Hilbert Nullstellensatz is in the Polynomial Hierarchy

Presentation by: Ashish Dwivedi
Paper by: Pascal Koiran

Depatment of Computer Science and Engineering
IIT Kanpur

November 11, 2017

Hilbert's Nullstellensatz

- Consistency Question: Does given polynomials $f_1(\overline{x}), \ldots, f_m(\overline{x}) \in \mathbb{F}[\overline{x}]$ have a common zero over $\overline{\mathbb{F}}$?
- Hilbert's Nullstellensatz (HN) says- answer is "NO" iff,

$$1 = a_1 f_1 + \ldots + a_n f_n$$

  for some $a_1, \ldots, a_n \in \overline{\mathbb{F}}[\overline{x}]$.
- Nullstellensatz= Null (Zero)+ Stellen (Places)+ Satz (Theorem). "Theorem of zeros".
- Hence, consistency checking is also called HN.

The Problem

- We are interested in the complexity of HN over $\mathbb{C}$.
- Input is a system $\mathcal{F} = \{f_1, f_2, \ldots, f_m\}$, where $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ with coefficients at most C and total degree at most d.
- Question: Is $\mathcal{F}$ satisfiable over $\mathbb{C}$?
- $|\mathcal{F}|$ is the bit size of the system.
- Sparse representation to represent polynomials.

- Koiran (1996) showed that this problem is in the polynomial hierarchy assuming Riemann hypothesis.
- In particular, he put the problem in "Arthur-Merlin" (AM) class.
- To understand the main idea, we need to see systems over $\mathbb{Z}$ as systems modulo p for prime p.

Some Examples

- Consider the following satisfiable system S over $\mathbb{Z}[x, y]$,

$$S = \begin{cases} xy - 6 = 0 \\ x - 2 = 0 \end{cases}$$

satisfiable over $\mathbb{Z}$- (2,3).

- What about its satisfiability is $\mathbb{Z}/p\mathbb{Z}$ for some prime p?
- It is satisfiable for all such p's- zeros are (2 mod p, 3 mod p).
- In $[N]$ it has $\pi(N)$ - number of primes in $[N]$ - solutions.

Some Examples

- Consider an unsatisfiable system S over $\mathbb{Z}[x, y]$,

$$S = \begin{cases} (xy)^6 - 1 = 0 \\ x - 2 = 0 \\ y - 3 = 0 \end{cases}$$

- What about its satisfiability is $\mathbb{Z}/p\mathbb{Z}$ for some prime p?
- It is satisfiable with zero (2 mod 5, 3 mod 5) in $\mathbb{Z}/5\mathbb{Z}$ and (2 mod 7, 3 mod 7) in $\mathbb{Z}/7\mathbb{Z}$
- But we can see the number of zeros are bounded - for any prime $p > 6^6$ it is unsatisfiable in $\mathbb{Z}/p\mathbb{Z}$

Some Examples

- Consider the given system of equation over $\mathbb{Z}[x, y, z]$

$$S = \begin{cases} xy - z^2 = 0 \\ 2x - 1 = 0 \\ x - 9y = 0 \end{cases}$$

- Satisfiable over $\mathbb{C}$- $(1/2, 1/18, \pm 1/6)$ or $(9/18, 1/18, \pm 3/18)$
- It is satisfiable for all primes p except $p = 2, 3$.
- 18 doesn't have inverse modulo 2 or 3.
- In $\mathbb{Z}/5\mathbb{Z}$ it has a solution $(3, 2, 1) \equiv (9.18^{-1} \bmod 5, 1.18^{-1} \bmod 5, 3.18^{-1} \bmod 5)$.
- In $[N]$, satisfiable for $\pi(N) - 2$ primes.

- What we observe by these examples?
- Do satisfiable systems over $\mathbb{C}$ are always satisfiable for unbounded number of primes p?
- Do unsatisfiable systems over $\mathbb{C}$ are satisfiable for only few primes p?

- The answer to all these questions is - Yes!
- There is a large gap between number of primes in the two cases.
- We will prove that-
  - If $\mathcal{F}$ is unsatisfiable over $\mathbb{C}$ then for at most N_1 primes p, $\mathcal{F}$ will be satisfiable modulo p, where $N_1 = exp(|\mathcal{F}|)$.
  - If $\mathcal{F}$ is satisfiable over $\mathbb{C}$ then, assuming ERH, for at least $N_2 := (\pi(N)/N_3 - N_4 - O(\sqrt{N}\log N))$ primes p in [N], $\mathcal{F}$ will be satisfiable modulo p where N_3 and N_4 are constants at most $exp(|\mathcal{F}|)$.
- $\pi(N) >> \sqrt{N}\log N$.
- $N = exp(|\mathcal{F}|)$ suffices for $N_2 >> N_1$

- We will exploit this large gap to put the question in AM.
- Class AM $\subseteq \Pi_2$ (second level in PH).
- We will first show that HN is in AM and then prove the statements about number of good primes in the two cases.
- Since, N_2 is arbitrarily large we can take $N_2 > 4N_1$.

