Algebraic proof complexity

Jan Krajíček

Charles University in Prague

language L is in class $\mathcal{NP}$

$$\Updownarrow$$

$\exists$ a proof system $R(x, y)$:

1. $u \in L$ iff $\exists v \;\; R(u, v)$

2. $R(x, y)$ is p-time decidable

which is p-bounded:

3. $R(u, v) \;\longrightarrow\; \exists w \;\; (|w| \leq |u|^c \wedge R(u, w))$

Basic example: 3SAT

satisfiable 3CNF formulas

$$C_1 \wedge \ldots \wedge C_k$$

with each clause C_i having 3 literals, e.g.

$$C_i \quad : \quad (x_r \vee \overline{x}_s \vee \overline{x}_t)$$

Theorem (Cook'71)

3SAT is $\mathcal{NP}$-complete: every other problem in the class can be polynomially reduced to 3SAT.

In particular,

$$\mathcal{P} = \mathcal{NP} \text{ iff } \text{3SAT} \in \mathcal{P}$$

$co\mathcal{NP}$: complements of languages from $\mathcal{NP}$

Observation

$$\varphi \notin \text{3SAT} \quad \text{iff} \quad \neg\varphi \in \text{TAUT}$$

A consequence of Cook's theorem:

$$\mathcal{NP} = co\mathcal{NP} \quad \text{iff} \quad \text{TAUT} \in \mathcal{NP}$$

Conjecture

$$\mathcal{NP} \neq co\mathcal{NP}$$

which implies also $\mathcal{NP} \neq \mathcal{P}$.

Propositional proof complexity:

Show that no proof system for TAUT can be p-bounded.

[Cook's program]

A shift to algebra:

replace TAUT by a *natural* $co\mathcal{NP}$-complete problem and study proof systems for it.

Examples

- unsolvable polynomial systems over a finite field

- 0-1-unsolvable systems of integer linear inequalities

  [has a more geometric flavor]

- aux.: Dehn function and lengths-of-proofs function, model theory, ...

Fix a finite prime field F_p.

Polynomial system:

$$f_i \ = \ 0 \ , \quad \text{for} \quad i = 1, \ldots, k$$

where

- $f_i \in F_p[x_1, \ldots, x_n]$
- f_i's include all polynomials

$$x_j^p - x_j$$

Nullstellensatz provides a natural proof system for showing the unsolvability:

$$\{f_i = 0\}_i \text{ has no solution in } F_p$$

$$\Updownarrow$$

$$\{f_i = 0\}_i \text{ has no solution in } F_p^{acl}$$

$$\Updownarrow$$

for some $\{g_i\}_i$:

$$\sum_i g_i \cdot f_i \; = \; 1 \; .$$

An NS-proof: any such tuple $(g_1, \ldots, g_k)$

A subtle point: how can we verify in p-time an alleged NS-proof?

Polynomial Identity Testing

Decide if

$$f = g$$

holds in $F_p[x_1, \ldots, x_n]$.

Fact

If f, g are given by general terms, it is not known if PIT can be done in p-time (yes, if randomization is used).

A simple special case which is OK:

polynomial = an explicit sum of monomials

Note that then:

$$\text{size } \sim n^{\text{deg}}$$

super-polynomial size $\Leftrightarrow$ unbounded degree

The task

Find an unsolvable polynomial system

$$\{f_i = 0\}_i$$

of bounded degree requiring NS-proofs of unbounded degree, i.e.

$$\max_i deg(f_i)$$

is bounded by a constant independent of n, k while

$$\max_i deg(g_i)$$

is unbounded as $n, k \to \infty$.

A general context from algebraic geometry:

the effective NS of Brownawell, Kollar, ...
(late '80s)

Examples given that require exponential degree (in n) NS-proofs over an algebraically closed field.

When equations $x_j^p - x_j = 0$ are added these bounds collapse to a constant.

Note In our case the degree is a priori at most $(p-1)n$.

