On some GCD, linear recurrences and unlikely intersection problems

Alina Ostafe

The University of New South Wales

Motivation

Outline some recent results motivated by the following

Basic Question:

Given $a, b \in \mathbb{Z}$, $a, b \geq 2$, what can one say about

$$\gcd\left(a^n - 1, b^n - 1\right)$$

and in particular prove that $a^n - 1$ and $b^n - 1$ are coprime for infinitely many n.

Bugeaud, Corvaja & Zannier (*2003*): Let $a, b \in \mathbb{Z}$, $a, b \geq 2$, be multiplicatively independent in $\mathbb{Q}^*$, and let $\varepsilon > 0$. For sufficiently large n,

$$\log \gcd\left(a^n - 1, b^n - 1\right) \leq \varepsilon n.$$

Motivation

Outline some recent results motivated by the following

Basic Question:

Given $a, b \in \mathbb{Z}$, $a, b \geq 2$, what can one say about

$$\gcd\left(a^n - 1, b^n - 1\right)$$

and in particular prove that $a^n - 1$ and $b^n - 1$ are coprime for infinitely many n.

Bugeaud, Corvaja & Zannier (*2003*): Let $a, b \in \mathbb{Z}$, $a, b \geq 2$, be multiplicatively independent in $\mathbb{Q}^*$, and let $\varepsilon > 0$. For sufficiently large n,

$$\log \gcd\left(a^n - 1, b^n - 1\right) \leq \varepsilon n.$$

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd \left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n \geq 1}$, $(G_m)_{m \geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \ldots, f_\ell^n)$, $G_m = G(g_1^m, \ldots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and

$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$

4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd\left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n\geq 1}$, $(G_m)_{m\geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \ldots, f_\ell^n)$, $G_m = G(g_1^m, \ldots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and
$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$
4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd\left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n\geq 1}$, $(G_m)_{m\geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \ldots, f_\ell^n)$, $G_m = G(g_1^m, \ldots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and
$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$
4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd\left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n\geq 1}$, $(G_m)_{m\geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \ldots, f_\ell^n)$, $G_m = G(g_1^m, \ldots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and

$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$

4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd\left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n\geq 1}$, $(G_m)_{m\geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \dots, f_\ell^n)$, $G_m = G(g_1^m, \dots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \dots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and

$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$

4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

In this talk we discuss the **function field** case, where the Basic Question becomes: for $f, g \in \mathbb{C}[X]$, give upper bounds for

$$\deg \gcd\left(f^n - 1, g^n - 1\right).$$

More generally, let $(F_n)_{n\geq 1}$, $(G_m)_{m\geq 1}$ be two interesting sequences of polynomials in $\mathbb{C}[X]$. We want uniform bounds for

$$\deg \gcd(F_n(X), G_m(X)) \quad \text{for all } n, m \geq 1.$$

Some examples include:

1. $F_n = F(f_1^n, \ldots, f_\ell^n)$, $G_m = G(g_1^m, \ldots, g_\ell^m)$, where $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$, $f_i, g_j \in \mathbb{C}[X]$.
2. (F_n), (G_m) are two linear recurrence sequences (LRS).
3. $F_n = f^{(n)} - c$, $G_m = g^{(m)} - c$, where $f, g, c \in \mathbb{C}[X]$, and

$$f^{(n)}(X) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ copies}}(X).$$

4. Combinations of the above, e.g., $F_n = X^n - 1$, $G_m = f^{(m)} - 1$.

Some of these GCD problems are intimately related to **unlikely intersection** problems for parametric curves, such as, intersection of curves with:

- torsion points (= roots of unity);
- division groups;
- algebraic subgroups of $\mathbb{G}_m^n$.

Why are we interested?

These problems are just *simply beautiful*!

They also naturally appear in various algorithmic/cryptographic applications. For example,

- *Sorenson & Webster* (*2017*): finding strong pseudoprimes to several bases simultaneously.
- *Luca & Shparlinski* (*2005*): Lower bounds on
  - exponents of the group of points,
  - embedding degree,

  of elliptic curves over high degree extensions of finite fields; both are related to *cryptography*.
- Links to the theory of exponential Diophantine equations, such as $F_m = G_n$ for two linear recurrence sequences and to the *Skolem Problem*.

Why are we interested?

These problems are just *simply beautiful*!

They also naturally appear in various algorithmic/cryptographic applications. For example,

- *Sorenson & Webster* (*2017*): finding strong pseudoprimes to several bases simultaneously.
- *Luca & Shparlinski* (*2005*): Lower bounds on
  - exponents of the group of points,
  - embedding degree,

  of elliptic curves over high degree extensions of finite fields; both are related to *cryptography*.
- Links to the theory of exponential Diophantine equations, such as $F_m = G_n$ for two linear recurrence sequences and to the *Skolem Problem*.

Why are we interested?

These problems are just *simply beautiful*!

They also naturally appear in various algorithmic/cryptographic applications. For example,

- *Sorenson & Webster* (*2017*): finding strong pseudoprimes to several bases simultaneously.
- *Luca & Shparlinski* (*2005*): Lower bounds on
  - exponents of the group of points,
  - embedding degree,

  of elliptic curves over high degree extensions of finite fields; both are related to *cryptography*.
- Links to the theory of exponential Diophantine equations, such as $F_m = G_n$ for two linear recurrence sequences and to the *Skolem Problem*.

Why are we interested?

These problems are just *simply beautiful*!

They also naturally appear in various algorithmic/cryptographic applications. For example,

- *Sorenson & Webster* (*2017*): finding strong pseudoprimes to several bases simultaneously.
- *Luca & Shparlinski* (*2005*): Lower bounds on
  - exponents of the group of points,
  - embedding degree,

  of elliptic curves over high degree extensions of finite fields; both are related to *cryptography*.
- Links to the theory of exponential Diophantine equations, such as $F_m = G_n$ for two linear recurrence sequences and to the *Skolem Problem*.

- *Chang* (*2013*) (plane curves), improving *Voloch* (*2007, 2010*), and *Chang, Kerr, Shparlinski and Zannier* (*2014*) (algebraic varieties): lower bounds for the order of points on curves or higher dimensional varieties over $\overline{\mathbb{F}}_p$, as steps toward Poonen's Conjecture.

  Such bounds also lead to explicit constructions of elements of finite fields of high order.
- Some of the above results and ideas have been used by *Bourgain, Gamburd & Sarnak* (*2016*) to describe the structure of solutions of the Markoff equation in reductions modulo sufficiently large primes. Building on these results *Chen* (*2021*) has essentially completed this characterisation.

  $$\Downarrow$$

  Fuchs, Lauter, Litman & Tran (*2021*): Markoff equation based cryptographic hash function.
- ...

- *Chang* (*2013*) (plane curves), improving *Voloch* (*2007, 2010*), and *Chang, Kerr, Shparlinski and Zannier* (*2014*) (algebraic varieties): lower bounds for the order of points on curves or higher dimensional varieties over $\overline{\mathbb{F}}_p$, as steps toward Poonen's Conjecture.

  Such bounds also lead to explicit constructions of elements of finite fields of high order.

- Some of the above results and ideas have been used by *Bourgain, Gamburd & Sarnak* (*2016*) to describe the structure of solutions of the Markoff equation in reductions modulo sufficiently large primes. Building on these results *Chen* (*2021*) has essentially completed this characterisation.

  $$\Downarrow$$

  Fuchs, Lauter, Litman & Tran (*2021*): Markoff equation based cryptographic hash function.

- ...

Notation and Formal Set Up

- $\alpha_1, \ldots, \alpha_s \in \mathbb{C}^*$ are multiplicatively independent (mult. indep.) if

$$\alpha_1^{k_1} \cdots \alpha_s^{k_s} \neq 1 \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

Otherwise $\alpha_1, \ldots, \alpha_s$ are multiplicatively dependent (mult. dep.).

- $f_1, \ldots, f_s \in \mathbb{C}(X)$ are mult. indep. with constants if

$$f_1^{k_1} \cdots f_s^{k_s} \notin \mathbb{C}^* \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

- $\mathbb{G}_m^n = (\mathbb{C}^*)^n$ the n-dimensional torus
$(\omega_1, \ldots, \omega_n) \in \mathbb{G}_m^n$ is called torsion point if all ω_i are roots of unity.

- $\alpha_1, \ldots, \alpha_s \in \mathbb{C}^*$ are multiplicatively independent (mult. indep.) if

$$\alpha_1^{k_1} \cdots \alpha_s^{k_s} \neq 1 \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

  Otherwise $\alpha_1, \ldots, \alpha_s$ are multiplicatively dependent (mult. dep.).

- $f_1, \ldots, f_s \in \mathbb{C}(X)$ are mult. indep. with constants if

$$f_1^{k_1} \cdots f_s^{k_s} \notin \mathbb{C}^* \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

- $\mathbb{G}_m^n = (\mathbb{C}^*)^n$ the n-dimensional torus
  $(\omega_1, \ldots, \omega_n) \in \mathbb{G}_m^n$ is called torsion point if all ω_i are roots of unity.

Notation and Formal Set Up

- $\alpha_1, \ldots, \alpha_s \in \mathbb{C}^*$ are multiplicatively independent (mult. indep.) if

$$\alpha_1^{k_1} \cdots \alpha_s^{k_s} \neq 1 \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

  Otherwise $\alpha_1, \ldots, \alpha_s$ are multiplicatively dependent (mult. dep.).

- $f_1, \ldots, f_s \in \mathbb{C}(X)$ are mult. indep. with constants if

$$f_1^{k_1} \cdots f_s^{k_s} \notin \mathbb{C}^* \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

- $\mathbb{G}_m^n = (\mathbb{C}^*)^n$ the n-dimensional torus
  $(\omega_1, \ldots, \omega_n) \in \mathbb{G}_m^n$ is called torsion point if all ω_i are roots of unity.

