The Skolem-Mahler-Lech Theorem

Adam B Block

11 August 2017

1 Introduction

The theorem of Skolem, Mahler, and Lech gives a condition on the set $S_a = \{n \in \mathbb{N} | a_n = 0\}$, where we have some rational function, where for a field K of characteristic 0, with $f, g \in K[x]$,

$$\frac{f(x)}{g(x)} = \sum_{i=0}^{\infty} a_i x^i$$

Note that we can always find such $\{a_i\}$ because of Taylor's theorem. As [Lec53] noted, Skolem proved the result for $K = \mathbb{Q}$ and Mahler proved the result for algebraic extensions of $\mathbb{Q}$, before Lech himself proved the theorem for all fields of characteristic 0. More recently, there do exist generalizations to fields of positive characteristic, with [Der05] fully generalizing the theorem. We will prove the result for $K = \mathbb{Q}$ using a simpler proof than Lech's, due to Hansel (see [Han86]).

2 Linear Recurrence, Rational Functions, and Prerequisites

We will work over the field $K = \mathbb{Q}$. First, we need a definition.

Definition 1. A linear recurrence of dimension k is a sequence $(a_n)_{n\in\mathbb{N}}$ such that $a_0, ..., a_{k-1} \in \mathbb{Q}$ and there exist $c_1, ..., c_k$ such that for all $n \geq k$,

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + a_k c_{n-k} = \sum_{i=1}^{k} c_i a_{n-i}$$

For the sake of avoiding redundancy, we assume $c_k \neq 0$. Given a linear recurrence (a_n), we define the zero set,

$$S_a = \{n \in \mathbb{N} | a_n = 0\}$$

A natural question to ask is what sets $S_a \subset \mathbb{N}$ can occur? Let us try some examples.

Example 2. Let $a_0 = 0$, $a_1 = 1$ and let $a_n = a_{n-1} + a_{n-2}$. This is, of course, the Fibbonacci sequence. It is easy to see that $a_n \geq a_{n-1}$ for all n, so in this case $S_a = \{0\}$.

Example 3. Let $a_0 = 1$, $a_1 = -5$, $a_2 = 13$ and $a_n = 5a_{n-1} - 16a_{n-2} + 12a_{n-3}$. Our trick in the above sequence clearly does not work. However, we do find, after a little thought, that after reduction $\pmod 4$ we get $a_n \equiv a_{n-1}$ and so we get $S_a = \emptyset$.

Example 4. Now consider $a_0 = a_1 = 1$, $a_n = a_{n-1} - a_{n-2}$. It is immediate that

$$S_a = \{n \in \mathbb{N} | n \equiv 2 \pmod 3\}$$

.

At first glance, these seem very different, but we will show that these three examples demonstrate all of the possibilities. Our main theorem:

Theorem 5 (Skolem-Mahler-Lech)**.** *Let $(a_n)_{n\in\mathbb{N}}$ be a linear recurrence. Then there exists some $r \in \mathbb{N}$ and $j_1, ..., j_m \in \mathbb{N}$ with m possibly equal to 0 distinct elements and some finite subset $Z \subset \mathbb{N}$ such that*

$$S_a = Z \cup \bigcup_{i=1}^{m} \{j_i + rq | q \in \mathbb{N}\}$$

In other words, the zero set of the sequence is a union of a finite set and a finite number of arithmetic progressions all with the same common difference.

The astute reader may note that this is not the same as the traditional theorem of Skolem, Mahler, and Lech. To translate between our statement and theirs, we need the following proposition.

Proposition 6 (Schützenberger)**.** *If $P \in K[\![x]\!]$ such that*

$$P = \sum_{i=0}^{\infty} a_i x^i$$

Then P is rational if and only if there exists some $N, k \in \mathbb{N}$ such that for all $n > N$, the (a_i) form a linear recurrence of dimension k.

Proof. Note that P is rational if and only if there exist $f, g \in K[x]$ such that $P = \frac{f}{g}$. Let $g = g_m x^m + ... + g_0$. There always exists a power series expansion of a rational function by applying Taylor's theorem. Thus we have P rational if and only if there is some polynomial g such that $gP = f$ a polynomial. Thus if $\deg f = n_0$, and $gP = \sum_{n=0}^{\infty} b_n x^n$ then for $n > n_0$, $b_n = 0$. Note however that $0 = b_n = g_0 a_n + g_{n-1} a_{n-1} + ... + g_0 a_{n-k}$. This is clearly true if and only if the a_i form a linear recurrence. ■

Remark 7. Note that using Proposition 6, the equivalence between our Theorem 5 and the original is immediate.

