Effective Isotrivial Mordell-Lang in positive characteristic

Jason Bell (Joint with Dragos Ghioca and Rahim Moosa)

March 26, 2021

Linear recurrences

Given a field K and a sequence $f : \mathbb{N} \to K$, we say that f *satisfies a linear recurrence over* K (with constant coefficients) if there exists some $d \geq 1$ and $c_1, \ldots, c_d \in K$ such that

$$f(n) = \sum_{i=1}^{d} c_i f(n-i)$$

for n sufficiently large.

The following are equivalent conditions for a K-valued sequence:

- f satisfies a linear recurrence over K;
- $\sum f(n)x^n$ is the generating series for a rational function $P(x)/Q(x)$ with $Q(0) = 1$;
- there exists an invertible matrix A with entries and K and column vectors v and w such that $f(n) = w^T A^n v$ for n large;
- for n large, we have an expression

$$f(n) = \sum_{i=1}^{r} \sum_{j=1}^{s} c_{i,j} n^i \alpha_j^n.$$

Skolem's problem asks whether the following is true: Given an integer-valued sequence $f(n)$ satisfying a linear recurrence, is it decidable whether $f(n) = 0$ for some $n \in \mathbb{N}$?

This problem is still open, and it is one of these problems that's right on the cusp of being decidable/undecidable. I'll tell you a bit about why it's so hard right now.

When confronted with a difficult Diophantine problem over the integers, it's often natural to look at its counterpart over $\mathbb{F}_q[t]$ and ask what happens in this setting, since results over $\mathbb{Z}$ often have counterparts over $\mathbb{F}_q[t]$ and vice versa.

Here the problem is still quite difficult, but notice some simplifications hold. If K is a field of characteristic $p > 0$ and

$$f(n) = \sum_{i=1}^{r} \sum_{j=1}^{s} c_{i,j} n^i \alpha_j^n,$$

then for $a \in \{0, \ldots, p-1\}$,

$$f(pn + a) = \sum_{j=1}^{s} b_{a,j} \alpha_j^n$$

for some new constants $b_{a,j} \in \bar{K}$.

Linear recurrences that are of the form

$$f(n) = \sum_{i=1}^{q} c_i \beta_i^n$$

are called *simple* linear recurrences and they tend to be a bit easier to study. For example, the problem of eventual positivity is known to be decidable for simple linear recurrences (Ouaknine & Worrell) whereas it is still open in general.

In 2005, Derksen showed that Skolem's problem over fields of positive characteristic is decidable!

Derksen's Theorem

To explain Derksen's result, we give some background on finite automata. Let k be a positive integer ≥ 2. Then every nonnegative integer has a unique base-k expansion on the digits $0, \ldots, k-1$ with no "leading zeros".

For example, if $k = 3$, then the base-k expansion of 17 is 122, since $17 = 1 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0$.

In general, if w is a word on the alphabet $\{0, \ldots, k-1\}$ with no leading zeros that is the base-k expansion of n, we write $[w]_k = n$ and $(n)_k = w$.

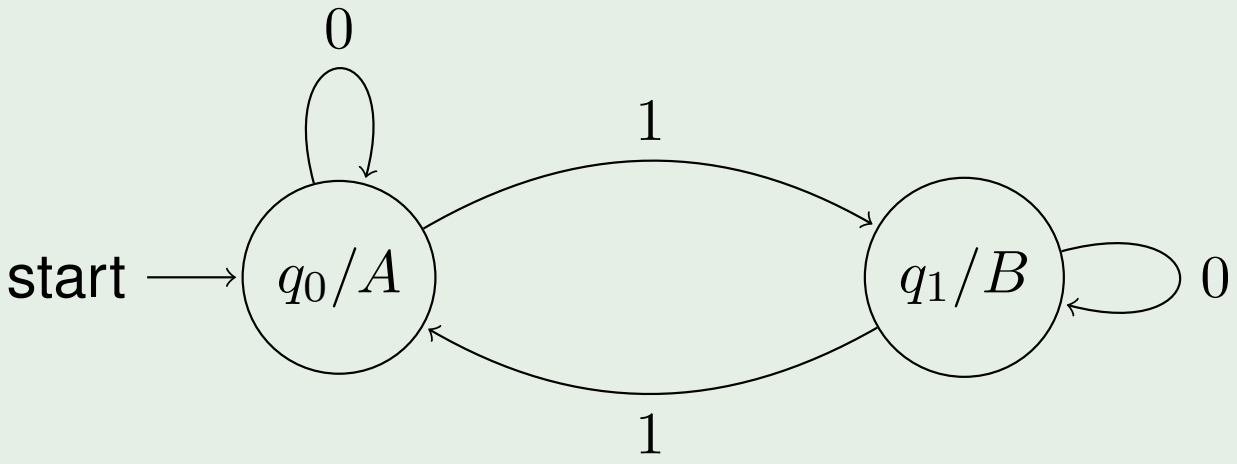
Convention: $[\epsilon]_k = 0$ and $(0)_k = \epsilon$, where ϵ is the empty word (the identity in the free monoid on the set $\{0, \ldots, k-1\}$.

