{R}}$$

PRAMs w/o bit operations

Definition

A SRAM *command* is a pair (ℓ, I) of a *label* (or *line*) $\ell \in \mathbf{N}^\star$ and a *command* $\mathtt{I}$ among the following ($i,j \in \mathbf{N}$, $\ell, \ell' \in \mathbf{N}^\star$ labels):

$$\begin{array}{rcl} \text{Commands} & := & \mathtt{skip}; \quad \mathtt{X_i} := \mathtt{X_i} + 1; \quad \mathtt{X_i} := \mathtt{X_i} - 1; \\ & & \mathtt{X_i} := \mathtt{X_j}; \quad \mathtt{X_i} := \sharp\mathtt{X_j}; \quad \sharp\mathtt{X_i} := \mathtt{X_j}; \\ & & \mathtt{if}\ \mathtt{X_i} = 0\ \mathtt{goto}\ \ell\ \mathtt{else}\ \ell'; \end{array}$$

Definition

A PRAM machine M is simply given as a finite sequence of SRAM machines $M_1, \ldots, M_p$, where p is the number of *processors* of M. Each processor M_i has access to its own, private, set of registers $(\mathtt{X}^i_k)_{k \geqslant 0}$ and a *shared memory* represented as a set of registers $(\mathtt{X}^0_k)_{k \geqslant 0}$.

PRAMs w/o bit operations

Definition

A PRAM machine M is simply given as a finite sequence of SRAM machines $M_1,\ldots,M_p$, where p is the number of *processors* of M. Each processor M_i has access to its own, private, set of registers $(\mathrm{X}^i_k)_{k\geqslant 0}$ and a *shared memory* represented as a set of registers $(\mathrm{X}^0_k)_{k\geqslant 0}$.

Lemma

Let G be a regular deterministic graphing interpreting a PRAM *with p processors. The k-th cell decomposition of $\mathbf{X}$ w.r.t. G is determined by at most $2^k p^k$ algebraic varieties of degree at most 2^k.*

Lower Bounds results III

The following result provides a geometric representation of a PTIME-complete problem on $\mathbf{R}^3$. (Need whiteboard here.)

Theorem (Murty, Carstensen)

1. *there exists an affine parametrization of bitsize $O(n)$ and complexity $2^{\Omega(n)}$ of combinatorial linear programming, where n is the total number of variables and constraints of the problem.*
2. *there exists an affine parametrization of bitsize $O(n^2)$ and complexity $2^{\Omega(n)}$ of the maxflow problem for directed and undirected networks, where n is the number of nodes in the network.*

Lower Bounds results III-2

Definition

Let K be a compact of $\mathbf{R}^3$.
A finite set of surfaces S on K *separates* a ρ-fan **Fan** on K if the partition on $\mathbf{Z}^3 \cap K$ induced by S is finer than the one induced by **Fan**.

Theorem (Mulmuley)

Let S be a finite set of algebraic surfaces of total degree δ.
There exists a polynomial P such that, for all $\rho > P(\delta)$, S does not separate ρ-fans.

Corollary

Let G be a deterministic graphing interpreting a PRAM *without bit operations with $2^{O(N^c)}$ processors (N is the length of the inputs and c any positive integer).*
G does not decide maxflow in $O(N^c)$ steps.

Theorem

$$\mathrm{NC}^{\mathrm{PRAM}^-} \subsetneq \mathrm{Ptime}$$

A Remark

- Algebraic Computational Trees.
  - Results of Dobkin and Lipton, Yao, Steele and Yao, Ben-Or –> 83.
- Algebraic Circuits and Algebraic Ptime.
  - Result of Cucker –> 92
- PRAMs w/o bit operations.
  - Result of Mulmuley –> 99

A Remark

- Algebraic Computational Trees.
  - Results of Dobkin and Lipton, Yao, Steele and Yao, Ben-Or –> 83.
  - Not cited by Cucker
  - Not cited by Mulmuley
- Algebraic Circuits and Algebraic Ptime.
  - Result of Cucker –> 92
- PRAMs w/o bit operations.
  - Result of Mulmuley –> 99

A Remark

- Algebraic Computational Trees.
  - Results of Dobkin and Lipton, Yao, Steele and Yao, Ben-Or –> 83.
  - Not cited by Cucker
  - Not cited by Mulmuley
- Algebraic Circuits and Algebraic Ptime.
  - Result of Cucker –> 92
  - Not cited by Mulmuley
- PRAMs w/o bit operations.
  - Result of Mulmuley –> 99

Realisability on Dynamical Systems and Complexity

Thomas Seiller
CNRS, LIPN (Paris 13 Univ.)

Workshop on Realisability
June 12th-13th 2018, Marseille

Realisability on Dynamical Systems and Complexity

Thomas Seiller
CNRS, LIPN (Paris 13 Univ.)

Workshop on Realisability
June 12th-13th 2018, Marseille