- $\alpha_1, \ldots, \alpha_s \in \mathbb{C}^*$ are multiplicatively independent (mult. indep.) if

$$\alpha_1^{k_1} \cdots \alpha_s^{k_s} \neq 1 \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

  Otherwise $\alpha_1, \ldots, \alpha_s$ are multiplicatively dependent (mult. dep.).

- $f_1, \ldots, f_s \in \mathbb{C}(X)$ are mult. indep. with constants if

$$f_1^{k_1} \cdots f_s^{k_s} \notin \mathbb{C}^* \qquad \forall (k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}.$$

- $\mathbb{G}_m^n = (\mathbb{C}^*)^n$ the n-dimensional torus
  $(\omega_1, \ldots, \omega_n) \in \mathbb{G}_m^n$ is called torsion point if all ω_i are roots of unity.

Some unlikely intersection problems

Underlying problem: Torsion points on plane curves

At the heart of the **function field** case, stays the following result conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Let $H(X,Y) \in \mathbb{C}[X,Y]$ be irreducible, not of the form $X^i - \rho Y^j$ or $X^iY^j - \rho$ with a root of unity ρ. Then the curve $H(X,Y) = 0$ has only finitely many torsion points (ζ_1, ζ_2).

Beukers & Smyth (*2002*): bound for the number of torsion points
Corvaja & Zannier (*2008*): bound for maximal order of torsion points

Remark: Since the orders are bounded we can effectively find all such points.

Reformulation of Lang's problem for plane rational curves: Let $f, g \in \mathbb{C}(X)$ be mult. indep. Then there are at most finitely many $\alpha \in \mathbb{C}$ such that

$$f(\alpha)^k = g(\alpha)^\ell = 1 \quad \text{for some } k, \ell \geq 1.$$

Underlying problem: Torsion points on plane curves

At the heart of the **function field** case, stays the following result conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Let $H(X,Y) \in \mathbb{C}[X,Y]$ be irreducible, not of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ with a root of unity ρ. Then the curve $H(X,Y) = 0$ has only finitely many torsion points (ζ_1, ζ_2).

Beukers & Smyth (*2002*): bound for the number of torsion points
Corvaja & Zannier (*2008*): bound for maximal order of torsion points

Remark: Since the orders are bounded we can effectively find all such points.

Reformulation of Lang's problem for plane rational curves: Let $f, g \in \mathbb{C}(X)$ be mult. indep. Then there are at most finitely many $\alpha \in \mathbb{C}$ such that

$$f(\alpha)^k = g(\alpha)^\ell = 1 \quad \text{for some } k, \ell \geq 1.$$

Underlying problem: Torsion points on plane curves

At the heart of the **function field** case, stays the following result conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Let $H(X,Y) \in \mathbb{C}[X,Y]$ be irreducible, not of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ with a root of unity ρ. Then the curve $H(X,Y) = 0$ has only finitely many torsion points (ζ_1, ζ_2).

Beukers & Smyth (*2002*): bound for the number of torsion points

Corvaja & Zannier (*2008*): bound for maximal order of torsion points

Remark: Since the orders are bounded we can effectively find all such points.

Reformulation of Lang's problem for plane rational curves: Let $f, g \in \mathbb{C}(X)$ be mult. indep. Then there are at most finitely many $\alpha \in \mathbb{C}$ such that

$$f(\alpha)^k = g(\alpha)^\ell = 1 \quad \text{for some } k, \ell \geq 1.$$

Underlying problem: Torsion points on plane curves

At the heart of the **function field** case, stays the following result conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Let $H(X,Y) \in \mathbb{C}[X,Y]$ be irreducible, not of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ with a root of unity ρ. Then the curve $H(X,Y) = 0$ has only finitely many torsion points (ζ_1, ζ_2).

Beukers & Smyth (*2002*): bound for the number of torsion points
Corvaja & Zannier (*2008*): bound for maximal order of torsion points

Remark: Since the orders are bounded we can effectively find all such points.

Reformulation of Lang's problem for plane rational curves: Let $f, g \in \mathbb{C}(X)$ be mult. indep. Then there are at most finitely many $\alpha \in \mathbb{C}$ such that

$$f(\alpha)^k = g(\alpha)^\ell = 1 \quad \text{for some } k, \ell \geq 1.$$

Underlying problem: Torsion points on plane curves

At the heart of the **function field** case, stays the following result conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Let $H(X,Y) \in \mathbb{C}[X,Y]$ be irreducible, not of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ with a root of unity ρ. Then the curve $H(X,Y) = 0$ has only finitely many torsion points (ζ_1, ζ_2).

Beukers & Smyth (*2002*): bound for the number of torsion points
Corvaja & Zannier (*2008*): bound for maximal order of torsion points

Remark: Since the orders are bounded we can effectively find all such points.

Reformulation of Lang's problem for plane rational curves: Let $f, g \in \mathbb{C}(X)$ be mult. indep. Then there are at most finitely many $\alpha \in \mathbb{C}$ such that

$$f(\alpha)^k = g(\alpha)^\ell = 1 \quad \text{for some } k, \ell \geq 1.$$

Unimodular points on rational curves

Instead of looking only at roots of unity, one can ask more generally about finiteness of $\alpha \in \mathbb{C}$ such that

$$|f(\alpha)| = |g(\alpha)| = 1.$$

Corvaja, Masser & Zannier (*2013*): finiteness result for $f(x) = x$, $g \in \mathbb{C}[x]$.

Pakovich & Shparlinski (2020)

Let $f, g \in \mathbb{C}(x)$. Then one has

$$\#\{\alpha \in \mathbb{C} : |f(\alpha)| = |g(\alpha)| = 1\} \leq (\deg f + \deg g)^2,$$

unless f and g are special (defined in terms of Blaschke products).

Remark 1: If $f, g \in \mathbb{C}[X]$, then

$$\text{special} = f \text{ and } g \text{ are mult. dep.}$$

Remark 2: Writing $\alpha = a + ib$ we obtain a system of two equations in a and b. Hence once we know the finiteness of solutions we can effectively find them all.

Unimodular points on rational curves

Instead of looking only at roots of unity, one can ask more generally about finiteness of $\alpha \in \mathbb{C}$ such that

$$|f(\alpha)| = |g(\alpha)| = 1.$$

Corvaja, Masser & Zannier (*2013*): finiteness result for $f(x) = x$, $g \in \mathbb{C}[x]$.

Pakovich & Shparlinski (2020)

Let $f, g \in \mathbb{C}(x)$. Then one has

$$\#\{\alpha \in \mathbb{C} : |f(\alpha)| = |g(\alpha)| = 1\} \le (\deg f + \deg g)^2,$$

unless f and g are special (defined in terms of Blaschke products).

Remark 1: If $f, g \in \mathbb{C}[X]$, then

special $=$ f and g are mult. dep.

Remark 2: Writing $\alpha = a + ib$ we obtain a system of two equations in a and b. Hence once we know the finiteness of solutions we can effectively find them all.

Unimodular points on rational curves

Instead of looking only at roots of unity, one can ask more generally about finiteness of $\alpha \in \mathbb{C}$ such that

$$|f(\alpha)| = |g(\alpha)| = 1.$$

Corvaja, Masser & Zannier (*2013*): finiteness result for $f(x) = x$, $g \in \mathbb{C}[x]$.

Pakovich & Shparlinski (2020)

Let $f, g \in \mathbb{C}(x)$. Then one has

$$\#\{\alpha \in \mathbb{C} : |f(\alpha)| = |g(\alpha)| = 1\} \le (\deg f + \deg g)^2,$$

unless f and g are special (defined in terms of Blaschke products).

Remark 1: If $f, g \in \mathbb{C}[X]$, then

$$\text{special} = f \text{ and } g \text{ are mult. dep.}$$

Remark 2: Writing $\alpha = a + ib$ we obtain a system of two equations in a and b. Hence once we know the finiteness of solutions we can effectively find them all.

Unimodular points on rational curves

Instead of looking only at roots of unity, one can ask more generally about finiteness of $\alpha \in \mathbb{C}$ such that

$$|f(\alpha)| = |g(\alpha)| = 1.$$

Corvaja, Masser & Zannier (*2013*): finiteness result for $f(x) = x$, $g \in \mathbb{C}[x]$.

Pakovich & Shparlinski (2020)

Let $f, g \in \mathbb{C}(x)$. Then one has

$$\#\{\alpha \in \mathbb{C} : |f(\alpha)| = |g(\alpha)| = 1\} \leq (\deg f + \deg g)^2,$$

unless f and g are special (defined in terms of Blaschke products).

Remark 1: If $f, g \in \mathbb{C}[X]$, then

special $=$ f and g are mult. dep.

Remark 2: Writing $\alpha = a + ib$ we obtain a system of two equations in a and b. Hence once we know the finiteness of solutions we can effectively find them all.

Intersection of curves with algebraic subgroups

Bombieri, Masser & Zannier (1999)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ *be mult. indep. with constants. Then*

$$\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}}) = \{\alpha \in \overline{\mathbb{Q}} : f_1(\alpha), \ldots, f_s(\alpha) \text{ are mult. dep.}\}$$

is a set of bounded Weil height.

Remarks:

- $\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}})$ is an infinite set.
- The proof is effective and gives explicit bound for the height.
- The condition on $f_1, \ldots, f_s$ being mult. indep. with constants is necessary, that is, it is not enough to be just mult. indep.

Example: Let $f_1(X) = 2X$, $f_2(X) = X^2$. Then f_1, f_2 are mult. indep., but there are infinitely many dependent values $(2^{m+1}, 2^{2m})$ for which the height is unbounded as $m \to \infty$.

Intersection of curves with algebraic subgroups

Bombieri, Masser & Zannier (1999)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ be mult. indep. with constants. Then

$$\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}}) = \{\alpha \in \overline{\mathbb{Q}} : f_1(\alpha), \ldots, f_s(\alpha) \text{ are mult. dep.}\}$$

is a set of bounded Weil height.

Remarks:

- $\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}})$ is an infinite set.
- The proof is effective and gives explicit bound for the height.
- The condition on $f_1, \ldots, f_s$ being mult. indep. with constants is necessary, that is, it is not enough to be just mult. indep.