Definition

A *finite-state k-automaton with output* is a finite directed graph where each vertex has out-degree k with labels $0, 1, 2, \ldots, k-1$, along with a special distinguished vertex (the initial state) and each vertex has an "output value" from some finite set Δ.

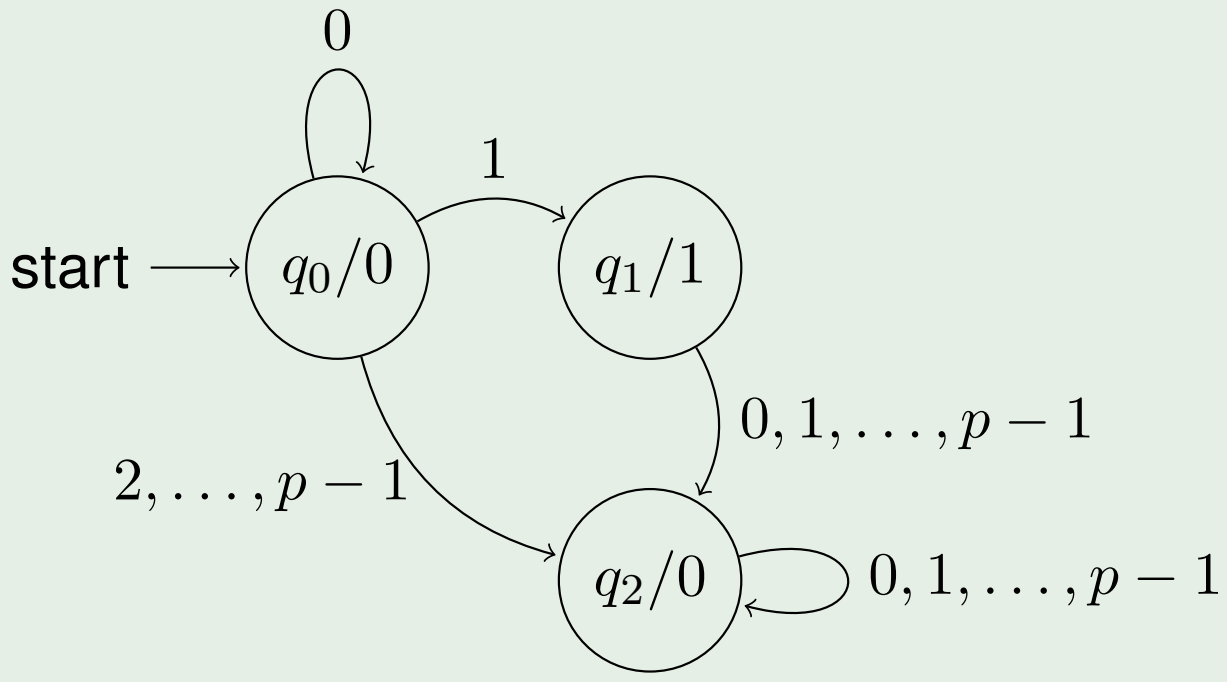
Note: if we have a finite-state k-automaton with output, we can associate a function from $f : \mathbb{N} \to \Delta$ as follows. Given $n \in \mathbb{N}$, we find $(n)_k \in \{0, \ldots, k-1\}^*$; we start at the initial state, reading the digits of $(n)_k$ from right-to-left, using the arrows to tell us where to go at each step. Once this process finishes, we look at the output value of the vertex we finish at and that is $\tau(n)$.

Example: The Thue-Morse automaton



Here: $k = 2$; If we look $(13)_2 = 1101$ and the output is B, so the associated map τ has $\tau(13) = B$. In general, we see that $\tau(n) = B$ if and only if n has an odd number of 1's in its binary expansion.

Example: A p-automaton generating powers of p



In the case that our k-automaton has output values $\{0, 1\}$, we can view the map $\tau : \mathbb{N} \to \{0, 1\}$ as giving us a subset of $\mathbb{N}$, which we call a *k-automatic set*.

Theorem

(Derksen) Let K be a field of positive characteristic p and let $f(n)$ be a K-valued sequence satisfying a linear recurrence. Then the set of n for which $f(n) = 0$ is a p-automatic set.

