Koiran's Nullstellensatz in PH

The Hilbert Nullstellensatz problem is defined as follows: given polynomials $f_1, \dots, f_s \in \mathbb{C}[\bar{x}]$, decide whether $V(f_1, \dots, f_s) \neq \emptyset$ (i.e., the given system of polynomial equations has a solution). If we have $\bar{x} = (x_1, \dots, x_n)$ and $\deg f_i \leq d$ for $i \in [s]$, in the last lecture we saw that $V(f_1, \dots, f_s) = \emptyset \iff \exists\, g_1, \dots, g_s \in \mathbb{C}[\bar{x}]$ with $\deg g_i \leq \max\{3, d\}^n$ s.t.

$$1 = f_1 g_1 + \cdots + f_s g_s. \qquad (*)$$

Thus, the foregoing reduces the Nullstellensatz problem to the solution of an exponentially large linear system.

Now, to properly talk about the computational complexity of the above problem, we need to specify our computational model. In the Turing model, we cannot talk about polynomials with complex coefficients, so we will restrict our attention to polynomials with integral coefficients. Moreover, we will assume that we are given our polynomials in sparse representation, that is, as a list of pairs (coefficient, monomial) and we denote the logarithmic height of a polynomial

$$ht(F) := \max_{\bar{e} \in supp(F)} \log |coeff_{\bar{e}}(F)|.$$

We also assume the exponent vectors are given to us in binary.

Thus, we define the Hilbert Nullstellensatz (HN) problem as follows:

Input: $\mathcal{F} := \{f_1, \dots, f_s\} \subset \mathbb{Z}[x_1, \dots x_n]$ where $ht(f_i) \leq h$ and $\deg f_i \leq d$

Output: YES, if $V_{\mathbb{C}}(\mathcal{F}) \neq 0$ or NO otherwise.

In the last lecture, we saw that the exponential degree bounds given by the effective Nullstellensatz put the above problem in PSPACE.
Today, we will see Koiran's seminal result: assuming GRH, $HN \in RP^{NP} \subset \Pi_2^P$.

Given that HN is NP-hard, this really tightens the computational complexity upper and lower bounds for this problem.

The main idea of Koiran's seminal paper is the following: let

$$\mathcal{F} := \{f_1, \dots, f_s\}$$

be our system of polynomial equations with $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$, $\deg f_i \leq d$ and with bit complexity b.

Given a field $\mathbb{F}$, we denote by $V_{\mathbb{F}}(\mathcal{F})$ the zero-set of $\mathcal{F}$ over $\mathbb{F}$.

Now, the Nullstellensatz together with $\mathcal{F} \subset \mathbb{Z}[x_1, \dots, x_n]$ tell us that

$V_{\mathbb{C}}(\mathcal{F}) = \emptyset \iff \exists\, a \in \mathbb{Z} \setminus \{0\}$ and $g_1, \dots, g_s$ in $\mathbb{Z}[x_1, \dots, x_s]$ s.t.

$$a = f_1 g_1 + \cdots + f_s g_s. \qquad (1)$$

Moreover, with the degree bounds from the last lecture we can obtain explicit bounds on the bit complexity of a.

Hence, if $p \in \mathbb{N}$ is a prime s.t. $p \nmid a$ we have that equation (1) implies that $V_{\overline{\mathbb{F}}_p}(\mathcal{F}) = \emptyset$ and thus $V_{\mathbb{F}_p}(\mathcal{F}) = \emptyset$.

Similarly, we can also show that $V_{\mathbb{C}}(\mathcal{F}) \neq \emptyset$ $\Rightarrow$ there is $\Delta \in \mathbb{Z} \setminus \{0\}$ s.t. whenever $p \in \mathbb{N}$ is a prime s.t. $p \nmid \Delta$ then $V_{\overline{\mathbb{F}}_p}(\mathcal{F}) \neq \emptyset$.
This Δ is simply the determinant of a matrix arising from the linear system $(*)$.

Koiran's main question is: if $V_{\mathbb{C}}(\mathcal{F}) \neq \emptyset$, could it be the case that $V_{\mathbb{F}_p}(\mathcal{F}) \neq \emptyset$ for infinitely many primes? And if this is indeed the case, can we obtain good quantitative bounds for the above? That is, can we show that $V_{\mathbb{F}_p}(\mathcal{F}) \neq \emptyset$ for sufficiently many "small" primes p?

As it turns out, the answers to the above questions are YES, under the Generalized Riemann Hypothesis.