Example: Let $f_1(X) = 2X$, $f_2(X) = X^2$. Then f_1, f_2 are mult. indep., but there are infinitely many dependent values $(2^{m+1}, 2^{2m})$ for which the height is unbounded as $m \to \infty$.

Intersection of curves with algebraic subgroups

Bombieri, Masser & Zannier (1999)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ *be mult. indep. with constants. Then*

$$\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}}) = \{\alpha \in \overline{\mathbb{Q}} : f_1(\alpha), \ldots, f_s(\alpha) \textit{ are mult. dep.}\}$$

is a set of bounded Weil height.

Remarks:

- $\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}})$ is an infinite set.
- The proof is effective and gives explicit bound for the height.
- The condition on $f_1, \ldots, f_s$ being mult. indep. with constants is necessary, that is, it is not enough to be just mult. indep.

Example: Let $f_1(X) = 2X$, $f_2(X) = X^2$. Then f_1, f_2 are mult. indep., but there are infinitely many dependent values $(2^{m+1}, 2^{2m})$ for which the height is unbounded as $m \to \infty$.

Intersection of curves with algebraic subgroups

Bombieri, Masser & Zannier (1999)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ be mult. indep. with constants. Then

$$\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}}) = \{\alpha \in \overline{\mathbb{Q}} : f_1(\alpha), \ldots, f_s(\alpha) \text{ are mult. dep.}\}$$

is a set of bounded Weil height.

Remarks:

- $\mathcal{S}_{f_1,\ldots,f_s}(\overline{\mathbb{Q}})$ is an infinite set.
- The proof is effective and gives explicit bound for the height.
- The condition on $f_1, \ldots, f_s$ being mult. indep. with constants is necessary, that is, it is not enough to be just mult. indep.

Example: Let $f_1(X) = 2X$, $f_2(X) = X^2$. Then f_1, f_2 are mult. indep., but there are infinitely many dependent values $(2^{m+1}, 2^{2m})$ for which the height is unbounded as $m \to \infty$.

Achieving finiteness

Maurin (2008)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ *be mult. indep. Then there are at most* **finitely** *many* $\alpha \in \overline{\mathbb{Q}}$ *such that*

$$f_1(\alpha)^{a_1} \cdots f_s(\alpha)^{a_s} = f_1(\alpha)^{b_1} \cdots f_s(\alpha)^{b_s} = 1$$

for some linearly independent vectors $(a_1, \ldots, a_s)$, $(b_1, \ldots, b_s) \in \mathbb{Z}^s$.

Bombieri, Masser & Zannier (*1999, 2003*): Proved this conclusion under the assumption that $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ are being mult. indep. modulo constants, and then extended their result to $\mathbb{C}$.

Bombieri, Habegger, Masser & Zannier (*2010*): gave a different proof (which is also effective) of Maurin's result.

Achieving finiteness

Maurin (2008)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ *be mult. indep. Then there are at most* **finitely** *many* $\alpha \in \overline{\mathbb{Q}}$ *such that*

$$f_1(\alpha)^{a_1} \cdots f_s(\alpha)^{a_s} = f_1(\alpha)^{b_1} \cdots f_s(\alpha)^{b_s} = 1$$

for some linearly independent vectors $(a_1, \ldots, a_s)$, $(b_1, \ldots, b_s) \in \mathbb{Z}^s$.

Bombieri, Masser & Zannier (*1999, 2003*): Proved this conclusion under the assumption that $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ are being mult. indep. modulo constants, and then extended their result to $\mathbb{C}$.

Bombieri, Habegger, Masser & Zannier (*2010*): gave a different proof (which is also effective) of Maurin's result.

Achieving finiteness

Maurin (2008)

Let $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ *be mult. indep. Then there are at most* **finitely** *many* $\alpha \in \overline{\mathbb{Q}}$ *such that*

$$f_1(\alpha)^{a_1} \cdots f_s(\alpha)^{a_s} = f_1(\alpha)^{b_1} \cdots f_s(\alpha)^{b_s} = 1$$

for some linearly independent vectors $(a_1, \ldots, a_s)$, $(b_1, \ldots, b_s) \in \mathbb{Z}^s$.

Bombieri, Masser & Zannier (*1999, 2003*): Proved this conclusion under the assumption that $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ are being mult. indep. modulo constants, and then extended their result to $\mathbb{C}$.

Bombieri, Habegger, Masser & Zannier (*2010*): gave a different proof (which is also effective) of Maurin's result.

Corollary: Let Γ be a finitely generated subgroup of $\overline{\mathbb{Q}}^*$ and $f_1, \ldots, f_s \in \overline{\mathbb{Q}}(X)$ mult. indep. modulo Γ. Then there are at most **finitely** many $\alpha \in \overline{\mathbb{Q}}$ such that

$$f_1(\alpha)^{a_1} \cdots f_s(\alpha)^{a_s}, f_1(\alpha)^{b_1} \cdots f_s(\alpha)^{b_s} \in \Gamma$$

for some linearly independent vectors

$$(a_1, \ldots, a_s), (b_1, \ldots, b_s) \in \mathbb{Z}^s.$$

Bounded height for zeros of polynomial recurrences

As a direct consequence of a more general result:

Amoroso, Masser & Zannier (2017)

Let $a_i, f_i \in \overline{\mathbb{Q}}(X)$, $i = 1, \ldots, k$, *be nonzero rational functions such that* f_s/f_r *is non-constant for any* $1 \le r < s \le k$. *There exists an effectively computable constant* C, *which depends on* $a_1, \ldots, a_k, f_1, \ldots, f_k$ *such that if for any* $n \ge C$ *and any* $\alpha \in \overline{\mathbb{Q}}$ *one has*

$$F_n(\alpha) = \sum_{i=1}^{k} a_i(\alpha) f_i(\alpha)^n = 0,$$

then

$$h(\alpha) \le C.$$

Remarks:

- If $a_i, f_i \in \overline{\mathbb{Q}}[X]$, for every given D there are only finitely many monic $h \in \overline{\mathbb{Q}}[X]$ of degree D such that $h \mid F_n$ for some n (if $F_n(X) \neq 0$).
- If $a_i \in \overline{\mathbb{Q}}$, then this is an instance of *unlikely intersection*, that is, we look at points P on a parametric curve such that $[n]P \in V$, where V is a hyperplane.

Kulkarni, Mavraki & Nguyen (*2015*): obtained a result of similar flavour.

Open Problem

Let

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$. Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \textit{ for some } n, m \geq 1\} < \infty.$$

Remarks:

- If $a_i, f_i \in \overline{\mathbb{Q}}[X]$, for every given D there are only finitely many monic $h \in \overline{\mathbb{Q}}[X]$ of degree D such that $h \mid F_n$ for some n (if $F_n(X) \neq 0$).
- If $a_i \in \overline{\mathbb{Q}}$, then this is an instance of *unlikely intersection*, that is, we look at points P on a parametric curve such that $[n]P \in V$, where V is a hyperplane.

Kulkarni, Mavraki & Nguyen (*2015*): obtained a result of similar flavour.

Open Problem

Let

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$. Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \text{ for some } n, m \geq 1\} < \infty.$$

Remarks:

- If $a_i, f_i \in \overline{\mathbb{Q}}[X]$, for every given D there are only finitely many monic $h \in \overline{\mathbb{Q}}[X]$ of degree D such that $h \mid F_n$ for some n (if $F_n(X) \neq 0$).
- If $a_i \in \overline{\mathbb{Q}}$, then this is an instance of *unlikely intersection*, that is, we look at points P on a parametric curve such that $[n]P \in V$, where V is a hyperplane.

Kulkarni, Mavraki & Nguyen (*2015*): obtained a result of similar flavour.

Open Problem

Let

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$. Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \text{ for some } n, m \geq 1\} < \infty.$$

Remarks:

- If $a_i, f_i \in \overline{\mathbb{Q}}[X]$, for every given D there are only finitely many monic $h \in \overline{\mathbb{Q}}[X]$ of degree D such that $h \mid F_n$ for some n (if $F_n(X) \neq 0$).
- If $a_i \in \overline{\mathbb{Q}}$, then this is an instance of *unlikely intersection*, that is, we look at points P on a parametric curve such that $[n]P \in V$, where V is a hyperplane.

Kulkarni, Mavraki & Nguyen (*2015*): obtained a result of similar flavour.

Open Problem

Let

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$. *Show that, under some natural conditions,*

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \text{ for some } n, m \geq 1\} < \infty.$$

GCD problems in function fields

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{C}$

Ailon & Rudnick (2004)

Let $f, g \in \mathbb{C}[X]$ *be mult. indep. over* $\mathbb{C}(X)$*. For all* $n \geq 1$*, there exists* $h \in \mathbb{C}[X]$ *such that*

$$\gcd(f^n - 1, g^n - 1) \mid h.$$

If in addition,

$$\gcd(f - 1, g - 1) = 1,$$

then there is a finite union of arithmetic progressions $\cup d_i\mathbb{N}$*,* $d_i \geq 2$*, such that for* n *outside these progressions,*

$$\gcd(f^n - 1, g^n - 1) = 1.$$

$\Uparrow$

Torsion points on plane curves

Remark: By *Beukers & Smyth* (*2002*):

$$\deg h \leq \left(11(\deg f + \deg g)^2\right)^{\min(\deg f, \deg g)}.$$

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{C}$

Ailon & Rudnick (2004)

Let $f, g \in \mathbb{C}[X]$ *be mult. indep. over* $\mathbb{C}(X)$*. For all* $n \geq 1$*, there exists* $h \in \mathbb{C}[X]$ *such that*

$$\gcd(f^n - 1, g^n - 1) \mid h.$$

If in addition,

$$\gcd(f - 1, g - 1) = 1,$$

then there is a finite union of arithmetic progressions $\cup d_i \mathbb{N}$, $d_i \geq 2$*, such that for* n *outside these progressions,*

$$\gcd(f^n - 1, g^n - 1) = 1.$$

$\Uparrow$

Torsion points on plane curves

Remark: By *Beukers & Smyth* (*2002*):

$$\deg h \leq \left(11(\deg f + \deg g)^2\right)^{\min(\deg f, \deg g)}.$$

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{C}$

Ailon & Rudnick (2004)

Let $f, g \in \mathbb{C}[X]$ *be mult. indep. over* $\mathbb{C}(X)$. *For all* $n \geq 1$, *there exists* $h \in \mathbb{C}[X]$ *such that*

$$\gcd(f^n - 1, g^n - 1) \mid h.$$

If in addition,

$$\gcd(f - 1, g - 1) = 1,$$

then there is a finite union of arithmetic progressions $\cup d_i\mathbb{N}$, $d_i \geq 2$, *such that for* n *outside these progressions,*

$$\gcd(f^n - 1, g^n - 1) = 1.$$

$$\Uparrow$$

Torsion points on plane curves

Remark: By *Beukers & Smyth* (*2002*):

$$\deg h \leq \left(11(\deg f + \deg g)^2\right)^{\min(\deg f, \deg g)}.$$

Let $S \subset \mathbb{C}$ be a finite set and let $u, v \in \mathbb{C}(X)$ be mult. indep. rational functions with all their zeroes and poles in S.