In fact, Derksen is able to explicitly construct the automaton associated to the sequence $f(n)$. To do this, observe we may assume K is finitely generated over $\mathbb{F}_p$. He then needs some data:

- A presentation $K = \mathrm{Frac}(R)$ with R a finitely presented $\mathbb{F}_p$-algebra;
- the recurrence satisfied by $f(n)$.

But this is enough to build the automaton and to bound the number of states!

Notice this shows that problems such as is $f(n) = 0$ for some n? is $f(n) = 0$ for infinitely many n decidable?

Recall that linear recurrences in positive characteristic are essentially simple: after passing to arithmetic progressions, we obtain simple recurrences, so it suffices to understand the simple case. If we look at

$$f(n) = c_1\alpha_1^n + \cdots + c_r\alpha_r^n,$$

then we can view the question "is there some n such that $f(n) = 0$?" geometrically.

If we let $G = (\bar{K}^*)^r$ and $\Gamma = \{(\alpha_1^j, \ldots, \alpha_r^j) \colon j \in \mathbb{N}\}$, then we are asking whether

$$\Gamma \cap X$$

is non-empty, where

$$X = \{(x_1, \ldots, x_r) \in G \colon \sum c_i x_i = 0\}.$$

The Mordell-Lang conjecture

When we put Skolem's problem in this geometric form, it is very closely related to the Mordell-Lang conjecture, which asks the following:

Let G be a semiabelian variety over a field of characteristic zero, let Γ be a finitely generated abelian subgroup of G, and let X be a closed subvariety of G. Then $X \cap \Gamma$ is a finite union of cosets of subgroups of Γ.

Note that $(\bar{K}^*)^r$ and abelian varieties are the prototypical examples of semiabelian varieties and all semiabelian varieties can be built up from such algebraic groups.

- Faltings proved this in 1994 in the case that G is an abelian variety, which was the context in which the problem was originally asked.
- Vojta proved the semiabelian case:

$$1 \to \mathbb{G}_m^r \to G \to A \to 1.$$

- McQuillan showed we could replace Γ by a finite rank abelian group.

Hrushovski's theorem

In postive characteristic, the Mordell-Lang conjecture does not hold in the form given:

- Let $K = \overline{\mathbb{F}_p(t)}$,
- let Γ be the group generated by $(1+t, t)$ in $(K^*)^2$,
- let $X = \{(x, y, z) \in (K^*)^2 : x - y = 1\}$.

What is $\Gamma \cap X$? Equivalently, what are the $n \in \mathbb{Z}$ for which $(1+t)^n - t^n = 1$?

When is

$$(1+t)^n - t^n = 1?$$

$n < 0$: Never! Look at poles!

$n = p^j$: $(1+t)^{p^j} - t^{p^j} = 1$!

$n > 0$ and not a power of p: $\binom{n}{j}$ is nonzero mod p for some $j \in \{1, \ldots, p-1\}$ and so $(1+t)^n - t^n \neq 1$ since t is an indeterminate.

So the set of n is $\{1, p, p^2, \ldots\}$. (A p-automatic set!)

So

$$X \cap \Gamma = \{((1+t)^{p^j}, t^{p^j}) \colon j \geq 1\},$$

which is not a union of cosets of subgroups of Γ.

Even for abelian varieties there are similar counterexamples. One way is to take a curve X defined over $\mathbb{F}_q$ of genus $g > 2$. Then take some finitely generated extension K of $\mathbb{F}_q$ such that X has a K-point that is not an $\overline{\mathbb{F}}_p$-point. Then by repeatedly applying the Frobenius, we get an infinite set of K-points on X.

Then X embeds in its Jacobian, G, and $\Gamma = G(K)$ is a finitely generated abelian group and $\Gamma \cap K$ will be infinite but will not contain a coset of an infinite subgroup of Γ.

Abramovich and Voloch gave a suggested way to salvage Mordell-Lang in positive characteristic (and proved it in some cases), which involves treating semiabelian G defined over a finite field (the isotrivial case) as special.

Theorem

(Hrushovski) Let G be a semiabelian variety defined over a field K/k (k algebraically closed), let X be a subvariety of G, and let Γ be a finitely generated subgroup of G. Suppose that $X \cap \Gamma$ is Zariski dense in X. Then there exists a semiabelian variety G_0 defined over k, a subvariety X_0 of G_0 defined over k, and a rational homomorphism h from a group subvariety of G into G_0, such that X is a translate of $h^{-1}(X_0)$.

We call such X *special*. So Hrushovski's result says that we just need to understand what happens over $\bar{\mathbb{Q}}$ in characteristic zero and over $\bar{\mathbb{F}}_p$ in characteristic p.

We've already seen what happens in characteristic 0, but what about positive characteristic.

Here we have beautiful work of Rahim Moosa and Tom Scanlon. To explain their work, we have to define F-sets.