Fix $q \geq 2$ s.t. $q \not\equiv 0 \pmod{p}$, and any $N \geq 2$ s.t. $N \not\equiv 0 \pmod{q}$.

The (N, q)-system. Variables:

$$x_e, \text{ for } e \subseteq [N] := \{1, \ldots, N\} \text{ s.t. } |e| = q$$

equations:

- $x_e^2 - x_e = 0$

- $x_e \cdot x_f = 0$, if $e \perp f$ which abbreviates
$$e \neq f \wedge e \cap f \neq \emptyset$$

- $(1 - \sum_{e:i \in e} x_e) \ = \ 0$, any $i \in [N]$.

A potential solution would define a q-partition of $[N]$: unsolvable.

Theorem (Beame, Impagliazzo, K., Pitassi, Pudlák '96)

The (N, q) system has no bounded degree NS-proofs.

Later improved to N^{ϵ} degree lower bound by (Buss, Impagliazzo, K., Pudlák, Razborov, Sgall '97)

The (N, q)-system is an example of a symmetric polynomial system:

Informal definition

- there is a parameter $N \geq 2$ determining the system

- variables are indexed by bounded size structures with universes inside $[N]$

  here simply subsets $e \subseteq [N]$ of size q

- every permutation π of $[N]$ induces a permutation of the variables and hence maps equations into equations

  $x_e \cdot x_f \mapsto x_{\pi(e)} \cdot x_{\pi(f)}$

- the system is invariant under all such maps

  if $e \perp f$ then also $\pi(e) \perp \pi(f)$

Ajtai: a work on symmetric systems of linear equations over F_p

(uses the characteristic-free representation theory of S_N of James)

Key example

Fix $d \geq 2$ and let $L_d(N)$ be the system of linear equations for coefficients of a degree $\leq d$ NS-proof $(g_1, \ldots)$ for the (N, q)-system.

Observation

$L_d(N)$ is symmetric. In particular, the variables are indexed by monomials of degree at most d, i.e. by $\leq d$-tuples of subsets of $[N]$ of size q.

Theorem (Ajtai '94)

For any symmetric system of linear equations $L(N)$ there is an $\ell \geq 1$ such that for $N >> 0$ the solvability of $L(N)$ in F_p depends only on the remainder

$$N \bmod p^\ell .$$

Observation

In any remainder class mod p^ℓ we can find N divisible by q. For such N:

- the (N, q)-system has a solution
- and hence no $L_d(N)$ has a solution, i.e. there are no degree $\leq d$ NS-proofs.

Generalizing a bit Ajtai's work in the direction of the definability of generators for submoduli of tabloid moduli ($F_p[S_N]$-moduli with Young tableaux) I proved (K. '00 and '01) that

- a lower bound $\Omega(\log N)$ for NS-proofs can be, in fact, deduced

- this whole theory applies to a stronger proof system PC (next slide) and gives there $\Omega(\log \log N)$ degree lower bounds

- a a model-theoretic criterion for symmetric polynomial systems can be formulated implying such lower bounds

  (the existence of a first-order structure with certain properties in terms of an abstract Euler characteristic in the sense of Schanuel)

Polynomial calculus PC

The NS proof system witnesses the triviality of the ideal $\langle f_i \rangle_i$ "statically": it produces at once a linear expression for 1 in terms of the generators.

The PC proof system deduces the triviality "sequentially": it proves gradually the membership of more and more polynomials in the ideal using two rules:

$$\frac{f \qquad\quad g}{f+g}$$

and

$$\frac{f}{h \cdot f}\ , \quad \text{any } h \in F_p[\overline{x}]$$

until 1 is derived.

Observation

The minimal PC-degree is at most the minimal NS-degree.

Theorem (K. '01)

The degree of PC proofs of the (N, q)-systems is at least $\log \log N$.

Earlier lower bound (Razborov '98)

An $N/2$ lower bound for the degree of PC-proofs for another polynomial system (encoding PHP).