Corvaja & Zannier (*2008*):

$$\deg \gcd(u-1, v-1) \ll_S \max(\deg u, \deg v)^{2/3}.$$

If we take $f, g \in \mathbb{C}[X]$ mult. indep., and $u = f^n, v = g^n$, then one gets

$$\deg \gcd(f^n - 1, g^n - 1) \ll n^{2/3}$$

which improves the trivial bound $\ll n$.

Remark: Although apparently weaker, one can still recover the Ailon-Rudnick result from this bound (when $f, g \in \overline{\mathbb{Q}}[X]$).

Let $S \subset \mathbb{C}$ be a finite set and let $u, v \in \mathbb{C}(X)$ be mult. indep. rational functions with all their zeroes and poles in S.

Corvaja & Zannier (*2008*):

$$\deg \gcd(u-1, v-1) \ll_S \max(\deg u, \deg v)^{2/3}.$$

If we take $f, g \in \mathbb{C}[X]$ mult. indep., and $u = f^n, v = g^n$, then one gets

$$\deg \gcd(f^n - 1, g^n - 1) \ll n^{2/3}$$

which improves the trivial bound $\ll n$.

Remark: Although apparently weaker, one can still recover the Ailon-Rudnick result from this bound (when $f, g \in \overline{\mathbb{Q}}[X]$).

Let $S \subset \mathbb{C}$ be a finite set and let $u, v \in \mathbb{C}(X)$ be mult. indep. rational functions with all their zeroes and poles in S.

Corvaja & Zannier (*2008*):

$$\deg \gcd(u-1, v-1) \ll_S \max(\deg u, \deg v)^{2/3}.$$

If we take $f, g \in \mathbb{C}[X]$ mult. indep., and $u = f^n, v = g^n$, then one gets

$$\deg \gcd(f^n - 1, g^n - 1) \ll n^{2/3}$$

which improves the trivial bound $\ll n$.

Remark: Although apparently weaker, one can still recover the Ailon-Rudnick result from this bound (when $f, g \in \overline{\mathbb{Q}}[X]$).

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{F}_q$

The exact analogue of the Ailon-Rudnick result does **not** hold over $\mathbb{F}_q$.

Let $f, g \in \mathbb{F}_q[X]$ nonconstant polynomials.

In this case, one needs to impose more restrictions on n as, for example,

$$\gcd\left(f^{np^k} - 1, g^{np^k} - 1\right) = \gcd\left(f^n - 1, g^n - 1\right)^{p^k}.$$

However, *Silverman* (*2004*) has observed that even forbidding cheating with powers of p does not save us.

Example: *Silverman* (*2004*)

Let $f(X) = X$, $g(X) = X + 1$ and $n = p^k - 1$. Then

$$\deg \gcd\left(f^n - 1, g^n - 1\right) = n - 1$$

since any $\alpha \in \mathbb{F}_{p^k} \setminus \{0, -1\}$ is a root.

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{F}_q$

The exact analogue of the Ailon-Rudnick result does **not** hold over $\mathbb{F}_q$.

Let $f, g \in \mathbb{F}_q[X]$ nonconstant polynomials.

In this case, one needs to impose more restrictions on n as, for example,

$$\gcd\left(f^{np^k} - 1, g^{np^k} - 1\right) = \gcd\left(f^n - 1, g^n - 1\right)^{p^k}.$$

However, *Silverman* (*2004*) has observed that even forbidding cheating with powers of p does not save us.

Example: *Silverman* (*2004*)

Let $f(X) = X$, $g(X) = X + 1$ and $n = p^k - 1$. Then

$$\deg\gcd\left(f^n - 1, g^n - 1\right) = n - 1$$

since any $\alpha \in \mathbb{F}_{p^k} \setminus \{0, -1\}$ is a root.

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{F}_q$

The exact analogue of the Ailon-Rudnick result does **not** hold over $\mathbb{F}_q$.

Let $f, g \in \mathbb{F}_q[X]$ nonconstant polynomials.

In this case, one needs to impose more restrictions on n as, for example,

$$\gcd\left(f^{np^k} - 1, g^{np^k} - 1\right) = \gcd\left(f^n - 1, g^n - 1\right)^{p^k}.$$

However, *Silverman* (*2004*) has observed that even forbidding cheating with powers of p does not save us.

Example: *Silverman* (*2004*)

Let $f(X) = X$, $g(X) = X + 1$ and $n = p^k - 1$. Then

$$\deg \gcd\left(f^n - 1, g^n - 1\right) = n - 1$$

since any $\alpha \in \mathbb{F}_{p^k} \setminus \{0, -1\}$ is a root.

$\gcd(f^n - 1, g^n - 1)$ over $\mathbb{F}_q$

The exact analogue of the Ailon-Rudnick result does **not** hold over $\mathbb{F}_q$.

Let $f, g \in \mathbb{F}_q[X]$ nonconstant polynomials.

In this case, one needs to impose more restrictions on n as, for example,

$$\gcd\left(f^{np^k} - 1, g^{np^k} - 1\right) = \gcd\left(f^n - 1, g^n - 1\right)^{p^k}.$$

However, *Silverman* (*2004*) has observed that even forbidding cheating with powers of p does not save us.

Example: *Silverman* (*2004*)

Let $f(X) = X$, $g(X) = X + 1$ and $n = p^k - 1$. Then

$$\deg \gcd\left(f^n - 1, g^n - 1\right) = n - 1$$

since any $\alpha \in \mathbb{F}_{p^k} \setminus \{0, -1\}$ is a root.

More generally, we have:

Silverman (*2004*): for any nonconstant polynomials $f, g \in \mathbb{F}_q[X]$, there exists a constant $c = c(f, g) > 0$ such that for infinitely many n,

$$\deg \gcd\left(f^n - 1, g^n - 1\right) \geq cn.$$

Corvaja & Zannier (*2013*): Let $S \subset \overline{\mathbb{F}}_q$ be a finite set and let $u, v \in \mathbb{F}_q(X)$ be mult. indep. rational functions modulo $\mathbb{F}_q^*$, with nonzero differentials and with all their zeroes and poles in S. We also denote $d = \max(\deg u, \deg v)$. Then,

$$\deg \gcd(u - 1, v - 1) \ll_S \max\left(d^{2/3}, d^2/p\right).$$

Nontrivial: when $d \ll p$.

Remark: If $d^4 \ll p^3$, the result is the same as over $\mathbb{C}$.

More generally, we have:

Silverman (*2004*): for any nonconstant polynomials $f, g \in \mathbb{F}_q[X]$, there exists a constant $c = c(f, g) > 0$ such that for infinitely many n,

$$\deg \gcd (f^n - 1, g^n - 1) \geq cn.$$

Corvaja & Zannier (*2013*): Let $S \subset \overline{\mathbb{F}}_q$ be a finite set and let $u, v \in \mathbb{F}_q(X)$ be mult. indep. rational functions modulo $\mathbb{F}_q^*$, with nonzero differentials and with all their zeroes and poles in S. We also denote $d = \max(\deg u, \deg v)$. Then,

$$\deg \gcd(u - 1, v - 1) \ll_S \max \left(d^{2/3}, d^2/p\right).$$

Nontrivial: when $d \ll p$.

Remark: If $d^4 \ll p^3$, the result is the same as over $\mathbb{C}$.

More generally, we have:

Silverman (*2004*): for any nonconstant polynomials $f, g \in \mathbb{F}_q[X]$, there exists a constant $c = c(f, g) > 0$ such that for infinitely many n,

$$\deg \gcd\left(f^n - 1, g^n - 1\right) \geq cn.$$

Corvaja & Zannier (*2013*): Let $S \subset \overline{\mathbb{F}}_q$ be a finite set and let $u, v \in \mathbb{F}_q(X)$ be mult. indep. rational functions modulo $\mathbb{F}_q^*$, with nonzero differentials and with all their zeroes and poles in S. We also denote $d = \max(\deg u, \deg v)$. Then,

$$\deg \gcd(u - 1, v - 1) \ll_S \max\left(d^{2/3}, d^2/p\right).$$

Nontrivial: when $d \ll p$.

Remark: If $d^4 \ll p^3$, the result is the same as over $\mathbb{C}$.

More generally, we have:

Silverman (*2004*): for any nonconstant polynomials $f, g \in \mathbb{F}_q[X]$, there exists a constant $c = c(f, g) > 0$ such that for infinitely many n,

$$\deg \gcd \left(f^n - 1, g^n - 1\right) \geq cn.$$

Corvaja & Zannier (*2013*): Let $S \subset \overline{\mathbb{F}}_q$ be a finite set and let $u, v \in \mathbb{F}_q(X)$ be mult. indep. rational functions modulo $\mathbb{F}_q^*$, with nonzero differentials and with all their zeroes and poles in S. We also denote $d = \max(\deg u, \deg v)$. Then,

$$\deg \gcd(u - 1, v - 1) \ll_S \max\left(d^{2/3}, d^2/p\right).$$

Nontrivial: when $d \ll p$.

