| **6.966 Algebra and Computation** | November 25, 1998 |
|---|---|
| Lecture 22 | |
| *Lecturer: Madhu Sudan* | *Scribe: Yevgeniy Dodis* |

In this lecture we will show that the Hilbert Nullstellensatz decision problem with integer coefficients (but complex witnesses!, denoted $\mathrm{HN}_{\mathbb{Z}}$) is in the polynomial time hierarchy (**PH**) under the Extended Riemann Hypothesis (ERH). This statement immediately implies that $0/1\text{–}\mathbf{NP}_{\mathbb{C}} \subseteq$ **PH** under the ERH, strengthening the unconditional guarantee that $0/1\text{–}\mathbf{NP}_{\mathbb{C}} \subseteq$ **PSPACE**. In fact, we will show even more, namely that $\mathrm{HN}_{\mathbb{Z}} \in \mathbf{AM} \subseteq \mathbf{PH}$ under the ERH, where **AM** is the class of languages having a constant round Arthur-Merlin game.

# 1 Problem Statement and Overview of the Proof

Here is the general instance of $\mathrm{HN}_{\mathbb{Z}}$:

INPUT: $\mathcal{F} = \{f_1, \ldots, f_m\}$, $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ of total degree at most $d$.

QUESTION: $\exists\, a_1, \ldots, a_n \in \mathbb{C}$ such that $f_i(a_1, \ldots, a_n) = 0$, for all $i \in [m]$?

So we are asking if our integer polynomials have at least one common zero over the *complexes*. We note that $\mathrm{HN}_{\mathbb{Z}}$ is indeed complete for $0/1\text{–}\mathbf{NP}_{\mathbb{C}}$. This follows from two facts that we indicated last lecture. Firstly, any language in $\mathbf{P}_{\mathbb{C}}$ can be decided by a polynomial-time $\mathbb{C}$-machine that uses only 0 and 1 as its constants. Using this and tracing carefully the reduction of any language $L \in \mathbf{NP}_{\mathbb{C}}$ to $\mathrm{HN}_{\mathbb{C}}$, we see that when $x \in \{0,1\}^*$, the resulting consistency checking polynomials indeed have all coefficients equal to 0 and 1, i.e. we indeed reduce $0/1\text{–}L$ to $0/1\text{–}\mathrm{HN}_{\mathbb{C}} \subseteq \mathrm{HN}_{\mathbb{Z}}$.

The input size is the number of bits to represent all the coefficients of $f_1, \ldots, f_m$, where each polynomial is given as a list of roughly $\binom{n+d}{d}$ coefficients, each of magnitude at most $C$. With a polynomial blowup in the input size, we could have assumed that $d = 2$ and all coefficients are 0 or 1. Thus, the issue of redundant/non-redundant representation of a given polynomial is not important. Let us denote by $|\mathcal{F}|$ the size of our input which can be assumed w.l.o.g. to be $|\mathcal{F}| = \mathrm{poly}(n, m, d, \log C)$.

**Main Idea:** Look at $f_i$'s modulo a prime $p$, where $p \in [N]$ and $N$ will be specified later. We hope that our system is unsatisfiable over $\mathbb{C}^n$ if and only if its version modulo $p$ is unsatisfiable over $\mathbb{Z}_p^n$ for "most" primes $p \in [N]$.

We note that proving that $\mathcal{F}$ has a solution over $\mathbb{Z}_p^n$ takes only $(n \log p)$ bits (unlike the proof over $\mathbb{C}^n$ that may take unbounded number of bits). We also note that the above equivalence will have "two-sided error" in that unsatisfiable $\mathcal{F}$ over $\mathbb{C}^n$ might become satisfiable over $\mathbb{Z}_p^n$, and satisfiable $\mathcal{F}$ over $\mathbb{C}^n$ might become unsatisfiable over $\mathbb{Z}_p^n$. However, $N$ will be chosen large enough so that there is a significant gap between the number of bad primes for a yes-instance and the number of bad primes for a no-instance. This will us allow to solve this "gap" problem (the gap is in the number of primes $p \in [N]$ for which $\mathcal{F}$ is satisfiable over $\mathbb{Z}_p^n$) in **AM**. More specifically, we show

**Theorem 1** *There exists a constant $N_1$ such that if $\mathcal{F}$ is unsatisfiable over $\mathbb{C}^n$, there are at most $N_1$ primes $p \in \mathbb{Z}$ such that $\mathcal{F}$ is satisfiable over $\mathbb{Z}_p^n$. Moreover, $N_1 = \exp(|\mathcal{F}|)$* [1].