F-sets

Notice that if K is a field extension of $\mathbb{F}_q$, then we have a q-Frobenius map on K: $x \mapsto x^q$. Then we have a q-Frobenius map on the K-points of $\mathbb{A}^n$ via

$$(\alpha_1, \ldots, \alpha_n) \mapsto (\alpha_1^q, \ldots, \alpha_n^q).$$

This is a regular map and if $X \subseteq \mathbb{A}^n$ is an affine variety, we can form $X^{(q)}$ by taking the Zariski closure of the $(\alpha_1^q, \ldots, \alpha_n^q)$ as we run over K-points in X. This gives us a map $F : X \to X^{(q)}$. By gluing, we can extend this construction to general quasiprojective varieties. Notice that if X is defined over $\mathbb{F}_q$, then $X^{(q)} = X$.

Then if we think of our isotrivial counterexamples to Mordell-Lang, we can phrase things in this language.

If $K = \overline{\mathbb{F}_p(t)}$ and $G = K^* \times K^*$ and $\Gamma = \langle((1+t), t)\rangle$ and $X = \{(x, y) \colon x - y = 1\}$. Then $X \cap \Gamma$ is the orbit of the point $((1+t), t)$ under the p-Frobenius map.

Moosa and Scanlon show that in the isotrivial case, the Mordell-Lang problem can be understood in terms of generalized Frobenius orbits, called F-sets, which we'll define soon.

Theorem

(Moosa-Scanlon) Let G be a semiabelian variety defined over a finite field $\mathbb{F}_q$, let $F : G \to G$ the q-Frobenius morphism, and let K be an algebraically closed field extension of $\mathbb{F}_q$. If $\Gamma \leq G(K)$ is a finitely generated $\mathbb{Z}[F]$-submodule of $G(K)$ and X is a closed subvariety of G then $X(K) \cap \Gamma$ is a finite union of F-sets.

But what is an F-set?

An F-set is a set that can be built up as a finite sums of these types of sets:

- cosets of $\mathbb{Z}[F]$-submodules of Γ;
- F^d-orbits of a point in Γ.

In particular, all the counterexamples to the classical Mordell-Lang conjecture in positive characteristic come from Frobenius orbits in a natural way.

What is the relationship between Derksen's Theorem and Moosa-Scanlon?

Notice we showed that you can encode finding the zero set of a linear recurrence sequence in positive characteristic as a question that looks a lot like Mordell-Lang. In particular, there should be some relationship between Moosa-Scanlon and Derksen. But it's not immediately clear what the connection is.

In work with Moosa, we showed (after a bit of work) that one can recover the *ineffective* aspects of Derksen's work using the work of Moosa and Scanlon. In that sense, one can view F-sets as a type of "automatic sets" in the context of semiabelian varieties. But interestingly, Derksen's work is effective and answers decidability questions, whereas Moosa-Scanlon does not.

This leads naturally to the question of whether one can do a more general effective version of Mordell-Lang in the isotrivial case, using methods from automata theory.

The answer is 'yes', but let's look first at some of the subtleties involved. Derksen was interested in the question of finding n such that $f(n) = 0$. Now we're interested in finding elements of Γ that are in X (i.e., describing $X \cap \Gamma$). For Derksen, he could use a machine that accepted the base-p expansion of n as input and gave 1 as output if and only if $f(n) = 0$.

So to carry out this plan, we need some way of having an analogue of "base-p" expansions of elements of Γ; that is, we need to be able to have some alphabet so that the elements of Γ correspond to strings on that alphabet.

F-expansions

Definition (Expansions)

Suppose M is an abelian group, $F : M \to M$ is an injective endomorphism, and $\Sigma \subseteq M$ is a finite subset. Given a word $w = x_0 x_1 \cdots x_m \in \Sigma^*$ we set

$$[w]_F := x_0 + Fx_1 + \cdots + F^m x_m \ \in \ M$$

and call this the *F-expansion of w*. Given $\mathcal{L} \subseteq \Sigma^*$ we denote by $[\mathcal{L}]_F$ the set of F-expansions of the words in $\mathcal{L}$. That is, $[\mathcal{L}]_F := \{[w]_F : w \in \mathcal{L}\}$.

Let $M = \mathbb{Z}$ and let $F : M \to M$ be the map $F(n) = 2n$ and let $\Sigma = \{-1, 0, 1\}$. Then every element of $\mathbb{Z}$ has a (not unique in general) F-expansion.

Why? If n is positive we write $n = 2^d a_d + \cdots + 2^0 a_0$ with each $a_i \in \{0, 1\}$ and $[a_d \cdots a_0]_F = n$. Similarly, for $n < 0$.