- Let universe U is the set of all prime numbers in [N].
- For input x, $Good(x)$ is set of all primes in U for which x is satisfiable.
- Membership testing in $Good(x)$ is in NP.
- A direct way for AM protocol can be:
  - Arthur picks a random y in U and gives it to Merlin.
  - Merlin gives a certificate that $y \in Good(x)$.
  - Arthur verifies efficiently.
- Problem is that $|U|$ can be exponentially large than N_2, so probability for yes instance $N_2/|U|$ is very small.

- The good thing is that N_2 is relatively much larger than N_1.
- We can use the idea of hashing discussed in last lecture.
- We contract the space size and hashing on average will maintain this relativity.
- We use pairwise independent family of hash functions $\mathcal{H}$ from U to S, where S is a set of size N_2.
- Pick a subset $T \subseteq U$ s.t. $|T| = \alpha|S|$ with $\alpha \leq 1$.
- For random h and $x \in S$,
  $\alpha - \alpha^2/2 \leq \Pr[x \in h(T)] \leq \alpha$

- Take $T = Good(x)$.
- Then for no instance x, Prob $\leq \alpha = |T|/|S| = 1/4$
- For yes instance x, Prob $\geq \alpha - \alpha^2/2 = 1/2$
- So Arthur picks random $h \in \mathcal{H}$ and $s \in S$.
- Merlin replies with $y \in Good(x)$ s.t. $h(y) = s$
- Arthur verifies efficiently. ($p < N = exp(|\mathcal{F}|)$)

Bound for N_1

- When $\mathcal{F}$ is unsatisfiable over $\mathbb{C}$, effective HN gives $g_1, \ldots, g_m$ of exponential degree s.t. $f_1 g_1 + \ldots + f_m g_m = 1$
- Since coefficients of f_i's are in $\mathbb{Z}$, we can have g_j's in $\mathbb{Z}[x_1, \ldots, x_n]$ s.t. $f_1 g_1 + \ldots + f_m g_m = a$ for some non-zero a in $\mathbb{Z}$.
- $a = exp(exp(|\mathcal{F}|))$.
- If $\mathcal{F}$ is satisfiable modulo p, then p must divide a.
- There are at most $N_1 = \log a = exp(|\mathcal{F}|)$ such p.

Bound for N_2

- Since f_is are in $\mathbb{Z}[x_1, \ldots, x_n]$, any zero $(a_1, \ldots, a_n)$ is in $\bar{\mathbb{Q}}^n$.
- We want some simple compact representation of a_is in $\mathbb{Z}$.
- The idea is to represent a_is by univariate polynomials and simplify the given system to a large enough size univariate system.
- Make the correspondence of the zeros of the univariate system to the zeros of a univariate polynomial modulo different primes p.
- Count of such ps gives N_2.

Bound for N_2

- $a_1, \ldots, a_n \in \mathbb{Q}(a_1, \ldots, a_n)$.
- By primitive element theorem, $\mathbb{Q}(a_1, \ldots, a_n) = \mathbb{Q}(\beta)$ for some $\beta \in \bar{\mathbb{Q}}$.
- $a_i = P_i(\beta)/b$, where $P_i \in \mathbb{Z}[x]$.
- Let $R(x) \in \mathbb{Z}[x]$ be minimal polynomial for β.
- Using classical results in quantifier elimination and complexity of primitive elements we get that $\exists(a_1, \ldots, a_n)$ s.t. b and coefficients of R are $exp(exp(|\mathcal{F}|))$ and degree D of R is $exp(|\mathcal{F}|)$.

Bound for N_2

- Define the univariate system $g_i(x) := b^d f_i(P_1(x)/b, \dots, P_n(x)/b)$.
- $g_i(\beta) = 0$ implies $R|g_i$.
- We want count on all primes p in [N] s.t. p does not divide b and for some p' in $\mathbb{Z}/p\mathbb{Z}$, $R(p') = 0$ mod p.
- To get count of such primes p we use the effective version of Chebotarev Density Theorem, which assumes ERH.

- Define X as the set of primes p in [N] s.t. p does not divide discriminant of squarefree R.
- Define W as the set of all solutions of R modulo p, where p is in X.
- Assuming ERH, $|W| = |X| - Error$, where Error is $O(\sqrt{N} \log N^D disc(R))$.
- N_2 is at least $|W|/D - \log b$.
- By taking $N = exp(|\mathcal{F}|)$, simplification gives the required expression for N_2.

Questions ?

Thank You !!

Acknowlegement

- Besides the original paper by Koiran [Koi96] I would like to thank Dr. Madhu Sudan for his 1998 lecture notes [Sud98], which contains great exposition of original paper.

Pascal Koiran.
Hilbert's Nullstellensatz is in the Polynomial Hierarchy.
J. Complexity, 12(4):273–286, 1996.

Madhu Sudan.
Lecture notes on Algebra and Computation.
1998.