Remark: If $d^4 \ll p^3$, the result is the same as over $\mathbb{C}$.

For $u = x^d$ and $v = (1-x)^d$ this is a question about the number of solutions to

$$x + y = 1$$

in variables from the subgroup of $\overline{\mathbb{F}}_q^*$ of order d. This dates back to

Garcia & Voloch (*1988*)
Heath-Brown & Konyagin (*2000*)

Ghioca, Hsia & Tucker (*2017*): several other extensions, for example proving finiteness result for the set of roots of gcd's of the form

$$\gcd\left(f_1^n - g_1, f_2^m - g_2\right), \quad n, m \geq 1,$$

where $f_1, f_2, g_1, g_2 \in \mathbb{F}[X]$ ($\mathbb{F}$ is a field of char $p > 0$) are fixed and f_1 and f_2 are algebraically independent over $\mathbb{F}_p$.

For $u = x^d$ and $v = (1-x)^d$ this is a question about the number of solutions to

$$x + y = 1$$

in variables from the subgroup of $\overline{\mathbb{F}}_q^*$ of order d. This dates back to

Garcia & Voloch (*1988*)
Heath-Brown & Konyagin (*2000*)

Ghioca, Hsia & Tucker (*2017*): several other extensions, for example proving finiteness result for the set of roots of gcd's of the form

$$\gcd\left(f_1^n - g_1, f_2^m - g_2\right), \quad n, m \geq 1,$$

where $f_1, f_2, g_1, g_2 \in \mathbb{F}[X]$ ($\mathbb{F}$ is a field of char $p > 0$) are fixed and f_1 and f_2 are algebraically independent over $\mathbb{F}_p$.

For $u = x^d$ and $v = (1-x)^d$ this is a question about the number of solutions to

$$x + y = 1$$

in variables from the subgroup of $\overline{\mathbb{F}}_q^*$ of order d. This dates back to

Garcia & Voloch (*1988*)
Heath-Brown & Konyagin (*2000*)

Ghioca, Hsia & Tucker (*2017*): several other extensions, for example proving finiteness result for the set of roots of gcd's of the form

$$\gcd\left(f_1^n - g_1, f_2^m - g_2\right), \quad n, m \geq 1,$$

where $f_1, f_2, g_1, g_2 \in \mathbb{F}[X]$ ($\mathbb{F}$ is a field of char $p > 0$) are fixed and f_1 and f_2 are algebraically independent over $\mathbb{F}_p$.

Coming back to $\mathbb{C}$

Corvaja & Zannier (*2008*):

$$\deg \gcd(u-1, v-1) \ll_S \max(\deg u, \deg v)^{2/3}.$$

Question: For $f_1, \ldots, f_s, g_1, \ldots, g_r \in \mathbb{C}[X]$, can we have a **uniform bound** when

$$u = f_1^{n_1} \cdots f_s^{n_s} \qquad \text{and} \qquad v = g_1^{m_1} \cdots g_r^{m_r}$$

for all $n_1, \ldots, n_s, m_1, \ldots, m_r$?

If one restricts the polynomials to being defined over number fields, one can achieve uniformness, even in the more general case of

$$\gcd\left(h_1(f_1^{n_1} \cdots f_s^{n_s}), h_2(g_1^{m_1} \cdots g_r^{m_r})\right), \quad n_i, m_j \geq 0.$$

Coming back to $\mathbb{C}$

Corvaja & Zannier (*2008*):

$$\deg \gcd(u-1, v-1) \ll_S \max(\deg u, \deg v)^{2/3}.$$

Question: For $f_1, \ldots, f_s, g_1, \ldots, g_r \in \mathbb{C}[X]$, can we have a **uniform bound** when

$$u = f_1^{n_1} \cdots f_s^{n_s} \qquad \text{and} \qquad v = g_1^{m_1} \cdots g_r^{m_r}$$

for all $n_1, \ldots, n_s, m_1, \ldots, m_r$?

If one restricts the polynomials to being defined over number fields, one can achieve uniformness, even in the more general case of

$$\gcd\left(h_1(f_1^{n_1} \cdots f_s^{n_s}), h_2(g_1^{m_1} \cdots g_r^{m_r})\right), \quad n_i, m_j \geq 0.$$

A.O. & Shparlinski (2020)

Let $\Gamma \subseteq \overline{\mathbb{Q}}^*$ *be a finitely generated group and* $f_1, \ldots, f_s, g_1, \ldots, g_r \in \overline{\mathbb{Q}}[X]$ *mult. indep. modulo* Γ. *Then there exists* $H \in \overline{\mathbb{Q}}[X]$ *such that for any monic* $h_1, h_2 \in \overline{\mathbb{Q}}[X]$ *of fixed degree, with roots in* Γ, *one has*

$$\gcd\left(h_1(f_1^{n_1} \cdots f_s^{n_s}), h_2(g_1^{m_1} \cdots g_r^{m_r})\right) \mid H.$$

Considering the factorisations of h_1 and h_2 into linear factors, we reduce the problem to looking at

$$\mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right)$$

for any roots ω_1 and ω_2 of h_1 and h_2, respectively, for any

$$\mathbf{n} = (n_1, \ldots, n_s), \quad \mathbf{m} = (m_1, \ldots, m_s).$$

$$\Uparrow$$

Intersection of parametric curves with algebraic subgroups

A.O. & Shparlinski (2020)

Let $\Gamma \subseteq \overline{\mathbb{Q}}^*$ *be a finitely generated group and* $f_1, \ldots, f_s, g_1, \ldots, g_r \in \overline{\mathbb{Q}}[X]$ *mult. indep. modulo* Γ*. Then there exists* $H \in \overline{\mathbb{Q}}[X]$ *such that for any monic* $h_1, h_2 \in \overline{\mathbb{Q}}[X]$ *of fixed degree, with roots in* Γ*, one has*

$$\gcd\left(h_1(f_1^{n_1} \cdots f_s^{n_s}), h_2(g_1^{m_1} \cdots g_r^{m_r})\right) \mid H.$$

Considering the factorisations of h_1 and h_2 into linear factors, we reduce the problem to looking at

$$\mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right)$$

for any roots ω_1 and ω_2 of h_1 and h_2, respectively, for any

$$\mathbf{n} = (n_1, \ldots, n_s), \quad \mathbf{m} = (m_1, \ldots, m_s).$$

$\Uparrow$

Intersection of parametric curves with algebraic subgroups

A.O. & Shparlinski (2020)

Let $\Gamma \subseteq \overline{\mathbb{Q}}^*$ *be a finitely generated group and* $f_1, \ldots, f_s, g_1, \ldots, g_r \in \overline{\mathbb{Q}}[X]$ *mult. indep. modulo* Γ*. Then there exists* $H \in \overline{\mathbb{Q}}[X]$ *such that for any monic* $h_1, h_2 \in \overline{\mathbb{Q}}[X]$ *of fixed degree, with roots in* Γ*, one has*

$$\gcd\left(h_1(f_1^{n_1} \cdots f_s^{n_s}), h_2(g_1^{m_1} \cdots g_r^{m_r})\right) \mid H.$$

Considering the factorisations of h_1 and h_2 into linear factors, we reduce the problem to looking at

$$\mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right)$$

for any roots ω_1 and ω_2 of h_1 and h_2, respectively, for any

$$\mathbf{n} = (n_1, \ldots, n_s), \quad \mathbf{m} = (m_1, \ldots, m_s).$$

$$\Uparrow$$

Intersection of parametric curves with algebraic subgroups

Maurin (*2008*)

$\Downarrow$

There are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X-\alpha) \mid \mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1}\cdots f_s^{n_s}-\omega_1, g_1^{m_1}\cdots g_r^{m_r}-\omega_2\right).$$

$+$

Controlling multiplicities via *Mason's* (*1984*) polynomial ABC

$\Downarrow$

One can construct the polynomial $H_{\omega_1,\omega_2} \in \overline{\mathbb{Q}}[X]$ such that

$$\gcd\left(f_1^{n_1}\cdots f_s^{n_s}-\omega_1, g_1^{m_1}\cdots g_r^{m_r}-\omega_2\right) \mid H_{\omega_1,\omega_2}.$$

Remark: If $s=r=1$, *Bérczes, Evertse, Györy & Pontreau* (*2013*):
$h(\alpha), [\mathbb{K}(\alpha):\mathbb{K}] \ll_{f,\mathbb{K},\Gamma} 1 \Longrightarrow$ We get an explicit bound for $\deg H_{\omega_1,\omega_2}$.

Maurin (*2008*)

$$\Downarrow$$

There are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right).$$

$$+$$

Controlling multiplicities via *Mason's* (*1984*) polynomial ABC

$$\Downarrow$$

One can construct the polynomial $H_{\omega_1,\omega_2} \in \overline{\mathbb{Q}}[X]$ such that

$$\gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right) \mid H_{\omega_1,\omega_2}.$$

Remark: If $s = r = 1$, *Bérczes, Evertse, Györy & Pontreau* (*2013*):
$h(\alpha), [\mathbb{K}(\alpha) : \mathbb{K}] \ll_{f,\mathbb{K},\Gamma} 1 \Longrightarrow$ We get an explicit bound for $\deg H_{\omega_1,\omega_2}$.

Maurin (2008)

$$\Downarrow$$

There are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right).$$

$$+$$

Controlling multiplicities via *Mason's* (*1984*) polynomial ABC

$$\Downarrow$$

One can construct the polynomial $H_{\omega_1,\omega_2} \in \overline{\mathbb{Q}}[X]$ such that

$$\gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right) \mid H_{\omega_1,\omega_2}.$$

Remark: If $s = r = 1$, *Bérczes, Evertse, Györy & Pontreau* (*2013*):
$h(\alpha), [\mathbb{K}(\alpha) : \mathbb{K}] \ll_{f,\mathbb{K},\Gamma} 1 \Longrightarrow$ We get an explicit bound for $\deg H_{\omega_1,\omega_2}$.

