TECHNISCHE
UNIVERSITÄT
WIEN

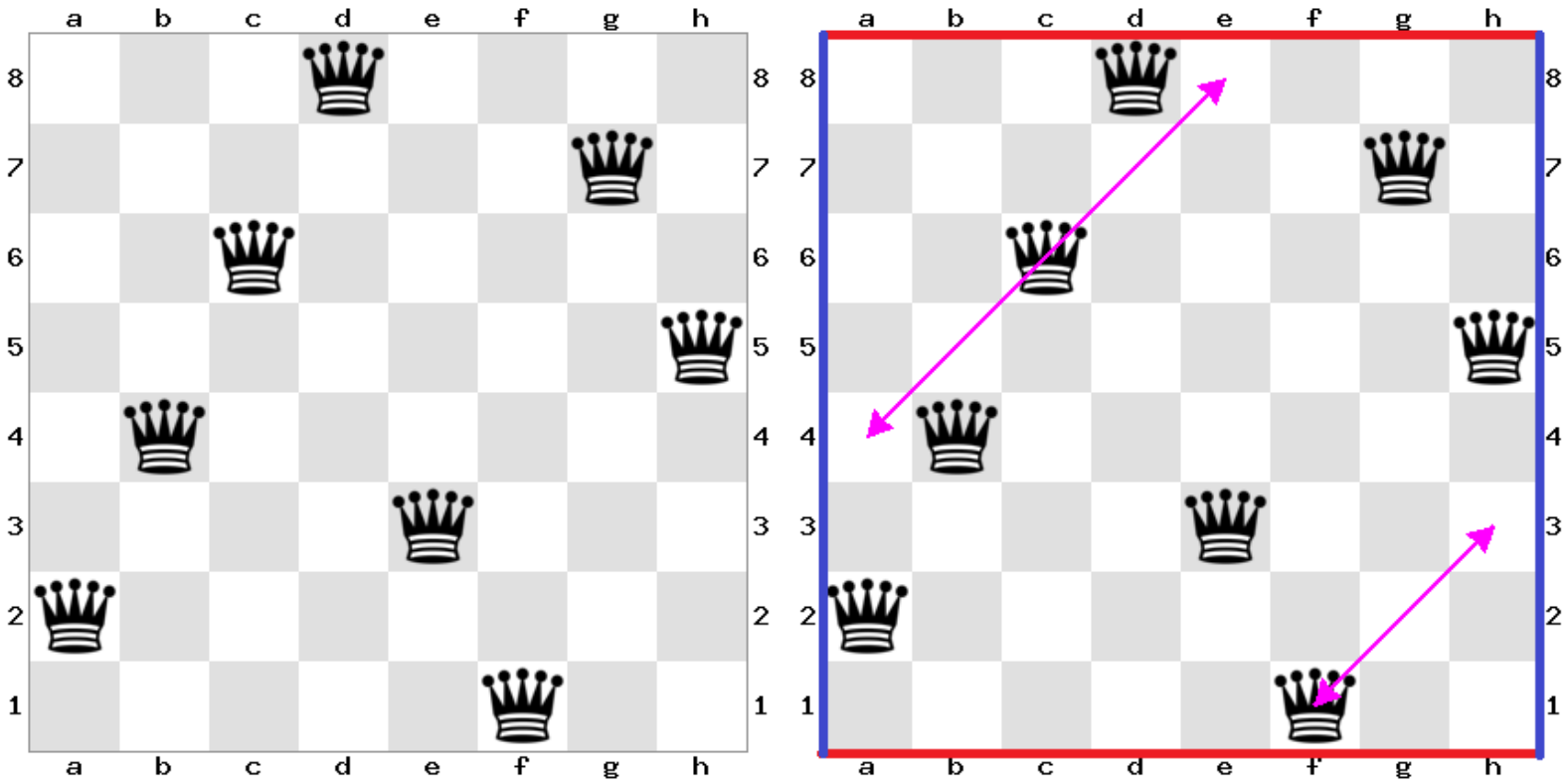
On the Skolem Problem for Reversible Sequences

George Kenison
Institute of Logic and Computation

Partially Supported by:

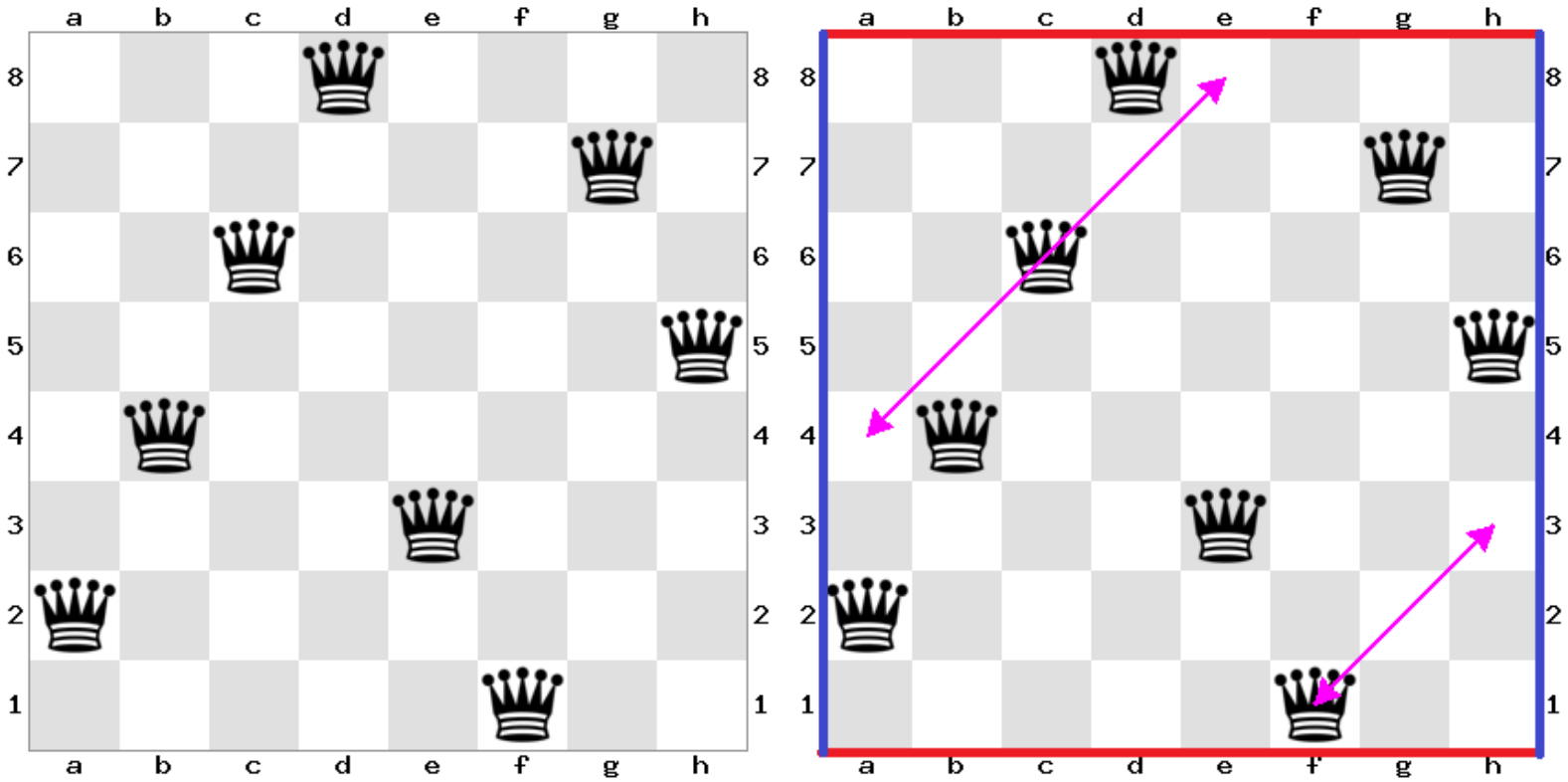
WWTF Grant ProbInG (ICT19-018) and ERC Consolidator Grant ARTIST (101002685)

Attacking Queens



LHS: An arrangement of 8 non-attacking queens on an 8×8 board.