Given our system $\mathcal{F}$ above and $x \in \mathbb{N}$, let
$\pi_{\mathcal{F}}(x) := \{p \in \mathbb{N} \mid p \text{ prime}, V_{\mathbb{F}_p}(\mathcal{F}) \neq \emptyset\}$.
Also, let $\sigma = 2 + sd$.
More precisely, we will prove the following:

Theorem 1 (Theorem 1, Koiran '1996): there is a constant $c > 0$ s.t. if $A = d^{cn} \cdot s \cdot (h + \lceil \log s \rceil)$ and $x_0 \geq h^c \cdot 2^{(n \log \sigma)^c}$ the following holds:

① $V_{\mathbb{C}}(\mathcal{F}) = \emptyset \Rightarrow \pi_{\mathcal{F}}(x_0) \leq A$

② $V_{\mathbb{C}}(\mathcal{F}) \neq \emptyset \Rightarrow \pi_{\mathcal{F}}(x_0) \geq 8A(\log A + 3)$.

The above theorem, together with Stockmeyer's or Goldwasser-Sipser protocols puts $HN \in RP^{NP}$.

Algebraic Number Theory Facts

The following is in Koiran 1996, Theorem 4.

Theorem 2 (Complexity of primitive element): there is a universal constant $c \geq 1$ such that the following holds: let $\alpha_1, \ldots, \alpha_m$ be m algebraic numbers which are roots of polynomials $P_i \in \mathbb{Z}[z]$ with $\deg P_i \leq d$ and $ht(P_i) \leq h$. There is a primitive element γ for $\alpha_1, \ldots, \alpha_m$ which is a root of an irreducible polynomial $Q \in \mathbb{Z}[z]$ with $\deg Q \leq d^m$ and $ht(Q) \leq h \cdot d^{m^c}$. Moreover, there are non-zero $a \in \mathbb{Z}$ and $Q_i \in \mathbb{Z}[z]$ with $ht(a) \leq h \cdot d^{m^c}$, $\deg Q_i < \deg Q$, $ht(Q_i) \leq h \cdot d^{m^c}$ s.t. $\alpha_i = Q_i(\gamma)/a \quad \forall i \in [m]$.

The following is in Koiran 1996, Theorem 7. It tells us that if our system is satisfiable then there are solutions which are "small" algebraic numbers.

Theorem 3: there is an absolute constant $c \geq 1$ such that if $V_{\mathbb{C}}(\mathcal{F}) \neq \emptyset$ then there is a solution $\bar{\alpha} := (\alpha_1, \ldots, \alpha_n)$ s.t. each α_i is a root of a polynomial $P_i \in \mathbb{Z}[z]$ satisfying $\deg P_i \leq 2^{(n \log \sigma)^c}$ and $ht(P_i) \leq h \cdot 2^{(n \log \sigma)^c}$.

The following lemma gives us a sufficient condition to determine when an algebraic numerical solution of our system will yield a solution over $\mathbb{F}_p$. (Koiran 1996, Lemma 3)

Lemma 4: let $\bar{\alpha} := (\alpha_1, \ldots, \alpha_n) \in V_{\mathbb{C}}(\mathcal{F})$ where each α_i is an algebraic number. Let γ be a primitive element for $\alpha_1, \ldots, \alpha_n$. Then are $Q_1, \ldots, Q_n \in \mathbb{Z}[z]$ and $a \in \mathbb{Z}$ s.t. $\alpha_i = Q_i(\gamma)/a$. Let $R \in \mathbb{Z}[z]$ be an irreducible polynomial s.t. $R(\gamma) = 0$. If R has a root in $\mathbb{F}_p$ and $a \not\equiv 0 \bmod p$ then $V_{\mathbb{F}_p}(\mathcal{F}) \neq \emptyset$.

Proof: for $i \in [s]$, let

$$g_i(z) := a^{d_i} f_i\left(Q_1(z)/a, \ldots, Q_n(z)/a\right). \quad (2)$$

Note that $g_i(z) \in \mathbb{Z}[z]$. Since $g_i(\gamma) = 0$ and R irreducible we must have $R(z) \mid g_i(z)$. Thus, there are $A_1, \ldots, A_n \in \mathbb{Z}[z]$ s.t.

$$g_i(z) = R(z) \cdot A_i(z). \quad (3)$$

If $a \not\equiv 0 \bmod p$ then (2) and (3) also hold over $\mathbb{F}_p$. Thus, if $\beta \in \mathbb{F}_p$ is a root of R, we have $(Q_1(\beta)/a, \ldots, Q_n(\beta)/a) \in V_{\mathbb{F}_p}(\mathcal{F})$. $\square$

Now, the last ingredient we need is an estimate on how often an irreducible univariate polynomial in $\mathbb{Z}[z]$ will have a root over $\mathbb{F}_p$, as we vary p along the prime numbers. (This is where we will need the GRH).