[1] Notation $a = \exp(b)$ denotes the fact that $a = 2^{\mathrm{poly}(b)}$ for an appropriately chosen polynomial of $b$.

**Theorem 2** *Under the ERH, there are constants $N_2$ and $N_3$ such that if $\mathcal{F}$ is satisfiable over $\mathbb{C}^n$, there are at least $(\frac{\pi(N)}{N_2} - N_3 - O(\sqrt{N}\log N))$ primes $p \le N$ such that $\mathcal{F}$ is also satisfiable over $\mathbb{Z}_p^n$, where $\pi(N)$ is the number of primes less than or equal to $N$ (asymptotically, $\pi(N) \approx N/\log N \gg \sqrt{N}\log N$). Moreover, $N_2, N_3 = \exp(|\mathcal{F}|)$.*

Let $N$ be such that $\frac{\pi(N)}{N_2} - N_3 - O(\sqrt{N}\log N) \gg N_1$, so in particular $N = \exp(|\mathcal{F}|)$ suffices. Then, Theorems 1 and 2 imply that it is sufficient to solve in **AM** the following promise problem that we call Gap-HN. Let $N = \exp(|\mathcal{F}|)$ be as specified, $N_1 = P_1 \ll P_2 = \frac{\pi(N)}{N_2} - N_3 - O(\sqrt{N}\log N)$.

Input: $\mathcal{F} = \{f_1, \ldots, f_m\}$, $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ of total degree at most $d$.

Define $Primes(\mathcal{F}) = \{p \in [N] \mid p \text{ - prime}, \mathcal{F} \text{ is satisfiable over } \mathbb{Z}_p^n\}$.

No Instances: $|Primes(\mathcal{F})| \le P_1$.

Yes Instances: $|Primes(\mathcal{F})| \ge P_2$.

**Theorem 3** Gap-HN $\in$ **AM**

In the remaining sections, we prove Theorems 1, 2, 3. For Theorems 1 and 2 we will separate conceptual ideas with the messy details by leaving the (sketch of the) details in a separate section.

## 2 Overview of AM and Proof of Theorem 3

First, let us recall what the class **AM** is. It is a class of (promise, but we ignore it for now) languages $L$ for which there is a constant round Arthur-Merlin game. An Arthur-Merlin game is simply a public coin interactive protocol between an all-powerful prover Merlin and a probabilistic polynomial time verifier Arthur. Except for the verification stage, at each round Arthur only flips new truly random coins and gives them to Merlin. Merlin has to provide some reply (which can be thought as commitment) for each sequence of random coins (which are kind of challenges) from Arthur. At the verification stage, Arthur simply performs some polynomial time computation on his random coins and Merlin's responses. For an yes-instance $x$, honest Merlin can make Arthur accept with probability at least $\frac{2}{3}$. For a no-instance $x$, Arthur should reject with probability at least $\frac{2}{3}$ no matter how hard Merlin tries to cheat.

A crucial characteristic of an Arthur-Merlin game is the number of rounds. With polynomially many rounds, we can recognize any language in **IP** = **PSPACE**. With any constant number of rounds, it is possible to show that we can collapse them to only 1 round: a random challenge from Arthur, followed by a reply from Merlin. Using this and the standard boosting probability of error trick, we can place **AM** in the hierarchy: $\mathbf{AM} \subseteq \Pi_2^p \subseteq \mathbf{PH}$.

One of the most useful properties of **AM** is its ability to recognize the following languages. Assume that we have some universe $U$ and every input $x$ defines "good" set $Good(x) \subseteq U$. Assume further that for each $x$, the membership in $Good(x)$ is in **NP**, i.e. given $y \in U$, there is a polynomial-size witness proving that $y \in Good(x)$. Define a promise language $L$ where $x$ is a yes-instance if $|Good(x)| \ge P_2$, and a no-instance if $|Good(x)| \le P_1$, where $P_2 > 4P_1$.

