D4: Decidability

Montag, 23. Juni 2025 16:44

Skolem problem (open): Is it decidable whether a $\mathbb{Q}$-LRS $(a_n)_{n\geq 0}$ has a zero?

Remark: 1) Infinite zero sets can be computed, so w.l.o.g. $(a_n)_{n\geq 0}$ has finitely many zeros.

2) If $(a_n)_{n\geq 0}$ is an LRS of order $d \leq 4$: Yes

($d=1,2$ easy, $d=3,4$ Mignotte–Shorey–Tijdemann '84, Vereshchagin '85)

(S) Skolem Conjecture: If $(a_n)_{n\in\mathbb{Z}}$ is a simple (char. polys separable) $\mathbb{Z}[\frac{1}{M}]$-LRBS, without zero in $\mathbb{Z}$, there exists $m \geq 1$ with $\gcd(M,m)=1$, s.t. $(a_n + m\mathbb{Z})_{n\geq 0}$ does not have a zero.

If (S) holds, the „Skolem problem for simple LRBS" is decidable: search simultaneously for a zero and a witness m. Does not give a procedure to find all zeros of a bisequence! Does not immediately resolve the problem for LRS.

Thm 4.1 (Bilu–Luca–Nieuwveld–Ouaknine–Purser–Worrell '22)
There is an algorithm taking a simple $\mathbb{Q}$-LRS $(a_n)_{n\geq 0}$ as input, that outputs all zeros of $(a_n)_{n\geq 0}$ if it terminates.
Under Conjectures (S) and (P) (below), the algorithm terminates.

Sketch. Wlog. $(a_n)_{n\geq 0}$ is simple and has finitely many zeros (in $\mathbb{Z}$)
Check if $(a_n)_{n\in\mathbb{Z}}$ has a zero (Terminates by (S))
If it has, wlog, $a_0 = 0$ (shift)
Find M s.t. $a_{Mn} \neq 0$ for $n \neq 0$. [Prop 4.1, terminates under (P)]
Recursion on $\{ a_{Mn+r} : 1 \leq r \leq M-1 \}$.

Recursion on $\{a_{Mn+r} : 1 \leq r \leq M-1\}$.
(Terminates, because each step removes at least one zero). $\square$

Schanuel's Conjecture: If $z_1, \dots, z_n \in \mathbb{C}$ are $\mathbb{Q}$-linearly independent, then $\operatorname{trdeg} \mathbb{Q}(z_1, \dots, z_n, \exp(z_1), \dots, \exp(z_n)) \geq n$.

E.g. $\operatorname{trdeg} \mathbb{Q}(i\pi, \exp(i\pi) = -1) \geq 1 \to \pi$ transcendental (known)

$\operatorname{trdeg} \mathbb{Q}(1, i\pi, e, \exp(i\pi) = -1) \geq 2 \to \pi, e$ alg. independent (open)

Conjecture (P) (Weak p-adic Schanuel Conjecture)

for convergence of $\log(x)$ series

If $\alpha_1, \dots, \alpha_d \in \mathbb{Q}_p$ with $|1 - \alpha_i|_p < \frac{1}{p}$ are s.t. $\log(\alpha_1), \dots, \log(\alpha_d)$ are $\mathbb{Q}$-linearly independent, then $\log(\alpha_1), \dots, \log(\alpha_d)$ are $\mathbb{Q}$-algebraically independent ($\Rightarrow$ alg. indep over every finite field ext. of $\mathbb{Q}$)

Prop 4.2: Suppose (P) holds. If $(a_n)_{n \in \mathbb{Z}}$ is a strict simple LRBS with $a_0 = 0$, then one can compute $M \geq 1$ s.t. $a_{Mn} \neq 0$ for all $n \neq 0$.

Idea: $a_n = f(n)$ p-adic analytic interpolation, find a p-adic nbhd U of 0 s.t. $f(U \setminus \{0\}) \not\ni \{0\}$ ($\Rightarrow U \supseteq p^v \mathbb{Z}$ for some v; take $M = p^v$)

Lemma 4.3 If $f = \sum_{n=0}^{\infty} \alpha_n x^n \in \mathbb{Z}_p[[x]]$ converges in $\mathbb{Z}_p$, $0 = \alpha_0 = \dots = \alpha_{e-1}$, $\alpha_e \neq 0$, then $f(\beta) \neq 0$ $\forall \beta \in \mathbb{Z}_p$ with $0 < |\beta|_p < |\alpha_e|_p$

Proof Sketch: $|\alpha_e \beta^e|_p > \max\{|\alpha_n \beta^n|_p : n > e\} \geq \left|\sum_{n=e+1}^{\infty} \alpha_n \beta^n\right|_p$. $\square$

Lemma 4.4: Let $\lambda_1, \dots, \lambda_d \in \mathbb{Q}_p$ be algebraic over $\mathbb{Q}$. Then the group

$$\{(e_1, \dots, e_d) \in \mathbb{Z}^d : \lambda_1^{e_1} \cdots \lambda_d^{e_d} = 1\}$$ is computable.