Attacking Queens



RHS: The same arrangement of 8 queens on an 8×8 toroidal board. The queens are now attacking each other.

Queens and Bicycles

Consider the following sets of natural numbers: the set of $n \in \mathbb{N}$ such that

1. n non-attacking queens can be placed on an $n \times n$ toroidal board. (The queen numbers[1].)
2. there exists an irreducible polynomial in $\mathbb{Z}[X]$ of degree n whose roots lie on precisely two concentric circles centred at the origin. (The bicycle numbers.)

Describe the set of natural numbers n given by the union of the queen and bicycle numbers.

[1] Pólya gave a solution in *Uber die doppelt-periodischen Lösungen des n-Damen-Problems* (1918)

Does this loop terminate?

Given: $A \in \mathbb{Z}^{d \times d}$ and $b, x_0 \in \mathbb{Z}^d$

$x \leftarrow x_0$

while $b^\top x \neq 0$ **do**

    $x \leftarrow Ax$

end while

Does this loop terminate?

Given: $A \in \mathbb{Z}^{d \times d}$ and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Example

Let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $b, x_0 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ then

$$\text{Update:} \quad \langle A^n x_0 \rangle_n = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 \\ 2 \end{smallmatrix}\right), \ldots \rangle$$

$$\text{Guard:} \quad \langle b^\top A^n x_0 \rangle_n = \langle 1, 1, 2, 3, \ldots \rangle$$

Decidability

Given: $A \in \mathbb{Z}^{d \times d}$
and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Given: unimodular $A \in \mathbb{Z}^{d \times d}$
and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Skolem Problem

Termination decidable if $d \leq 4$.

Decidability is open for $d \geq 5$.

Mignotte, Shorey, and Tijdeman, 1984; Vereshchagin, 1985

Reversible Skolem Problem

Termination is decidable if $d \leq 7$.

Decidability is open for $d \geq 8$.

Lipton et al. (LICS '22)

$A \in \mathbb{Z}^{d \times d}$ is unimodular if $\det(A) = \pm 1$.

Decidability

Given: $A \in \mathbb{Z}^{d \times d}$
and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Given: unimodular $A \in \mathbb{Z}^{d \times d}$
and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Skolem Problem

Termination decidable if $d \leq 4$.

Decidability is open for $d \geq 5$.

Mignotte, Shorey, and Tijdeman, 1984; Vereshchagin, 1985

Reversible Skolem Problem

Termination is decidable if $d \leq 7$.

Decidability is open for $d \geq 8$.

Lipton et al. (LICS '22)

New Proof by K. (MFCS '22)

$A \in \mathbb{Z}^{d \times d}$ is unimodular if $\det(A) = \pm 1$.

Does this loop terminate?

Given: $A \in \mathbb{Z}^{d \times d}$ and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Equivalently,

For $\langle u_n \rangle_n = \langle b^\top x_0, b^\top A x_0, b^\top A^2 x_0, \ldots \rangle$,
does $\langle u_n \rangle_n$ vanish at some n?

Does this loop terminate?

Given: $A \in \mathbb{Z}^{d \times d}$ and $b, x_0 \in \mathbb{Z}^d$
$x \leftarrow x_0$
while $b^\top x \neq 0$ **do**
    $x \leftarrow Ax$
end while

Equivalently,

For $\langle u_n \rangle_n = \langle b^\top x_0, b^\top A x_0, b^\top A^2 x_0, \ldots \rangle$,
does $\langle u_n \rangle_n$ vanish at some n?

What class of sequences describes $\langle u_n \rangle_n$?

Integer Linear Recurrence Sequences (LRS)

$\langle u_n \rangle_n = \langle b^\top x_0, b^\top A x_0, b^\top A^2 x_0, \ldots \rangle$ is an LRS[2].

For each $n \in \mathbb{N}_0$,

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_1 u_{n+1} + a_0 u_n$$

with $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ and $a_0 \neq 0$.
Initial values $u_0, u_1, \ldots, u_{d-1} \in \mathbb{Z}$.