**Lemma 4** $L \in$ **AM**

**Proof:** A first attempt that fails is for Arthur to pick a random element $y \in U$ and ask Merlin to prove that $y \in Good(x)$. However, $P_2$ is often exponentially smaller than $|U|$. So even a yes-instance $x$ will convince Arthur with a negligible probability $P_2/|U|$. A solution is to use a *universal family of hash functions.* Assume $|S| = P_2$ and $\mathcal{H}$ is a family of universal hash functions from $U$ to $S$.

Take any $T \subseteq U$ with $|T| = \alpha|S|$, $\alpha \leq 1$. Then universality of $\mathcal{H}$ easily implies that if we choose a random $h \in \mathcal{H}$ and a random point $s \in S$ we have

$$\alpha - \frac{\alpha^2}{2} \leq \Pr[s \in h(T)] \leq \alpha \tag{1}$$

Let us now apply this to $T = Good(x)$. For a no-instance $x$, $\alpha = \frac{|Good(x)|}{|S|} \leq \frac{P_1}{P_2} \leq \frac{1}{4}$ and we get $\Pr[s \in h(Good(x))] \leq \frac{1}{4}$. For a yes-instance $x$, we can make $\alpha = 1$ by considering any $P_2$ elements of $Good(x)$, and get $\Pr[s \in h(Good(x))] \geq 1 - \frac{1}{2} = \frac{1}{2}$. This suggests the following **AM** protocol. Arthur chooses a random $h \in \mathcal{H}$ and a random $s \in S$. Merlin has to reply with any preimage $y \in Good(x)$ such that $h(y) = s$ and a proof that indeed $y \in Good(x)$ (which is possible as the language is in **NP**). Above analysis shows that yes-instances are accepted with probability $\frac{1}{2}$ and no-instances are accepted with probability at most $\frac{1}{4}$, so $L \in$ **AM**. ∎

This Lemma proves Theorem 3. Take $U$ to be all the primes below $N$, $Good(\mathcal{F}) = Primes(\mathcal{F})$ and the membership in $Primes(\mathcal{F})$ can be proven in **NP** by giving a common zero $\in \mathbb{Z}_p^n$ of $f_1, \ldots, f_m$. Here we used the fact that $N = \exp(|\mathcal{F}|)$, so that for all $p < N$, $\log p = \text{poly}(|F|)$, i.e. the common zero in $\mathbb{Z}_p^n$ takes only polynomial number of bits to specify.

## 3 Proof of Theorem 1

Assume $\mathcal{F}$ is not satisfiable over $\mathbb{C}^n$. By Hilbert Nullstellensatz, $\exists q_1, \ldots, q_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that $\sum q_i f_i = 1$. How low can we place coefficients of $q_i$'s? Clearly we can place them in $\bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) since $\bar{\mathbb{Q}}$ is an algebraically closed field (so HN holds) and $f_i \in \mathbb{Z}[x_1, \ldots, x_n] \subseteq \bar{\mathbb{Q}}[x_1, \ldots, x_n]$. Can we place them in $\mathbb{Q}$? Yes. Effective HN gives us the bounds on degrees of $q_i \in \bar{\mathbb{Q}}[x_1, \ldots, x_n]$, so we can set up a linear system to obtain the coefficients of $q_i$'s. Since all the coefficients of the system will be in $\mathbb{Q}$ and we know that the solution in $\bar{\mathbb{Q}}$ exists, the solution in $\mathbb{Q}$ exists as well (since $\mathbb{Q}$ is a field).

Let $a$ be the least common denominator of coefficients of these $q_i$'s. We will demonstrate later that we can ensure the following bound on $a$.