Theorem (Effective Chebotarev Density Theorem): Let $R \in \mathbb{Z}[z]$ be an irreducible polynomial and let $D := \deg R$, $\Delta := |disc(R)|$. Assuming the GRH, there is an absolute constant $C > 0$ s.t.

$$\pi_R(x) \geq \frac{1}{D}\left(\pi(x) - C \cdot x^{1/2} \cdot \log(x^D \cdot \Delta) - \log \Delta\right)$$

where $\pi(x) := \#$ primes $\leq x$ and $\pi_R(x) := \#$ primes $p \leq x$ s.t. R has a root over $\mathbb{F}_p$.

Theorem (prime bound estimate): for $x \geq 17$, $\pi(x) \geq \frac{x}{\ln x}$.

Proof of main theorem

We are now ready to prove theorem 1.

Proof of theorem 1: if $V_{\mathbb{C}}(\mathcal{F}) = \emptyset$, then by the degree bounds on the Nullstellensatz from last lecture, there are $g_1, \dots, g_s$ in $\mathbb{C}[x_1, \dots, x_n]$ with $\deg(f_i g_i) \leq d^n$ s.t.

$$1 = \sum_{i=1}^{s} f_i g_i .$$

In particular, we know that the system $M_{\mathcal{F}, d^n} \cdot \vec{g} = 1$ has a solution $\therefore$ by Cramer's rule, there is a solution where $g_i = h_i / a$ where $h_i \in \mathbb{Z}[x_1, \dots, x_n]$ and $a \in \mathbb{Z} \setminus \{0\}$ is the determinant of a submatrix of $M_{\mathcal{F}, d^n}$.

Since the size of $M_{\mathcal{F}, d^n}$ is $\leq s \binom{d^n + n}{n} \leq s d^{2n^2}$ and the height of each entry of $M_{\mathcal{F}, d^n}$ is $\leq h$, we have

$$ht(a) \leq h \cdot s \cdot d^{2n^2} + n \log n . \qquad (4)$$

So long as p prime is such that $p \nmid a$ then $V_{\overline{\mathbb{F}}_p}(\mathcal{F}) = \emptyset \Rightarrow V_{\mathbb{F}_p}(\mathcal{F}) = \emptyset$.

Now, if $V_{\mathbb{C}}(\mathcal{F}) \neq \emptyset$, Theorem 3 implies that there is $\bar{\alpha} := (\alpha_1, \dots, \alpha_n) \in V_{\mathbb{C}}(\mathcal{F})$ where each α_i is a root of a $P_i \in \mathbb{Z}[z]$ with $ht(P_i) \leq h \cdot 2^{(n \cdot \log \sigma)^{c_1}}$, $\deg P_i \leq 2^{(n \log \sigma)^{c_1}}$, for some universal constant c_1.

By Theorem 2, there is a universal constant c_2 s.t. there is a primitive element γ for $\alpha_1, \dots, \alpha_n$ which is a root of an irreducible polynomial $R \in \mathbb{Z}[z]$ with $\deg R \leq 2^{(n \log \sigma)^{c_1+1}}$ and $ht(R) \leq h \cdot 2^{(n \log \sigma)^{c_1}} \cdot 2^{(n \log \sigma)^{c_1 + c_2}}$. Moreover there are $a \in \mathbb{Z} \setminus \{0\}$ and $Q_i \in \mathbb{Z}[z]$ with $ht(a) \leq h \cdot 2^{(n \log \sigma)^{c_1}} \cdot 2^{(n \log \sigma)^{c_1 + c_2}}$ s.t. $\alpha_i = Q_i(\gamma) / a \quad \forall i \in [m]$.

By the effective Chebotarev density theorem applied to R obtained above, we have

$$\pi_R(x) \geq \frac{1}{D} \cdot \left(\pi(x) - c' x^{1/2} \log(x^D \cdot \Delta) - \log \Delta \right)$$

where $D = \deg R$ and $\Delta := |\operatorname{disc} R|$.

Out of the $\pi_R(x)$ many good primes for R, at most $ht(a)$ of these primes divide a $\therefore$ by Lemma 4 we have that $V_{\mathbb{F}_p}(\mathcal{F}) \neq 0$ for at least $\pi_R(x) - ht(a)$ many primes $\leq x$.

Using $\pi(x) > \frac{x}{\ln x}$ and plugging in the above bounds we get that

$$\pi_{\mathcal{F}}(x) \geq \pi_R(x) - ht(a)$$

$$\geq \frac{1}{2^{(n \log \sigma)^{c_1+1}}} \left[\frac{x}{\ln x} - c' x^{1/2} \left(2^{(n \log \sigma)^{c_1+1}} \log x + ht(\Delta) \right) - ht(\Delta) \right]$$

$$- h \cdot 2^{(n \log \sigma)^{2c_1 + c_2}}$$

$$\geq$$