We have one more way of characterizing linear recurrences. Given a linear recurrence (a_n) of dimension k, we can form a $k \times k$ matrix M such that $M_{i,1} = c_i$ for all i, $M_{i,i-1} = 1$ for $2 \le i \le k$ and everything else is 0. Let

$$\mathbf{u} = \begin{bmatrix} a_{k-1} & a_{k-2} & \dots & a_0 \end{bmatrix}$$
$$\mathbf{v} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \end{bmatrix}$$

Then we get for $n \ge k$, $a_n = \mathbf{u} M^{n+1-k} \mathbf{v}$. This is clear by induction.

We now review some basic facts about the p-adic valuation. Fix some prime p. For any $\frac{a}{b} \in \mathbb{Q}$ with a, b coprime, we get a unique integer k such that $p^k = \frac{a'}{b'}$ and $p \nmid a'b'$. Let $v_p(\frac{a}{b}) = k$. Call this the p-adic valuation. There are a few properties that fall immediately out of this definition.

1. For all $\alpha, \alpha' \in \mathbb{Q}$, $v_p(\alpha\alpha') = v_p(\alpha) + v_p(\alpha')$
2. For all $\alpha, \alpha' \in \mathbb{Q}$, $v_p(\alpha + \alpha') \ge v_p(\alpha) + v_p(\alpha')$
3. For all $n \in \mathbb{N}$, $v_p(n!) \le \frac{n}{p-1}$

Of these, only the last requires some explanation. It is easy to see that $v_p(n!) = \sum_{i=1}^{\infty} [\frac{n}{p^i}]$, where $[\alpha]$ denotes the greatest integer function. Thus we get that $v_p(n!) \le \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}$. Given a polynomial $f(x) = \alpha_n x^n + ... + \alpha_0 \in \mathbb{Q}[x]$, we define

$$v_p^i(x) := \min_{j \ge i}(v_p(\alpha_j))$$

It is clear by the properties above that $v_p^0(f) \le v_p(m)$ for all $m \in \mathbb{N}$. We are now ready to start proving Theorem 5.

3 Proof of Theorem 5

The general idea involves constructing a special sequence associated to our sequence and then to consider reduction $\pmod p$ for some fixed prime p. Before we do this, we need a few lemmata and propositions.

Lemma 8. *Let $m \in \mathbb{N}$ and $f(x) \in \mathbb{Q}[x]$. Let $g(x) = (x-m)f(x)$. Then $v_p^i(f) \geq v_p^{i+1}(g)$.*

Proof. Let $f = a_n x^n + ... + a_0$. Let $g = b_{n+1}x^{n+1} + b_n x^n + ... + b_0$. Note that $b_0 = -ma_0$. For $i > 0$, we get that $b_i = a_{i-1} - ma_i$. Rearranging, we get $a_j = b_{j+1} + ma_{j+1}$. We can now iterate this process, replacing $a_{j+1} = b_{j+2} + ma_{j+2}$. Continuing this, we get

$$a_j = b_{j+1} + mb_{j+2} + m^2 b_{j+3} + ... + m^{n-j} b_{n+1}$$

Apply the properties of v_p mentioned above and we win. ■

Now that we have the lemma, we are able to prove a result reminiscent of our desired one.

Proposition 9. *Let (d_n) be a sequence in $\mathbb{Z}$ and let*

$$b_n = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$$

Then if there exists some $b_n \neq 0$, then S_b is finite.

Proof. Suppose S_b is infinite. We will show that then S_b is all of $\mathbb{N}$. Let $R_n(x) = \sum_{i=0}^{n} \binom{x}{i} d_i p^i$. It is clear that if $m \leq n$, then $R_n(m) = R_m(m) = b_m$. Let $R_n(x) = \alpha_n x^n + ... + \alpha_0$. Then each α_i is a $\mathbb{Z}$-linear combination of $d_j \frac{p^j}{j!}$. But using the properties of v_p mentioned above, we immediatley get the chain of inequalities

$$v_p(\frac{d_j p^j}{j!}) \geq j - v_p(j!) \geq j - \frac{j}{p-1} = j\frac{p-2}{p-1}$$

If $j \geq i$, then it follows that $v_p^j(R_n) \geq i\frac{p-2}{p-1}$.

We now fix $r, s \in \mathbb{N}$. Let $i \in \mathbb{N}$ such that $i\frac{p-2}{p-1} > s$. Because S_b is infinite, for all i, there exist $m_1, ..., m_i \in S_b$ the first i elements. Let $N > \max(r, m_i)$. Then we get that $R_N(m_j) = b_{m_j} = 0$ for all $1 \leq j \leq i$ so we can factor $R_N = (x-m_1)...(x-m_i)f$ for some $f \in \mathbb{Q}[x]$. Then we get that

$$v_p(b_r) = v_p(R_N(r)) \geq v_p(f(r)) \geq v_p^0(f)$$

. By Lemma 8,

$$v_p^0(f) \geq v_p^i(R_N) \geq i\frac{p-2}{p-1} \geq s$$

Thus, we have shown that $v_p(b_r) \geq s$ for all $r, s \in \mathbb{N}$. Embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ immediately yields that $b_r = 0$. Because r was arbitrary, thiss holds for all r and we get that $b_r = 0$ for all $r \in \mathbb{N}$ and we are done. ■

We need one more proposition and we will get Theorem 5 as a corollary.