A yet stronger proof system F:

- uses arbitrary terms to represent polynomials

- uses equational logic over the commutative ring axioms to derive new terms from initial terms (elements of the polynomial system)

For F we cannot define the size in terms of the degree as for NS and PC: we want a lower bound for the total number of symbols in all terms in a proof.

Open problem

Prove a super-polynomial lower bound on the size of F-proofs.

Sad fact

Only quadratic lower bound is known.

A broader perspective

We aim at

- $\mathcal{NP} \neq co\mathcal{NP}$, i.e. proof-hardness

which implies

- $\mathcal{P} \neq \mathcal{NP}$, i.e. computational-hardness.

No reason to shy away from using a suitable

computational hardness hypothesis!

A form of **hardness hypothesis**

"Every Boolean circuit performing
a specific task must be large."

Examples

- $\mathcal{P} \neq \mathcal{NP}$ if circuits solving SAT must be super-polynomial

- $\mathcal{P} = \mathcal{BPP}$ if circuits solving some problem in $\mathcal{E}$ must be exponential

- PRNG exists if circuits computing factoring with a non-negligible success must be super-polynomial

Task (hope)

Extract some computational information from a proof of unsolvability of a polynomial system.

Example

of an idea which works for systems weaker than F:

feasible interpolation

(K. early 90s, then Razborov, and Bonet-Pitassi-Raz, and K.-Pudlák, and ....)

To simplify assume $p = 2$.

Consider an unsolvable system

$$f_i(\overline{x}, \overline{y}) = 0 \quad \text{and} \quad g_j(\overline{x}, \overline{z}) = 0$$

where

$$\overline{x} = (x_1, \ldots, x_n)$$

are the only common variables.

Definition

$U := \{\overline{a} \in \{0,1\}^n \mid \{f_i(\overline{a}, \overline{y}) = 0\}_i$ is solvable $\}$

$V := \{\overline{a} \in \{0,1\}^n \mid \{g_j(\overline{a}, \overline{z}) = 0\}_j$ is solvable $\}$

Facts

$$U \cap V = \emptyset$$

and any pair of disjoint $\mathcal{NP}$-sets can be defined in this way, by a system of total size $n^{O(1)}$.

Theorem Assume P is a degree d NS-proof of the unsolvability of the system and that $U \cup V = \{0,1\}^n$.

Then there is a polynomial time algorithm deciding for an input $a \in \{0,1\}^n$ whether $a \in U$ or $a \in V$.

Claim One of the systems

$$\{f_i(a,y) = 0\}_i \text{ or } \{g_j(a,z) = 0\}_j$$

has a degree d NS-proof.

Proof-claim

Substitute $x := a$ in P. It becomes an NS-proof of unsolvability of

$$\{f_i(a,y) = 0,\ g_j(a,z) = 0\}_{i,j}\ .$$

As a belongs to either U or V, one can further substitute in P for either y to satisfy the f-system, or for z to to satisfy the g-system.

The algorithm

Given an input $a \in \{0,1\}^n$, look for a solution of the linear system for coefficients of polynomials in degree d NS-proofs for

$$\{f_i(a,y) = 0\}_i \text{ and } \{g_j(a,z) = 0\}_j \ .$$

One of them has a solution and this gives the answer.

Hardness hypothesis

Hard to separate pairs of disjoint $\mathcal{NP}$-sets exists.

RSA example

U: encryptions of bit 0

V: encryptions of bit 1

Summary

One derives a degree lower bound for NS from the security of RSA.

Remarks

(1)

An analogous theory exists for many proof systems, and there are generalizations proposed that - it is hoped - may work also for F.

(2)

It is consistent with the present knowledge that the proof system F is optimal: no other proof system has a super-polynomial speed-up.

In such a case it would hold

$$\mathcal{NP} \neq co\mathcal{NP} \quad \text{iff} \quad F \text{ is not p-bounded.}$$

Hence it may only take to prove a lower bound for equational logic to ... .