Now we really want some list of properties that say on the set $\Sigma \subset M$ that say that it can play a similar role that $\{0, \ldots, k-1\}$ does when dealing with base-k expansions. Here there are three key things that hold in base k-expansions that we want to capture.

- Every element of $\mathbb{N}$ has some base-k expansion. (Not necessarily unique.)
- Addition should be "nice" (i.e., while there may be carries, the sum of r, m-digit numbers has at most $m + c$-digits for c depending only on r and k.
- Multiplication by k should be "nice".

Really, we're thinking of multiplication by k as being our F and we want every element to have an F-expansion and for the F-expansion to be well-behaved with respect to the $\mathbb{Z}[F]$-module structure.

Rahim and I found the (somewhat technical conditions) one wants in the general setting.

Definition (Spanning sets)

Suppose M is an abelian group and $F : M \to M$ is an injective endomorphism. By an *F-spanning set for M* we will mean a finite subset $\Sigma \subseteq M$ satisfying the following properties:

(i) $[\Sigma^*]_F = M$,

(ii) Σ contains 0 and is symmetric (i.e., if $x \in \Sigma$ then $-x \in \Sigma$),

(iii) for all $x_1, \ldots, x_5 \in \Sigma$ there exist $t, t' \in \Sigma$ such that $x_1 + \cdots + x_5 = t + Ft'$, and

(iv) If $x_1, x_2, x_3 \in \Sigma$ and $x_1 + x_2 + x_3 \in F(M)$, then there exists $t \in \Sigma$ such that $x_1 + x_2 + x_3 = Ft$.

Rahim and I showed that even if this is a bit technical, there is always some r such that one can always find an F^r spanning set Σ in for a finitely generated $\mathbb{Z}[F]$-module M. So with this in place, we now have the foundations to try to build automata where the alphabet is a finite spanning set Σ of a $\mathbb{Z}[F]$-module $\Gamma \subseteq G$.

So back to M-L...

- Let G a commutative algebraic group over $\mathbb{F}_q$,
- Let $F : G \to G$ the q-power Frobenius endomorphism,
- Let $\Gamma \leq G$ a finitely generated $\mathbb{Z}[F]$-submodule of $G(K)$,
- Let $X \subseteq G$ is a closed subvariety.
- Let Σ be an F^r-spanning set of Γ (we'll assume $r = 1$ for simplicity).

How can we build a machine? We'll build a big directed graph in which each vertex will have $|\Sigma|$ out arrows, one with each label from Σ, and the vertices (states) will be a finite set of subvarieties of G, including X. Then the automaton will output 1 on a word $w \in \Sigma^*$ if and only if $[w]_F \in X$. So this will give a description of the intersection of $X \cap \Gamma$.

So what's the main idea? We have an element $[w]_F$ of Γ. So $w = a_0 \cdots a_d$ with each $a_i \in \Sigma$ and $[w]_F = a_0 + F(a_1) + \cdots + F^d(a_d)$ and we want to know whether $[w]_F \in X$. Notice that $[w]_F = a_0 + F([w']_F)$, where $w' = a_1 \cdots a_d$.

Then

$$[w]_F \in X \iff [w]_F \in X(K) \iff a_0 + F([w']_F) \in X(K)$$

So

$$[w]_F \in X \iff F^{-1}((X - a_0)(K^q)).$$

So now let X' be the Zariski closure of $F^{-1}((X - a_0)(K^q))$. Then $[w]_F \in X$ if and only if $[w']_F \in X'$.

Notice that we can repeat this process and we have $[w']_F = a_1 + F([w'']_F)$, where $w'' = a_2 \cdots a_d$, and we have

$$[w']_F \in X' \iff [w''] \in X'',$$

where X'' is the Zariski closure of $F^{-1}((X' - a_1)(K^q))$.

Now consider the smallest set $\mathcal{T}$ of subvarieties of G such that $X \in \mathcal{T}$ and such that if $Y \in \mathcal{T}$ and $a \in \Sigma$ then the Zariski closure of $F^{-1}((Y - a)(K^q))$ is in $\mathcal{T}$.

Rahim and Tom had shown that $\mathcal{T}$ is finite. By using a variant of Derksen's "Frobenius splitting" argument, we are able to effectively bound the size of $\mathcal{T}$ in terms of presentations of G, X, and K, and a generating set for Γ.