**Claim 5** *There are valid $q_i$'s such that $a$ is at most doubly exponential in $|\mathcal{F}|$.*

Now, by multiplying all the $q_i$'s by $a$ we obtain:

**Lemma 6** *If $\mathcal{F}$ is not satisfiable over $\mathbb{C}^n$, then*

$$\exists r_1, \ldots, r_m \in \mathbb{Z}[x_1, \ldots, x_n],\ a \in \mathbb{Z},\ 0 \neq a = \exp(\exp(|\mathcal{F}|)) \text{ such that } \sum r_i f_i = a$$

Therefore, if $f_1, \ldots, f_m$ have a common zero over $\mathbb{Z}_p^n$, it must be the case that $p$ divides $a$. The number of such $p$'s is at most $N_1 := \log a = \exp(|\mathcal{F}|)$. ∎

### 3.1 Bound on $a$ (Proof of Claim 5)

Let us look closer at the linear system for the coefficients of $q_i$'s. Effective HN tells us that degrees of $q_i$ are at most $\exp(|F|)$, so the number of unknowns in the system is still at most $\exp(|\mathcal{F}|)$. Notice also that each coefficient of this system is a coefficient of some $f_i$ and thus takes $|\mathcal{F}|$ bits to represent. Hence, we have an exponential size system over $\mathbb{Q}$ where each coefficient is $|\mathcal{F}|$ bits long. Moreover, we know the system has some solution. Let us throw away all redundant equations and take some principal minor whose determinant is not zero. Set all the variables outside this principal minor to 0. The remaining variables are then set in a unique way. Moreover, all of them have a denominator divisible by the determinant of this principal minor. Let the size of the minor be $D = \exp(|\mathcal{F}|)$. Then its denominator is at most $\log(D! \cdot 2^{|\mathcal{F}|D}) = \exp(|\mathcal{F}|)$ bits long. So all the variables (including the ones that we set to 0) in this particular solution have a common denominator $a$ that is at most $\exp(|\mathcal{F}|)$ bits long, proving the claim. ■

# 4 Proof of Theorem 2

This is the most technical part where we will end up using ERH. Assume that $f_1, \ldots, f_m$ have a common zero $(a_1, \ldots, a_n) \in \mathbb{C}^n$. First of all, since all the coefficients of $f$ are in $\mathbb{Z} \subseteq \bar{\mathbb{Q}}$, we can assume that $a_i \in \bar{\mathbb{Q}}$, i.e. there is a common zero in $\bar{\mathbb{Q}}^n$. This follows from Hilbert Nullstellensatz. Indeed, a zero in $\mathbb{C}^n$ implies that the linear system $\sum q_i f_i = 1$ is unsatisfiable over $\mathbb{C}$. Since all the coefficients are also in $\mathbb{Z} \subseteq \bar{\mathbb{Q}}$, this system is unsatisfiable over $\bar{\mathbb{Q}}$ as well. And since $\bar{\mathbb{Q}}$ is algebraically closed, the converse of HN tells us that there is a common zero in $\bar{\mathbb{Q}}^n$. Let us develop some intuition by looking at some easy sub-cases.

Assume all $a_i \in \mathbb{Z}$. In this case $(a_i \bmod p)$ form a solution in $\mathbb{Z}_p^n$ for any prime $p$, so the number of such $p$'s is exactly $\pi(N)$ which is great. The next sub-case is when all $a_i \in \mathbb{Q}$, i.e. $a_i = \frac{a'_i}{b}$, where $a'_i, b \in \mathbb{Z}$. Define $g_i(y_1, \ldots, y_n) = b^d f_i(\frac{y_1}{b}, \ldots, \frac{y_n}{b})$, so that $g_i \in \mathbb{Z}[x_1, \ldots, x_n]$. Then $f_i(\frac{a'_1}{b}, \ldots, \frac{a'_n}{b}) = 0 \implies g_i(a'_1, \ldots, a'_n) = 0$. Hence, for any prime $p$, $(a'_i \bmod p)$ is a common zero of $g_1, \ldots, g_m$ over $\mathbb{Z}_p^n$. Then, provided $p$ does not divide $b$, $(a'_i b^{-1} \bmod p)$ form a common zero of $f_1, \ldots, f_m$ over $\mathbb{Z}_p^n$. This follows from $f_i(x_1, \ldots, x_n) = b^{-d} g_i(bx_1, \ldots, bx_n)$. Hence, the number of good primes is at least $\pi(N) - \log b$. We will not do it, but it is possible to show that $b = \exp(\exp(|\mathcal{F}|))$, so we would get $\pi(N) - \exp(|\mathcal{F}|)$ good primes.