Maurin (2008)

$$\Downarrow$$

There are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X-\alpha) \mid \mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1}\cdots f_s^{n_s} - \omega_1, g_1^{m_1}\cdots g_r^{m_r} - \omega_2\right).$$

$$+$$

Controlling multiplicities via *Mason's* (*1984*) polynomial ABC

$$\Downarrow$$

One can construct the polynomial $H_{\omega_1,\omega_2} \in \overline{\mathbb{Q}}[X]$ such that

$$\gcd\left(f_1^{n_1}\cdots f_s^{n_s} - \omega_1, g_1^{m_1}\cdots g_r^{m_r} - \omega_2\right) \mid H_{\omega_1,\omega_2}.$$

Remark: If $s = r = 1$, *Bérczes, Evertse, Győry & Pontreau* (*2013*): $h(\alpha), [\mathbb{K}(\alpha):\mathbb{K}] \ll_{f,\mathbb{K},\Gamma} 1 \Longrightarrow$ We get an explicit bound for $\deg H_{\omega_1,\omega_2}$.

Maurin (*2008*)

$$\Downarrow$$

There are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \mathcal{D}_{\mathbf{n},\mathbf{m}} = \gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right).$$

$$+$$

Controlling multiplicities via *Mason's* (*1984*) polynomial ABC

$$\Downarrow$$

One can construct the polynomial $H_{\omega_1,\omega_2} \in \overline{\mathbb{Q}}[X]$ such that

$$\gcd\left(f_1^{n_1} \cdots f_s^{n_s} - \omega_1, g_1^{m_1} \cdots g_r^{m_r} - \omega_2\right) \mid H_{\omega_1,\omega_2}.$$

Remark: If $s = r = 1$, *Bérczes, Evertse, Győry & Pontreau* (*2013*):
$h(\alpha), [\mathbb{K}(\alpha) : \mathbb{K}] \ll_{f,\mathbb{K},\Gamma} 1 \Longrightarrow$ We get an explicit bound for $\deg H_{\omega_1,\omega_2}$.

Levin & Wang (*2019*): Let $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$ be nonconstant and coprime, such that not both vanish at $\mathbf{0} \in \mathbb{C}^\ell$. Let $g_1, \ldots, g_\ell \in \mathbb{C}[X]$ be mult. indep. with constants. For any $\varepsilon > 0$, one has

$$\deg \gcd \left(F(g_1^k, \ldots, g_\ell^k), G(g_1^k, \ldots, g_\ell^k) \right) < \varepsilon k$$

provided that k is large enough.

Remarks:

- If $F = h_1(X_1 \cdots X_r)$ and $G = h_2(X_{r+1} \cdots X_\ell)$, then *A.O. & Shparlinski* (*2020*) give a uniform bound independent of k.
- The results of *Levin & Wang* (*2019*) are more general, applying to meromorphic functions $g_1, \ldots, g_\ell$, and they are based on Nevanlinna theory: $\gcd =$ common zeros.
- If $F = \sum_{i=1}^{\ell} a_i X_i$ and $G = \sum_{i=1}^{\ell} b_i Y_i$, then $F(g_1^k, \ldots, g_\ell^k)$ is a linear recurrence sequence (LRS), and similarly G, which brings us to . . .

Levin & Wang (*2019*): Let $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$ be nonconstant and coprime, such that not both vanish at $\mathbf{0} \in \mathbb{C}^\ell$. Let $g_1, \ldots, g_\ell \in \mathbb{C}[X]$ be mult. indep. with constants. For any $\varepsilon > 0$, one has

$$\deg \gcd \left(F(g_1^k, \ldots, g_\ell^k), G(g_1^k, \ldots, g_\ell^k) \right) < \varepsilon k$$

provided that k is large enough.

Remarks:

- If $F = h_1(X_1 \cdots X_r)$ and $G = h_2(X_{r+1} \cdots X_\ell)$, then *A.O. & Shparlinski* (*2020*) give a uniform bound independent of k.
- The results of *Levin & Wang* (*2019*) are more general, applying to meromorphic functions $g_1, \ldots, g_\ell$, and they are based on Nevanlinna theory: $\gcd =$ common zeros.
- If $F = \sum_{i=1}^{\ell} a_i X_i$ and $G = \sum_{i=1}^{\ell} b_i Y_i$, then $F(g_1^k, \ldots, g_\ell^k)$ is a linear recurrence sequence (LRS), and similarly G, which brings us to ...

Levin & Wang (*2019*): Let $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$ be nonconstant and coprime, such that not both vanish at $\mathbf{0} \in \mathbb{C}^\ell$. Let $g_1, \ldots, g_\ell \in \mathbb{C}[X]$ be mult. indep. with constants. For any $\varepsilon > 0$, one has

$$\deg \gcd \left(F(g_1^k, \ldots, g_\ell^k), G(g_1^k, \ldots, g_\ell^k) \right) < \varepsilon k$$

provided that k is large enough.

Remarks:

- If $F = h_1(X_1 \cdots X_r)$ and $G = h_2(X_{r+1} \cdots X_\ell)$, then *A.O. & Shparlinski* (*2020*) give a uniform bound independent of k.
- The results of *Levin & Wang* (*2019*) are more general, applying to meromorphic functions $g_1, \ldots, g_\ell$, and they are based on Nevanlinna theory: $\gcd =$ common zeros.
- If $F = \sum_{i=1}^{\ell} a_i X_i$ and $G = \sum_{i=1}^{\ell} b_i Y_i$, then $F(g_1^k, \ldots, g_\ell^k)$ is a linear recurrence sequence (LRS), and similarly G, which brings us to ...

Levin & Wang (*2019*): Let $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$ be nonconstant and coprime, such that not both vanish at $\mathbf{0} \in \mathbb{C}^\ell$. Let $g_1, \ldots, g_\ell \in \mathbb{C}[X]$ be mult. indep. with constants. For any $\varepsilon > 0$, one has

$$\deg \gcd \left(F(g_1^k, \ldots, g_\ell^k), G(g_1^k, \ldots, g_\ell^k) \right) < \varepsilon k$$

provided that k is large enough.

Remarks:

- If $F = h_1(X_1 \cdots X_r)$ and $G = h_2(X_{r+1} \cdots X_\ell)$, then *A.O. & Shparlinski* (*2020*) give a uniform bound independent of k.
- The results of *Levin & Wang* (*2019*) are more general, applying to meromorphic functions $g_1, \ldots, g_\ell$, and they are based on Nevanlinna theory: $\gcd =$ common zeros.
- If $F = \sum_{i=1}^{\ell} a_i X_i$ and $G = \sum_{i=1}^{\ell} b_i Y_i$, then $F(g_1^k, \ldots, g_\ell^k)$ is a linear recurrence sequence (LRS), and similarly G, which brings us to ...

GCD of LRS

Let $(F_n)_{n=1}^{\infty}, (G_n)_{n=1}^{\infty}$ be two simple LRS defined by

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$.

Open Problem

Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \textit{ for some } n, m \geq 1\} < \infty$$

This would show that there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \gcd(F_n(X), G_m(X)) \quad \text{for some } n, m \geq 1.$$

GCD of LRS

Let $(F_n)_{n=1}^{\infty}, (G_n)_{n=1}^{\infty}$ be two simple LRS defined by

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$.

Open Problem

Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \textit{ for some } n, m \geq 1\} < \infty$$

This would show that there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \gcd(F_n(X), G_m(X)) \quad \text{for some } n, m \geq 1.$$

GCD of LRS

Let $(F_n)_{n=1}^{\infty}, (G_n)_{n=1}^{\infty}$ be two simple LRS defined by

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$.

Open Problem

Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \textit{ for some } n, m \geq 1\} < \infty$$

This would show that there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \gcd(F_n(X), G_m(X)) \quad \text{for some } n, m \geq 1.$$

GCD of LRS

Let $(F_n)_{n=1}^{\infty}, (G_n)_{n=1}^{\infty}$ be two simple LRS defined by

$$F_n = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \quad G_n = \sum_{i=1}^{\ell} b_i(X) g_i(X)^n, \quad n \geq 0,$$

where $a_i, b_i, f_i, g_i \in \overline{\mathbb{Q}}[X]$.

Open Problem

Show that, under some natural conditions,

$$\#\{\alpha \in \overline{\mathbb{Q}} : F_n(\alpha) = G_m(\alpha) = 0 \textit{ for some } n, m \geq 1\} < \infty$$

This would show that there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that

$$(X - \alpha) \mid \gcd(F_n(X), G_m(X)) \quad \text{for some } n, m \geq 1.$$

What we really really want .... is to show, under some conditions, that

$$\deg \gcd(F_n(X), G_m(X)) \ll 1 \quad \text{for all } n, m \geq 1,$$

which would be a uniform function field analogue of the results on gcd's of LRS over number fields.

If $k = 2$ this follows immediately from *Bombieri, Masser & Zannier* (*1999*) and our previous discussion.

If $k > 2$: no results.

What we really really want .... is to show, under some conditions, that

$$\deg \gcd(F_n(X), G_m(X)) \ll 1 \quad \text{for all } n, m \geq 1,$$

which would be a uniform function field analogue of the results on gcd's of LRS over number fields.

If $k = 2$ this follows immediately from *Bombieri, Masser & Zannier* (*1999*) and our previous discussion.

If $k > 2$: no results.

What we really really want .... is to show, under some conditions, that

$$\deg \gcd(F_n(X), G_m(X)) \ll 1 \quad \text{for all } n, m \geq 1,$$

which would be a uniform function field analogue of the results on gcd's of LRS over number fields.

If $k = 2$ this follows immediately from *Bombieri, Masser & Zannier* (*1999*) and our previous discussion.

If $k > 2$: no results.