Bounding $|\mathcal{T}|$—the main idea

We recall that K is a finite-dimensional K^q-vector space, and if we fix a basis $e_1, \ldots, e_s$, we can construct Cartier operators $\pi_1, \ldots, \pi_s : K \to K$ via the rule

$$\alpha = \sum_{i=1}^{s} \pi_i(\alpha)^q e_i.$$

Then we have

$$\pi_i(\alpha + \beta^q \gamma) = \pi_i(\alpha) + \beta \pi_i(\gamma).$$

As an example, suppose $G \subseteq \mathbb{P}^2$ and

$$X = \{aX^3 + bY^3 + cZ^3 = 0\}.$$

Then $[\alpha^p : \beta^p : \gamma^p] \in X(K^p)$ if and only if

$$a\alpha^{3p} + b\beta^{3p} + c\gamma^{3p} = 0$$

And this holds if and only if

$$[\alpha : \beta : \gamma] \in X_i$$

for $i = 1, \ldots, s$, where

$$X_j = \{\pi_j(a)X^3 + \pi_j(b)Y^3 + \pi_j(c)Z^3\}$$

The Machine

Now we may a directed graph whose vertices are the varieties in $\mathcal{T}$. Given $Y, Y' \in \mathcal{T}$ and $a \in \Sigma$, we draw a directed edge from Y to Y' with label a if Y' is the Zariski closure of $F^{-1}((Y - a)(K^q))$.

Now we make X our distinguished starting vertex. Then a word $w \in \Sigma^*$ gives us a path on our directed graph that starts at the vertex X and ends at some vertex Z and by construction

$$[w]_F \in X \iff [\epsilon]_F = 0 \in Z.$$

So now we call $Z \in \mathcal{T}$ an accepting state if and only if Z contains 0. Then $[w]_F \in X$ if and only if the string w is accepted by our automaton.

Theorem

(B-G-M) Let G be a commutative algebraic group defined over $\mathbb{F}_q$, let F be q-Frobenius, and let Γ be a finitely generated $\mathbb{Z}[F]$-submodule of G.

Then $X \cap \Gamma$ is "automatic"; that is there is a spanning set Σ of Γ such that $[\mathcal{L}]_F = X \cap \Gamma$, where $\mathcal{L} \subseteq \Sigma^*$ is the set of words accepted by some finite-state automaton.

Moreover, one can effectively bound the size of the automaton from presentations for G, X, K, and generators for Γ as a $\mathbb{Z}[F]$-module.

This gives us an extension of Moosa-Scanlon to general commutative algebraic groups:

Theorem

(B-G-M) Let G be a commutative algebraic group over $\mathbb{F}_q$, $F : G \to G$ the q-power Frobenius, $X \subseteq G$ a closed subvariety, and $\Gamma \leq G$ a finitely generated $\mathbb{Z}[F]$-submodule. Then $X \cap \Gamma$ is a finite union of sets of the form $S + \Lambda$ where $S \subseteq \Gamma$ is is a translate of a sum of F-orbits and $\Lambda = H \cap \Gamma$ for some $H \leq G$ an algebraic subgroup over a finite field.

Remark.

Arguably the most interesting case is when G is an isotrivial abelian variety and $\Gamma = G(K)$, K a finitely generated extension of $\mathbb{F}_q$.

Here, there is a mechanism for producing generators for Γ due to Poonen, Testa, van Luijk:

Here one reduces to the case when K is the function field of a curve C over $\mathbb{F}_q$ and then one identifies $G(K)/G(\mathbb{F}_q)$ with $\mathrm{Hom}(\mathrm{Jac}(C), G)$.

This homomorphism group can be computed using the algorithm given by Poonen, Testa, and van Luijk to compute the Néron-Severi group for $G \times \mathrm{Jac}(C)$, using the fact that the Tate conjecture is known for abelian varieties.

Just as with Derksen's resolution of Skolem's problem in positive characteristic, we see that all of the following are decidable (with the given input data as above):

- Is $X \cap \Gamma$ empty?
- Is $X \cap \Gamma$ infinite?
- Does $X \cap \Gamma$ contain a coset of an infinite $\mathbb{Z}[F]$-submodule of Γ?

How do we tell if $X \cap \Gamma$ is really infinite? So there is the problem that maybe our machine accepts infinitely many distinct strings in Σ^* but how do we know if they give rise to infinitely many elements of Γ? The problem is that F-expansions are not in general unique.

Here we use a process that we call refinement. What it does is takes our old machine and creates a new one (with many more states, but which we can effectively bound), but which now, for each $c \in \Gamma \cap X$ accepts exactly one word w with $[w]_F = c$.

Refinement

We'd like to produce a regular sublanguage (meaning there's a machine that accepts it) $\mathcal{E}$ of Σ^* such that every element of Γ can be realized uniquely as the F-expansion from $\mathcal{E}$. This is implicitly done with base-k expansions, where we take $\mathcal{E}$ to be the elements of $\{0, \ldots, k-1\}^*$ without any leading zeros. So we'll put some order on the elements of Σ (where we make 0 the least element) and for each $c \in \Gamma$ we'd like to find the degree lexicographically least element $w \in \Sigma^*$ such that $[w]_F = c$.