With these ideas, let us move now to the general case when all $a_i \in \bar{\mathbb{Q}}$. First, we want a simple compact representation of $a_i$ in terms of $\mathbb{Z}$. Consider $\mathbb{Q}(a_1, \ldots, a_n)$, the field extension of $\mathbb{Q}$ obtained by adjoining $a_1, \ldots, a_n$ to it. By the famous primitive element theorem, we know that there exists $\beta \in \bar{\mathbb{Q}}$ such that in fact $\mathbb{Q}(a_1, \ldots, a_n) = \mathbb{Q}(\beta)$, i.e. a single algebraic extension suffices. Let $R(x) \in \mathbb{Q}[x]$ be the minimal polynomial for $\beta$ (i.e. $R(\beta) = 0$ and $R'(\beta) = 0 \implies \deg R' \geq \deg R$). By multiplying by the least common denominator, we can assume that $R \in \mathbb{Z}[x]$. Also, since $a_1, \ldots, a_n \in \mathbb{Q}(\beta)$, there are polynomials $p_1, \ldots, p_n \in \mathbb{Z}[x]$ and a least common denominator $b$ such that $a_i = p_i(\beta)/b$. This is the concise representation that we wanted. We will sketch later the proof of the following claim that we assume for now:

**Claim 7** *By an appropriate choice of the common zero $(a_1, \ldots, a_n)$, $b$ and the coefficients of $R$ are at most doubly exponential in $|\mathcal{F}|$, while the degree $D$ of $R$ is at most singly exponential in $|\mathcal{F}|$.*

Define $g_i(x) = b^d f_i(\frac{p_1(x)}{b}, \ldots, \frac{p_n(x)}{b})$, so that for $i \in [m]$

1. $g_i(x) \in \mathbb{Z}[x]$.

2. $g_i(\beta) = b^d f_i(\frac{p_1(\beta)}{b}, \ldots, \frac{p_n(\beta)}{b}) = b^d f_i(a_1, \ldots, a_n) = 0$.

3. $R(x)$ divides $g_i(x)$ (since $R$ is a minimal polynomial of $\beta$ and $g_i(\beta) = 0$).

Suppose now that a prime $p$ does not divide $b$ and that $R(x)$ has a root $\gamma$ in $\mathbb{Z}_p$, i.e. $R(\gamma) \bmod p = 0$. Then $g_i(\gamma) \bmod p = 0$ as well since $R$ divides $g_i$. Then, $\mathcal{F}$ is satisfiable over $\mathbb{Z}_p^n$ by $(p_1(\gamma)b^{-1} \bmod p, \ldots, p_n(\gamma)b^{-1} \bmod p)$ since $f_i(\frac{p_1(\gamma)}{b}, \ldots, \frac{p_n(\gamma)}{b}) = b^{-d} g_i(\gamma) = 0 \bmod p$. Define

$$S_{N,R} = \{p \in [N] \mid p \text{ - prime}, p \text{ does not divide } b, \exists \gamma \in \mathbb{Z}_p \text{ s.t. } R(\gamma) = 0 \bmod p\}$$

From the above discussion, the number of primes satisfying Theorem 2 is at least $|S_{N,R}|$. Since $b$ is doubly exponential, there are at most $\log b = \exp(|\mathcal{F}|)$ primes dividing $b$. We would be done except we need $R$ to have a root in $\mathbb{Z}_p$. For that, we will need to use ERH by using (as a black-box) the following powerful theorem telling us that we will have roots for a lot of $p$'s.