Skolem Problem

A motivation for the above result comes also from:

Skolem Problem

Given an LRS $\{u_n\}$, $n \geq 0$, defined over $\mathbb{C}$, decide if there is $n \geq 1$ such that $u_n = 0$.

Let us define

$$\mathcal{S}(\{u_n\}) = \{n \in \mathbb{N} : u_n = 0\}.$$

Skolem-Mahler-Lech

The set $\mathcal{S}(\{u_n\})$ is the union of finitely many arithmetic progressions and a finite set. If $\{u_n\}$ is non-degenerate, then $S(\{u_n\})$ is finite.

($\{u_n\}$ is non-degenerate if the ratio of any two distinct roots of the characteristic polynomial is not a root of unity.)

Skolem Problem

A motivation for the above result comes also from:

Skolem Problem

Given an LRS $\{u_n\}$, $n \geq 0$, defined over $\mathbb{C}$, decide if there is $n \geq 1$ such that $u_n = 0$.

Let us define

$$\mathcal{S}(\{u_n\}) = \{n \in \mathbb{N} : u_n = 0\}.$$

Skolem-Mahler-Lech

The set $\mathcal{S}(\{u_n\})$ is the union of finitely many arithmetic progressions and a finite set. If $\{u_n\}$ is non-degenerate, then $S(\{u_n\})$ is finite.

($\{u_n\}$ is non-degenerate if the ratio of any two distinct roots of the characteristic polynomial is not a root of unity.)

Skolem Problem

A motivation for the above result comes also from:

Skolem Problem

Given an LRS $\{u_n\}$, $n \geq 0$, defined over $\mathbb{C}$, decide if there is $n \geq 1$ such that $u_n = 0$.

Let us define

$$\mathcal{S}(\{u_n\}) = \{n \in \mathbb{N} : u_n = 0\}.$$

Skolem-Mahler-Lech

The set $\mathcal{S}(\{u_n\})$ is the union of finitely many arithmetic progressions and a finite set. If $\{u_n\}$ is non-degenerate, then $S(\{u_n\})$ is finite.

($\{u_n\}$ is non-degenerate if the ratio of any two distinct roots of the characteristic polynomial is not a root of unity.)

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

There are many results giving bounds for the number of arith. progressions or for $\#\mathcal{S}(u_n)$ (when finite), including:

van der Poorten & Schlickewei (*1990*), *Schmidt* (*1999, 2000*), *Evertse, Schlickewei & Schmidt* (*2002*)

Amoroso & Viada (*2009*): significantly (by an exponential) improved the previously known bounds.

Remark: All these bounds depend only on the order of $\{u_n\}$.

There are also non-uniform bounds that depend on the characteristic roots of the non-degenerate LRS, e.g. *van der Poorten & Schlickewei* (*1991*).

The Skolem Problem has been settled in the following cases:

Mignotte, Shorey & Tijdeman (*1984*), *Vereshchagin* (*1985*), *Chonev, Ouaknine & Worrell* (*2016*): LRS of orders 2, 3 and 4

Sha (*2019*): for simple LRS, of any order, with at most two dominant roots, gave explicit lower bound for N such that $u_n \neq 0$ for all $n > N$.

Universal Skolem Sets

Instead of imposing restrictions on the LRS (eg, order, dominance of roots, etc), one can restrict the domain of search to so-caled:

Definition (Universal Skolem Set)

An infinite set $\mathcal{T} \subseteq \mathbb{N}$ is a Universal Skolem Set if there is an effective procedure that given an LRS, decides if it has a zero $n \in \mathcal{T}$.

Luca, Ouaknine & Worrell (2022):

- Let
$$s_0 = 1, \qquad s_n = n! + s_{\lfloor \sqrt{\log n} \rfloor}, \quad n > 0.$$
Then the set $\mathcal{T} = \{s_n : n \in \mathbb{N}\}$ is a Universal Skolem Set. However, this is a sparse set of density zero.
- More involved construction of a Universal Skolem Set which is of positive lower density, and conditionally on some assumptions on the distributions of primes, they prove this set if of density 1.

Universal Skolem Sets

Instead of imposing restrictions on the LRS (eg, order, dominance of roots, etc), one can restrict the domain of search to so-caled:

Definition (Universal Skolem Set)

An infinite set $\mathcal{T} \subseteq \mathbb{N}$ is a Universal Skolem Set if there is an effective procedure that given an LRS, decides if it has a zero $n \in \mathcal{T}$.

Luca, Ouaknine & Worrell (*2022*):

- Let
$$s_0 = 1, \qquad s_n = n! + s_{\lfloor \sqrt{\log n} \rfloor}, \quad n > 0.$$
Then the set $\mathcal{T} = \{s_n : n \in \mathbb{N}\}$ is a Universal Skolem Set. However, this is a sparse set of density zero.
- More involved construction of a Universal Skolem Set which is of positive lower density, and conditionally on some assumptions on the distributions of primes, they prove this set if of density 1.

Universal Skolem Sets

Instead of imposing restrictions on the LRS (eg, order, dominance of roots, etc), one can restrict the domain of search to so-caled:

Definition (Universal Skolem Set)

An infinite set $\mathcal{T} \subseteq \mathbb{N}$ is a Universal Skolem Set if there is an effective procedure that given an LRS, decides if it has a zero $n \in \mathcal{T}$.

Luca, Ouaknine & Worrell (*2022*):

- Let
$$s_0 = 1, \qquad s_n = n! + s_{\lfloor \sqrt{\log n} \rfloor}, \quad n > 0.$$
Then the set $\mathcal{T} = \{s_n : n \in \mathbb{N}\}$ is a Universal Skolem Set. However, this is a sparse set of density zero.
- More involved construction of a Universal Skolem Set which is of positive lower density, and conditionally on some assumptions on the distributions of primes, they prove this set if of density 1.

Skolem Problem for specialisations of LRS

Let

$$\mathbf{a} = (a_1, \dots, a_k), \mathbf{f} = (f_1, \dots, f_k) \in \overline{\mathbb{Q}}(X)^k,$$

and consider the linear recurrence sequences as above

$$F_n(X) = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \qquad n \geq 0.$$

We give a bound for the largest zero in (all but a set of bounded height of) specialisations of $F_n(X)$, $n \geq 1$.

$$\Downarrow$$

Skolem Problem is effectively decidable for specialisations as above.

Remark: The Skolem Problem is settled over functions fields by *Fuchs & Pethö* (*2005*).

Skolem Problem for specialisations of LRS

Let

$$\mathbf{a} = (a_1, \ldots, a_k), \mathbf{f} = (f_1, \ldots, f_k) \in \overline{\mathbb{Q}}(X)^k,$$

and consider the linear recurrence sequences as above

$$F_n(X) = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \qquad n \geq 0.$$

We give a bound for the largest zero in (all but a set of bounded height of) specialisations of $F_n(X)$, $n \geq 1$.

$$\Downarrow$$

Skolem Problem is effectively decidable for specialisations as above.

Remark: The Skolem Problem is settled over functions fields by *Fuchs & Pethö* (*2005*).

Skolem Problem for specialisations of LRS

Let

$$\mathbf{a} = (a_1, \dots, a_k), \mathbf{f} = (f_1, \dots, f_k) \in \overline{\mathbb{Q}}(X)^k,$$

and consider the linear recurrence sequences as above

$$F_n(X) = \sum_{i=1}^{k} a_i(X) f_i(X)^n, \qquad n \geq 0.$$

We give a bound for the largest zero in (all but a set of bounded height of) specialisations of $F_n(X)$, $n \geq 1$.

$$\Downarrow$$

Skolem Problem is effectively decidable for specialisations as above.

Remark: The Skolem Problem is settled over functions fields by *Fuchs & Pethö* (*2005*).

Bound on the zeros

We define the set

$$\mathcal{E}_{\mathbf{a},\mathbf{f}} = \{\alpha \in \overline{\mathbb{Q}} : \ f_i(\alpha)/f_j(\alpha) \text{ is a root of unity for some } 1 \le i < j \le k \\ \text{ or } a_i(\alpha) = 0 \text{ or } f_i(\alpha) = 0 \text{ for some } 1 \le i \le k\}.$$

A.O. & Shparlinski (2020)

Let $a_i, f_i \in \overline{\mathbb{Q}}(Z)$, $i = 1, \ldots, k$, be nonzero of degree at most d such that f_i/f_j is non-constant for any $1 \le i < j \le k$. Assume that for any $1 \le r < s < t \le k$, the pairs $(f_s/f_r, f_t/f_r)$ are "non-exceptional". For all but at most d^2k^3 elements $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ any zero $n \in \mathbb{N}$ of the equation

$$F_n(\alpha) = 0$$

satisfies

$$n \le \exp\left(CD_\alpha^4\right),$$

where $D_\alpha =$ degree of the smallest Galois field $\mathbb{K}$ with $\alpha \in \mathbb{K}$ and $C = C(a_i, f_i)$.

Application

A.O. & Shparlinski (2020)

Let $a_i, f_i \in \overline{\mathbb{Q}}[X]$, $i = 1, \ldots, k$, *be as above and such that* $\gcd(a_1 f_1, \ldots, a_k f_k) = 1$. *Then the splitting field* $\mathbb{L}_n$ *of the polynomial*

$$F_n(X) = \sum_{i=1}^{k} a_i f_i^n$$

is of degree

$$[\mathbb{L}_n : \mathbb{Q}] \geq c_0 (\log n)^{1/4},$$

where c_0 *is an effective constant depending only on* $a_1, f_1, \ldots, a_k, f_k$.

Remark: Apart form a finite set of polynomials, the degrees of the irreducible factors over $\mathbb{Q}$ of F_n tends to ∞.

This is an explicit version of

$$[\mathbb{L}_n : \mathbb{Q}] \to \infty, \qquad \text{as } n \to \infty,$$

given by *Amoroso, Masser & Zannier* (*2017*).