How can we do this?

Now we use $\Gamma \times \Gamma$ is a $\mathbb{Z}[F]$-submodule of $G \times G$ and $\Sigma \times \Sigma$ is a spanning set for $\Gamma \times \Gamma$. Now we first build a machine that only accepts pairs (w, w') of strings of the same length such that neither w nor w' ends with 0 and w is less than w' under the lexicographic ordering.

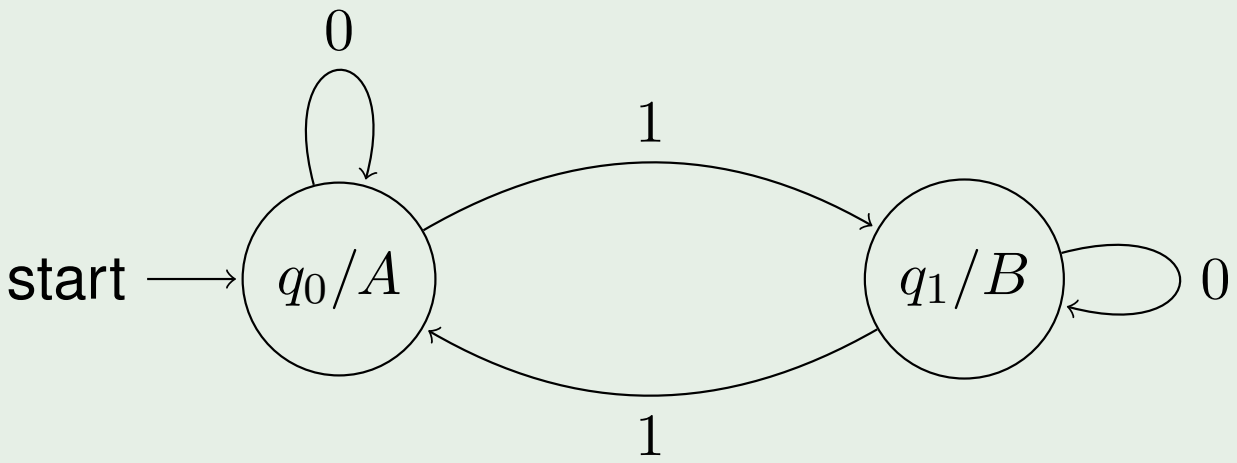
So now if we use our procedure from before with $X = \{(x, y) \in G \times G \colon x - y = 0\}$, to feed in all the pairs from above such that $[w]_F = [w']_F$.

Then we take the projection of the set of pairs of strings we found to the second coordinate. If we use the fact that intersections, complements, and projections of regular sets are regular, we can then build a machine that accepts the degree lexicographically least element of Σ^* realizing an element of Γ. So we have a refined sublanguage $\mathcal{E}$ of Σ^* that is recognized by a finite-state machine.

Now we can see that the question "Is $X \cap \Gamma$ infinite?" is decidable. We take the refinement $\mathcal{E}$ of Σ^* as given above and build a machine that accepts $w \in \mathcal{E}$ such that $[w]_F \in X$ using the fact that the intersection of two languages accepted by finite-state automata is again accepted by some other finite-state automaton, which can be built from the two machines.

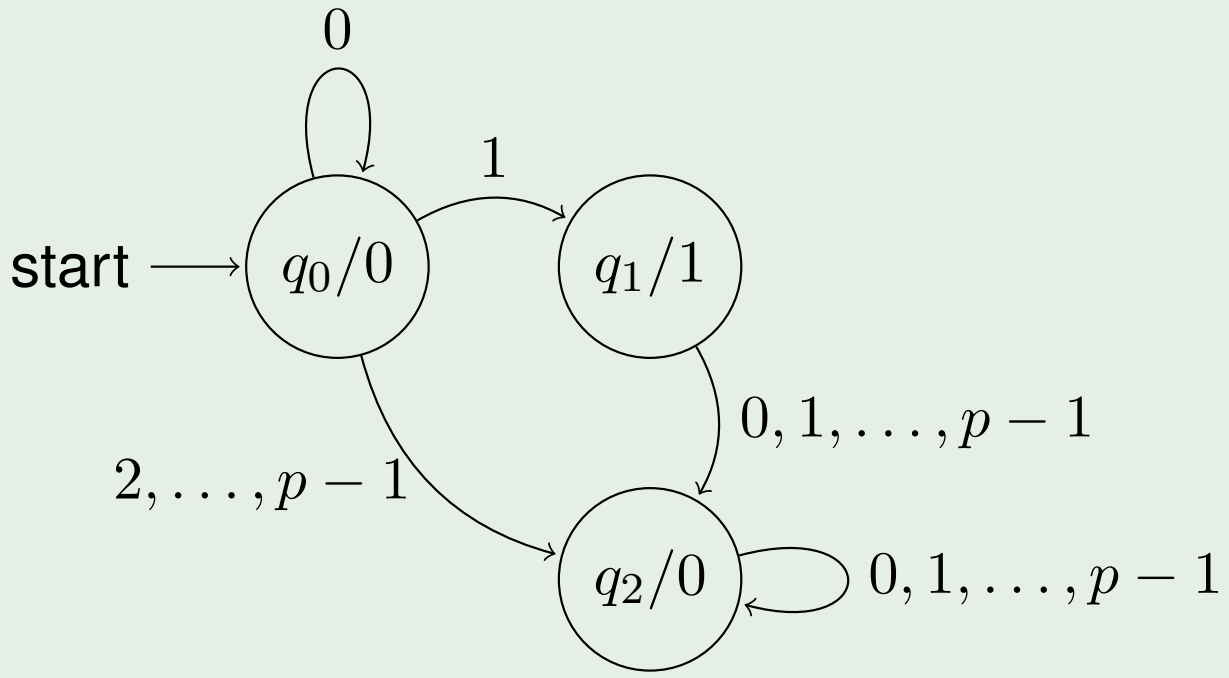
So this leaves us with the question of how do we tell when $X \cap \Gamma$ contains a coset of an infinite group? As it turns out, this is related to a well-known dichotomy in the theory of finite-state automata.