**Theorem 8 (Effective Chebotarev Density Theorem)** *Suppose $R \in \mathbb{Z}[x]$ is irreducible (square free suffices as well) of degree $D$. Let $\Delta = \mathrm{disc}(R)$ be the discriminant of $R$ (recall, the resultant of $R$ and the derivative of $R$, which is not zero since $R$ is square free). Define*

$$\Pi'_{N,R} = \{p \in [N] \mid p \textit{ - prime}, p \textit{ does not divide } \Delta\}$$

$$W_{N,R} = \{(\gamma, p) \mid p \in \Pi'_{N,R}, R(\gamma) = 0 \bmod p\}$$

*Then, assuming ERH,*

$$|W_{N,R}| = |\Pi'_{N,R}| - O(\sqrt{N}\log(N\Delta)) \tag{2}$$

We are almost done. First, using the fact that $D = \exp(|\mathcal{F}|)$ and the coefficients of $R$ are $2^{\exp(|\mathcal{F}|)}$, we bound the logarithm of the discriminant of $R$: $\log\Delta \leq \log((2D)! \cdot 2^{\exp(|\mathcal{F}|)2D}) = \exp(|F|)$. Also, $|\Pi'_{N,R}| \geq \pi(N) - \log\Delta$ since at most $\log\Delta$ primes divide $\Delta$. Using this, Chebotarev's Density Theorem and the fact that $R$ can have at most $D$ roots in $\mathbb{Z}_p$ (so that each $p$ is counted at most $D$ times in $|W_{N,R}|$), we get:

$$\begin{aligned}
|S_{N,R}| &\geq \frac{|W_{N,R}|}{D} - \log b \overset{(2)}{\geq} \frac{|\Pi'_{N,R}| - O(\sqrt{N}\log(N\Delta))}{D} - \log b \\
&\geq \frac{\pi(N) - \log\Delta - O(\sqrt{N}\log(N\Delta))}{D} - \log b = \frac{\pi(N)}{N_2} - N_3 - O(\sqrt{N}\log N)
\end{aligned}$$

Here $N_2 := D = \exp(|\mathcal{F}|)$, $N_3 := \frac{\log\Delta}{D} + \log b = \exp(|\mathcal{F}|)$, $\log(N\Delta) = O(\log N)$ provided $N = \exp(|\mathcal{F}|)$. This completes the proof. ■

## 4.1 Bounds on $b$, $D$ and the coefficients of $R$ (Proof of Claim 7)

This is the most annoying part that we sketch since it does not shed too much light on what is going on. Here for the first time we have to be slightly careful when dealing with the input size $|\mathcal{F}| = \mathrm{poly}(n, m, d, \log C)$. Let $R = \max(n, m, d)$, so that $|\mathcal{F}| = \mathrm{poly}(R, \log C)$ i.e. we separate out the sizes of the coefficients of $f_i$'s. Let us start with bounds on minimal polynomials over $\mathbb{Q}$ defining $a_i \in \bar{\mathbb{Q}}$, where $(a_1, \ldots, a_n)$ is our common zero. Recall that $\mathrm{HN}_{\mathbb{Z}}$ is the following problem: determine if $\exists x_1, \ldots, x_n$ such that $f_1(x_1, \ldots, x_n) = 0, \ldots, f_1(x_1, \ldots, x_n) = 0$. Let us use quantifier elimination and eliminate some $x_k$. Then the predicate that such $x_1, \ldots, x_n$ exist becomes a formula of $x_k$ that can be written in the form:

$$\Gamma^k(x_k) := \bigvee_i \bigwedge_j (\Phi^k_{ij}(x_k) = 0 \wedge \Psi^k_{ij}(x_k) \neq 0)$$

where (we mentioned these bounds when we studied quantifier elimination).

- $\Phi^k_{ij}$ and $\Psi^k_{ij}$ are polynomials over $\mathbb{Z}$.
- Their degree is at most $\exp(R)$.
- Their coefficients are at most $\exp(R)\log C$ bits long.

- The range of $i$ and $j$ is at most $\exp(R)$.

Since we know that $\Gamma^k(a_k)$ is true, there is a particular $i_0$ such that $\bigwedge_j(\Phi^k_{i_0j}(a_k) = 0 \wedge \Psi^k_{i_0j}(a_k) \neq 0)$ is true. We split the analysis into 2 cases.