Application

A.O. & Shparlinski (2020)

Let $a_i, f_i \in \overline{\mathbb{Q}}[X]$, $i = 1, \ldots, k$, *be as above and such that* $\gcd(a_1 f_1, \ldots, a_k f_k) = 1$. *Then the splitting field* $\mathbb{L}_n$ *of the polynomial*

$$F_n(X) = \sum_{i=1}^{k} a_i f_i^n$$

is of degree

$$[\mathbb{L}_n : \mathbb{Q}] \geq c_0 (\log n)^{1/4},$$

where c_0 *is an effective constant depending only on* $a_1, f_1, \ldots, a_k, f_k$.

Remark: Apart form a finite set of polynomials, the degrees of the irreducible factors over $\mathbb{Q}$ of F_n tends to ∞.

This is an explicit version of

$$[\mathbb{L}_n : \mathbb{Q}] \to \infty, \qquad \text{as } n \to \infty,$$

given by *Amoroso, Masser & Zannier* (*2017*).

Main tools

Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ such that $F_n(\alpha) = \sum_{i=1}^k a_i(\alpha) f_i(\alpha)^n = 0$.

- The characteristic roots $f_i(\alpha)$ with

$$|f_i(\alpha)| = \max\{|f_1(\alpha)|, \ldots, |f_k(\alpha)|\}$$

  are called dominant roots.
- If one has only one dominant root, it is easy to bound n as above.
- If one has only two dominant roots: we use *Sha* (*2019*) $\Longrightarrow$ $n \le \exp\left(CD_\alpha^4(h(\alpha)+1)\right)$.
- *Amoroso, Masser & Zannier* (*2017*): the set of $\alpha \in \overline{\mathbb{Q}}$ as above is a set of bounded Weil height $\Longrightarrow n \le \exp\left(CD_\alpha^4\right)$.

Main tools

Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ such that $F_n(\alpha) = \sum_{i=1}^k a_i(\alpha) f_i(\alpha)^n = 0$.

- The characteristic roots $f_i(\alpha)$ with

$$|f_i(\alpha)| = \max\{|f_1(\alpha)|, \ldots, |f_k(\alpha)|\}$$

  are called dominant roots.
- If one has only one dominant root, it is easy to bound n as above.
- If one has only two dominant roots: we use *Sha* (*2019*) $\Longrightarrow$ $n \le \exp\left(CD_\alpha^4 (h(\alpha)+1)\right)$.
- *Amoroso, Masser & Zannier* (*2017*): the set of $\alpha \in \overline{\mathbb{Q}}$ as above is a set of bounded Weil height $\Longrightarrow n \le \exp\left(CD_\alpha^4\right)$.

Main tools

Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ such that $F_n(\alpha) = \sum_{i=1}^{k} a_i(\alpha) f_i(\alpha)^n = 0$.

- The characteristic roots $f_i(\alpha)$ with

$$|f_i(\alpha)| = \max\{|f_1(\alpha)|, \ldots, |f_k(\alpha)|\}$$

  are called dominant roots.
- If one has only one dominant root, it is easy to bound n as above.
- If one has only two dominant roots: we use *Sha* (*2019*) $\Longrightarrow$ $n \le \exp\left(CD_\alpha^4(h(\alpha)+1)\right)$.
- *Amoroso, Masser & Zannier* (*2017*): the set of $\alpha \in \overline{\mathbb{Q}}$ as above is a set of bounded Weil height $\Longrightarrow n \le \exp\left(CD_\alpha^4\right)$.

Main tools

Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ such that $F_n(\alpha) = \sum_{i=1}^{k} a_i(\alpha) f_i(\alpha)^n = 0$.

- The characteristic roots $f_i(\alpha)$ with

$$|f_i(\alpha)| = \max\{|f_1(\alpha)|, \dots, |f_k(\alpha)|\}$$

  are called dominant roots.
- If one has only one dominant root, it is easy to bound n as above.
- If one has only two dominant roots: we use *Sha* (*2019*) $\Longrightarrow$ $n \le \exp\left(CD_\alpha^4(h(\alpha)+1)\right)$.
- *Amoroso, Masser & Zannier* (*2017*): the set of $\alpha \in \overline{\mathbb{Q}}$ as above is a set of bounded Weil height $\Longrightarrow n \le \exp\left(CD_\alpha^4\right)$.

Main tools

Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{E}_{\mathbf{a},\mathbf{f}}$ such that $F_n(\alpha) = \sum_{i=1}^{k} a_i(\alpha) f_i(\alpha)^n = 0$.

- The characteristic roots $f_i(\alpha)$ with

$$|f_i(\alpha)| = \max\{|f_1(\alpha)|, \ldots, |f_k(\alpha)|\}$$

  are called dominant roots.
- If one has only one dominant root, it is easy to bound n as above.
- If one has only two dominant roots: we use *Sha* (*2019*) $\Longrightarrow$ $n \leq \exp\left(CD_\alpha^4(h(\alpha)+1)\right)$.
- *Amoroso, Masser & Zannier* (*2017*): the set of $\alpha \in \overline{\mathbb{Q}}$ as above is a set of bounded Weil height $\Longrightarrow n \leq \exp\left(CD_\alpha^4\right)$.

At least three dominant roots

This means: $|f_r(\alpha)| = |f_s(\alpha)| = |f_t(\alpha)|$ for some $1 \le r < s < t \le k$, or equivalently,

$$\frac{|f_s(\alpha)|}{|f_r(\alpha)|} = \frac{|f_t(\alpha)|}{|f_r(\alpha)|} = 1.$$

$$\Uparrow$$

Unimodular points on plane curves

Pakovich & Shparlinski (2020)

Let $(f_1(X), f_2(X)) \in \mathbb{C}(X)$ be of degrees n_1 and n_2, respectively. Then

$$\#\{\alpha \in \mathbb{C} : \ |f_1(\alpha)| = |f_2(\alpha)| = 1\} \le (\deg f_1 + \deg f_2)^2,$$

unless $(f_1(X), f_2(X))$ is "exceptional".

At least three dominant roots

This means: $|f_r(\alpha)| = |f_s(\alpha)| = |f_t(\alpha)|$ for some $1 \le r < s < t \le k$, or equivalently,

$$\frac{|f_s(\alpha)|}{|f_r(\alpha)|} = \frac{|f_t(\alpha)|}{|f_r(\alpha)|} = 1.$$

$$\Uparrow$$

Unimodular points on plane curves

Pakovich & Shparlinski (2020)

Let $(f_1(X), f_2(X)) \in \mathbb{C}(X)$ *be of degrees* n_1 *and* n_2*, respectively. Then*

$$\#\{\alpha \in \mathbb{C} : \ |f_1(\alpha)| = |f_2(\alpha)| = 1\} \le (\deg f_1 + \deg f_2)^2,$$

unless $(f_1(X), f_2(X))$ *is "exceptional".*

At least three dominant roots

This means: $|f_r(\alpha)| = |f_s(\alpha)| = |f_t(\alpha)|$ for some $1 \le r < s < t \le k$, or equivalently,

$$\frac{|f_s(\alpha)|}{|f_r(\alpha)|} = \frac{|f_t(\alpha)|}{|f_r(\alpha)|} = 1.$$

$$\Uparrow$$

Unimodular points on plane curves

Pakovich & Shparlinski (2020)

Let $(f_1(X), f_2(X)) \in \mathbb{C}(X)$ *be of degrees* n_1 *and* n_2*, respectively. Then*

$$\#\{\alpha \in \mathbb{C} : \ |f_1(\alpha)| = |f_2(\alpha)| = 1\} \le (\deg f_1 + \deg f_2)^2,$$

unless $(f_1(X), f_2(X))$ *is "exceptional".*

Questions

- Uniform bound: We would like to obtain a bound which is independent of α, when α is restricted to special subsets of $\overline{\mathbb{Q}}$, such as the set of all roots of unity. This in particular would imply that the set

$$\{\alpha \in \overline{\mathbb{Q}} : \ \alpha^n = 1, \ F_m(\alpha) = 0 \text{ for some } n, m \geq 1\},$$

is finite.

$$\Downarrow$$

$$\deg \gcd\left(X^n - 1, F_m(X)\right) \ll 1 \qquad \text{for all } n, m \geq 1.$$

More generally, one can ask about the finiteness of the set

$$\{\alpha \in \mathbb{K}^c : F_n(\alpha) = 0 \text{ for some } n \geq 1\},$$

where $\mathbb{K}^c$ is the cyclotomic closure of $\mathbb{K}$ (one achieves this in the multiplicative case – *O., Sha, Shparlinski & Zannier* (*2019*)).

- Generalisation to S-unit equations: Let Γ be a finitely generated subgroup of $\overline{\mathbb{Q}}(X)$ and fix $a_1, \ldots, a_k \in \overline{\mathbb{Q}}(X)$.

  Amoroso, Masser & Zannier (*2017*): for any $u_1, \ldots, u_k \in \Gamma$ such that

  $$u_i/u_j \notin \overline{\mathbb{Q}}, \quad 1 \le i < j \le k, \qquad \text{and} \qquad \sum_{i=1}^{k} a_i u_i \ne 0,$$

  the set

  $$\mathcal{S}(a_1, \ldots, a_k; \Gamma) = \left\{ \alpha \in \overline{\mathbb{Q}} : \sum_{i=1}^{k} a_i(\alpha) u_i(\alpha) = 0 \right\}$$

  is of bounded height (depending only on $a_1, \ldots, a_k$ and Γ).

  A solution $\alpha \in \mathcal{S}(a_1, \ldots, a_k; \Gamma)$ is called *primitive* if $u_i(\alpha) = 1$ for some $i = 1, \ldots, k$.

  Is it true, under some natural conditions on Γ, that outside of a set of $\alpha \in \overline{\mathbb{Q}}$ of bounded height for every primitive $\alpha \in \mathcal{S}(a_1, \ldots, a_k; \Gamma)$, $\max_{i=1,\ldots,k} \deg u_i(\alpha)$ is bounded only in terms of the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, the coefficients $a_1, \ldots, a_k$ and the generators of Γ?