Proposition 10. *Let (a_n) be a linear recurrence of dimension k with integral coefficients such that $a = \mathbf{u}M^{n-k}\mathbf{v}$. If p is a prime such that $p \nmid \det M$, then there exist $N, r, j_1, ..., j_m \in \mathbb{N}$ with m possibly 0 and $r||GL_k(\mathbb{F}_p)|$, such that*

$$S_a \cap \{n \in \mathbb{N} | n > N\} = \bigcup_{i=1}^{m} \{j_i + rq | q \in \mathbb{N}\}$$

Proof. We let a bar denote passage from $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ by the canonical projection. Recall that $\det M$ is a polynomial in the elements of M and quotienting is a morphism so $\det \overline{M} = \overline{\det M} \neq 0 \in \mathbb{F}_p$ because

$p \nmid \det M$. Let G be the general linear group of $\mathbb{F}_p^k$. By Lagrange's theorem, there exists an $\mathbb{N} \ni r||GL_k(\mathbb{F}_p)|$ such that $\overline{M}^r = I$. Pulling back to working over $\mathbb{Z}$, we get that there exists a matrix M' such that

$$M^r = I + pM'$$

Fix $j \in \{0, 1, ..., r-1\}$ and let $d_n = \mathbf{u}M^j M'^n \mathbf{v}$. We get that

$$a_{rn+j} = \mathbf{u}M^{rn+j}\mathbf{v} = \mathbf{u}M^j(I + pM')^n\mathbf{v} = \sum_{i=0}^{n} p^i d_i \binom{n}{i}$$

By Proposition 9, $\{n \in \mathbb{N} | a_{rn+j} = 0\}$ is either finite or all of $\mathbb{N}$ Thus for $n > \max(r-1, k)$, $a_n = 0$ if and only if $a_{n+r} = 0$ as desired. ■

We can now prove Theorem 5 as a trivial consequence of the above theorem.

Proof of Theorem 5 assuming integral coefficients. Let (a_n) be a linear recurrence. If we can find a prime p such that $p \nmid \det M$ then we can apply Proposition 10, and $S_a \cap \{n \in \mathbb{N} | n > N\} = \bigcup_{i=1}^{m} \{j_i + rq | q \in \mathbb{N}\}$ for some $N \in \mathbb{N}$. But clearly $S_a \cap \{1, ..., N\}$ is finite so Theorem 5 follows trivially. It follows that it suffices to show that $\det M$ is nonzero. But it is trivial to see by induction that $|\det M| = |c_k| \neq 0$ so we are done. ■

There are several remarks to be made. First, note that the above proof effectively puts a bound on the size of the period, r. By taking the minimal prime p such that $p \nmid c_k$, we get that $r \leq |GL_k(\mathbb{F}_p)| = (p^k - 1)(p^k - p)...(p^k - p^{k-1})$. Bounding r also effectively bounds the size of the finite set because if r is big then N depends entirely on r. These are, of course, not very strict bounds and it is an area of active research to attempt better ones.

As stated in the beginning, the theorem holds in much greater generality, in particular in fields of characteristic 0. A natural question to ask is to what extent does the theorem hold in positive characteristic. To see this, we use an example from [Der05]. Consider the sequence over $\mathbb{F}_p(x)$ defined by

$$a_n = (2x + 2)a_{n-1} - (x^2 + 3x + 1)a_{n-2} + (x^2 + x)a_{n-3}$$

with $a_0 = -1$, $a_1 = 0$, and $a_2 = 2x^2$. The astute observer will note that this sequence is just given by

$$a_n = (x + 1)^n - x^n - 1$$

But by Frobenius, then, $a_{p^k} = 0$ for all $k \in \mathbb{N}$. This is clearly not a finite union of arithmetic progressions. There is, however, an extension of Theorem 5 that holds in arbitrary characteristic that says that the above is essentially the only way that our theorem can fail. Unfortunately, this lies outside of the scope of this paper and the interested reader is referred to [Der05].

References

[Der05] Harm Derkson. A Skolem-Mahler-Lech Theorem in Positive Characteristic and Finite Automata. *ArXiv Mathematics e-prints*, October 2005.

[Han86] Georges Hansel. A simple proof of the skolem-mahler-lech theorem. *Theor. Comput. Sci.*, 43(1):91–98, July 1986.

[Lec53] Christer Lech. A note on recurring series. *Ark. Mat.*, 2(5):417–421, 08 1953.