Assume that for some $1 \leq k \leq n$ all $\Phi^k_{i_0j}(x) \equiv 0$, say $k = n$ w.l.o.g. Then $\Gamma^n(x_n)$ has a clause of the form $\bigwedge_j(\Psi^n_{i_0j}(x_n) \neq 0)$. Since each $\Psi^n_{i_0j}$ has a singly exponential degree (everything is in $R$ for now), it has only that many zeros, and as there are exponentially many indices $j$, we get that only exponentially many $x_n$ make this clause false. Hence, the whole $\Gamma^n(x_n)$ is false only for at most *exponentially* many $x_n$. Thus, in this case we can redefine $a_n$ (if necessary) so that it even becomes a singly exponential *integer*, $a_n \leq \exp(R)$. This $a_n$ is trivially a root of a degree 1 integer polynomial $x - a_n = 0$. Of course, this implicitly redefines $a_1, \ldots, a_{n-1}$, but we know that our new $a_n$ still leaves $\mathcal{F}|_{x_n=a_n}$ satisfiable. Now we can completely eliminate $x_n$ by setting it equal to (integer) $a_n$ everywhere in $\mathcal{F}$. We get a new (satisfiable) system with only $n-1$ variables, same maximum degree $d$ and number of equation $m$ (so that we can use the same $R$ for this system). The only thing that grows is the magnitude of the largest coefficient that can be up to $(\exp(R) \cdot C)$. In this case we apply our analysis from scratch to an $(n-1)$-variable system $\mathcal{F}|_{x_n=a_n}$ with $R' = R$, $C' = \exp(R) \cdot C$.

The complementary case to the above is when for *all* $1 \leq k \leq n$ there exists some $j_0(k)$ such that $t_k(x) := \Phi^k_{i_0j_0(k)}(x) \not\equiv 0$. Then $t_k(a_k) = 0$, so some factor of $t_k(x)$ is a minimal polynomial for $a_k$. From the bounds above on quantifier elimination, we get that the degree of this minimal polynomial is at most $\exp(R)$ and its coefficients are at most $(\exp(R)\log C)$ bits long. In general, to obtain all $n$ minimal polynomials we will be in the first case for $0 \leq s \leq n$ times, and then be once in the second case. Since $R$ never grows, all the polynomials have degree at most $\exp(R) = \exp(|\mathcal{F}|)$. And the largest coefficient will be at most $\exp(R)\log(\exp(R)^s \cdot C) = \exp(R)\log C = \exp(|\mathcal{F}|)$ bits long. To summarize,

**Lemma 9** *If $\mathcal{F}$ is satisfiable, there exists a common zero $(a_1, \ldots, a_n) \in \bar{\mathbb{Q}}^n$ such that for any $k$, the minimal polynomial $q_k(x) \in \mathbb{Z}[x]$ for $a_k$ has at most singly exponential degree $d_i$ and at most doubly exponential coefficients (in $|\mathcal{F}|$).*

It is a classical theorem that if $a_1$ and $a_2$ have minimal polynomials of degree $d_1$ and $d_2$ and coefficients bounded by $C$, then the primitive element $\tau$ of the joint extension $\mathbb{Q}(a_1, a_2) = \mathbb{Q}(\tau)$ has minimal polynomial of degree at most $d_1d_2$ and coefficients at most $C^{d_1d_2}$. Moreover, $a_i$ can be written as $r_i(\tau)/m$, where $m < C^{d_1d_2}$ and $r_i$ is an integer polynomial, $i = 1, 2$. By adjoining $a_1$,...,$a_n$ one at a time and using the above lemma about the minimal polynomials of $a_i$'s, our claim on the degree $D$ of $R$, size of its coefficients and the size of $b$ follows. ■

# 5 Concluding Remarks

The proof presented here is due to Koiran. He also gives an example demonstrating that when $\mathcal{F}$ is satisfiable over $\mathbb{C}^n$, there could be indeed exponentially many primes for which $\mathcal{F}$ is unsatisfiable over $\mathbb{Z}_p^n$. Thus, Theorem 2 can not be improved too much. However, no example demonstrating the tightness of Theorem 1 is known. We note that the use of ERH was hidden by using the powerful Chebotarev's Density Theorem. While conceivably possible, no one knows how to prove an unconditional bound on $|S_{N,R}|$.