Thue-Morse revisited



If q_1 is accepting and q_0 is rejecting, the set of natural numbers up to x accepted by this automaton grows like $x/2$.

Prime powers revisited



If q_1 is accepting and the other states are rejecting, the set of natural numbers accepted by this automaton is $S = \{1, p, p^2, \ldots\}$ and so we accept roughly $\log_p(x)$ natural numbers up to x.

More generally, we have the following dichotomy for the growth type of automatic sets:
Let $S \subseteq \mathbb{N}$ be a k-automatic set. Then,

(i) either there exists an integer $d \geq 1$ such that $\pi_S(n) = O\left((\log n)^d\right)$ as $n \to \infty$,

(ii) or $\pi_S(n) > n^\alpha$ for some $\alpha > 0$ and for sufficiently large n.

Definition

In this setting, we call S *sparse* if (i) holds.

In terms of automata, sparseness is very easy to see: it's saying there's no vertices q with the property that there are two distinct cycles based at q and a path from q to an accepting state.

Theorem

(BGM) Let $\mathcal{E}$ be the refinement of Σ^* given above. Then $X \cap \Gamma$ contains a coset of an infinite group if and only if the automaton that accepts $w \in \mathcal{E}$ such that $[w]_F \in X$ is not sparse (i.e., it has a vertices q with the property that there are two distinct cycles based at q and a path from q to an accepting state).

The sparse/non-sparse dichotomy from automata gives rise to a corresponding dichotomy within the context of Mordell-Lang.

Theorem

(BGM) Let G be an abelian variety defined over $\mathbb{F}_q$, let $F : G \to G$ be the q-power Frobenius endomorphism, let K be a finitely generated field extension of $\mathbb{F}_q$, and let X be a closed subvariety of G over K. Denote by h the Néron-Tate canonical height on G. Then the following are equivalent:

1. *there are $C > 0$ and $d \geq 0$ such that for sufficiently large H*

$$\#\{c \in X(K) \colon h(c) \leq H\} \leq C(\log(H))^d;$$

2. $\#\{c \in X(K) \colon h(c) \leq H\} = \mathrm{o}(H^{1/2})$;
3. *$X(K)$ does not contain a coset of an infinite subgroup of Γ.*

Let's bring it back to Skolem's problem

We've seen that throughout the "natural" setting for isotrivial Mordell-Lang is to look at intersections of $X \cap \Gamma$ with Γ a finitely generated F-module. This is indeed the most common case one typically considers (e.g., K-points in an abelian variety, K finitely generated; finitely generated subgroups of multiplicative tori). But one can ask if it is decidable whether $X \cap \Gamma$ is non-empty when Γ is a finitely generated group that is not an F-module.

Surprisingly, the question brings us back to Skolem's problem for linear recurrences for the integers. If we have an abelian variety G and a finitely generated subgroup Γ_0 of $G(K)$ then the question of whether $\Gamma_0 \cap X$ is non-empty can be approached as follows:

- Find $G(K) \cap X$, which we know how to do.
- Then use the fact that Γ_0 can be recognized in terms of being the kernel of some $\mathbb{Z}$-module homomorphism $L : \Gamma \to \Gamma$.

If we do this procedure, we end up with a problem that is to decide whether one or more linear recurrences built from the eigenvalues of Frobenius take the value zero. This is actually very hard!

Thank you!