(w/o proof; explicit upper bound on size of generators). Special case $\lambda_1, \dots, \lambda_d \in \mathbb{Q}$ easy (prime factorization)

Proof of Prop 4.2: Choose p s.t. $a_n \in \mathbb{Z}_p$ $\forall n \in \mathbb{Z}$ and the minimal polynomial of $(a_n)_{n \geq 0}$ splits into distinct factors over $\mathbb{F}_p$ (Chebotarev's density theorem), and then $\mathbb{Z}_p$ (Hensel's Lemma). Let $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$ be the pairwise distinct and then $\mathbb{Z}_p$ (Hensel's Lemma). Let $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$ be the pairwise distinct eigenvalues. Then

$$a_n = u^T \underbrace{\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_d \end{pmatrix}}_{=: A}{}^{n} v = \sum_{i=1}^{d} \gamma_i \lambda_i^n \quad , \quad \gamma_i \in \mathbb{Q}_p, \ \lambda_i \in \mathbb{Z}_p$$

(algebraic / $\mathbb{Q}$)

Wlog. $2p \nmid \det(A)$. $\longrightarrow$ $A^N \equiv I \mod p\mathbb{Z}_p$ $\quad (\mathbb{Z}_p/_{p\mathbb{Z}_p} \cong \mathbb{F}_p)$ for some $N \geq 1$.

$\Rightarrow \forall i: \ \lambda_i^N \equiv 1 \mod p\mathbb{Z}_p \Rightarrow \log(\lambda_i^N)$ p-adically defined by power series

$$\Rightarrow \forall n \in \mathbb{Z}: \quad a_{Nn} = \sum_{i=1}^{d} \gamma_i \exp(n \log(\lambda_i^N))$$

$$f := \sum_{i=1}^{d} \gamma_i \exp(x \log(\lambda_i^N)) = \sum_{j=0}^{\infty} \beta_j x^j \in \mathbb{Q}_p[\![x]\!]$$

converges on $\mathbb{Z}_p$, $a_{Nn} = f(n) \quad \forall n \in \mathbb{Z}$.

$$\beta_j = \frac{1}{j!} \sum_{i=1}^{d} \gamma_i \cancel{\exp(0 \cdot \log(\lambda_i^N))} \cdot \log(\lambda_i^N)^j \qquad \text{(Taylor series)}$$

If $\beta_j \neq 0$, can compute $|\beta_j|_p$ numerically. Smallest j for which $\beta_j \neq 0$?

Let $\{\lambda_1, \ldots, \lambda_s\}$ be a max. multiplicatively indep subset of $\{\lambda_1, \ldots, \lambda_d\}$. (reindex),

$$\forall j > s: \quad \lambda_j^{e_{j0}} = \lambda_1^{e_{j1}} \cdots \lambda_s^{e_{js}} \qquad (e_{jk} \in \mathbb{Z}, e_{j0} \neq 0)$$

$$\Rightarrow \log(\lambda_j^N) = \sum_{k=1}^{s} \frac{e_{jk}}{e_{j0}} \log(\lambda_k^N).$$

$$\Rightarrow \beta_j = P_j(\log(\lambda_1^N), \ldots, \log(\lambda_s^N)) \quad \text{with} \quad P_j \in \overbrace{\mathbb{Q}(\gamma_1, \ldots, \gamma_d)}^{\text{finite}}[x_1, \ldots, x_s]$$

$\uparrow$ explicit.

$$\overset{(P)}{\Longrightarrow} [\beta_j = 0 \Leftrightarrow P_j = 0]$$

So find the smallest P_j with $P_j \neq 0 \Rightarrow \beta_j \neq 0$ - compute $|\beta_j|_p$ numerically

So find the smallest P_j with $P_j \neq 0 \Rightarrow \beta_j \neq 0$; compute $|\beta_j|_p$ numerically

Conclude using L4.3. $\square$