[2] by the Cayley–Hamilton Theorem

Integer Linear Recurrence Sequences (LRS)

$\langle u_n \rangle_n = \langle b^\top x_0, b^\top A x_0, b^\top A^2 x_0, \ldots \rangle$ is an LRS[2].

For each $n \in \mathbb{N}_0$,

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_1 u_{n+1} + a_0 u_n$$

with $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ and $a_0 \neq 0$.
Initial values $u_0, u_1, \ldots, u_{d-1} \in \mathbb{Z}$.

When do LRSs vanish?

[2] by the Cayley–Hamilton Theorem

Vanishing Set

Examples

- The vanishing set of $\langle 0, 1, 1, 2, \ldots \rangle$ is finite.
- The vanishing set of $\langle 0, 1, 0, 1, \ldots \rangle$ is infinite.

Vanishing Set

Examples

- The vanishing set of $\langle 0, 1, 1, 2, \ldots \rangle$ is finite.
- The vanishing set of $\langle 0, 1, 0, 1, \ldots \rangle$ is infinite.

Skolem–Mahler–Lech Theorem

For an LRS $\langle u_n \rangle_n$, the set $\{n \in \mathbb{N}_0 : u_n = 0\}$ is given by the union of a finite (possibly empty) set and a finite (possibly zero) number of arithmetic progressions.

Vanishing Set

Examples

- The vanishing set of $\langle 0, 1, 1, 2, \ldots \rangle$ is finite.
- The vanishing set of $\langle 0, 1, 0, 1, \ldots \rangle$ is infinite.

Skolem–Mahler–Lech Theorem

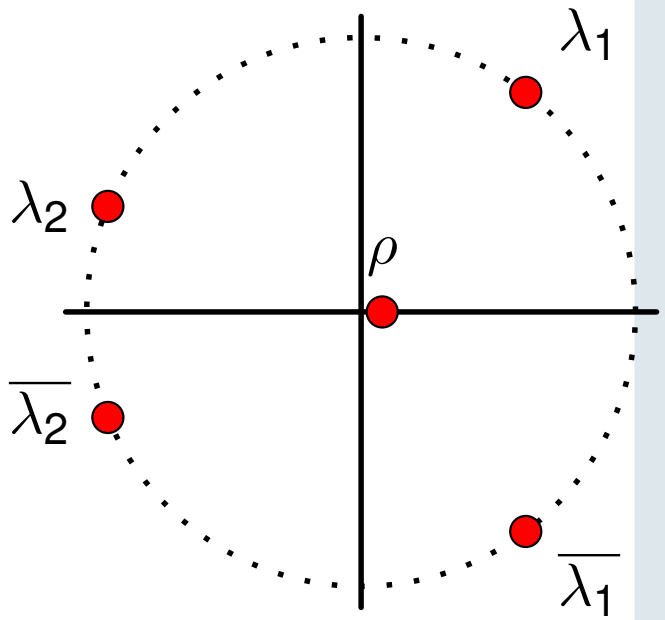
For an LRS $\langle u_n \rangle_n$, the set $\{n \in \mathbb{N}_0 : u_n = 0\}$ is given by the union of a finite (possibly empty) set and a finite (possibly zero) number of arithmetic progressions.

When is $\{n \in \mathbb{N}_0 : u_n = 0\}$ non-empty? (Skolem Problem)

State of the art (Skolem Problem)

When is $\{n \in \mathbb{N}_0 : u_n = 0\}$ non-empty?
Let f be the char poly of the LRS $\langle u_n \rangle_n$.
Decidability of Skolem is not known when both:
(H1) f has at least four dominant roots, and
(H2) roots of f lead to non-deg $\langle u_n \rangle_n$.

Decidability is not known for LRS
$u_n = c_1\lambda_1^n + \overline{c_1\lambda_1}^n + c_2\lambda_2^n + \overline{c_2\lambda_2}^n + \rho^n$.



Reversible LRS

An LRS with

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_1 u_{n+1} \pm u_n$$

is reversible.

Reversible LRS

An LRS with

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_1 u_{n+1} \pm u_n$$

is reversible.

TFAE:

1. $\langle u_n \rangle_{n=0}^{\infty}$ is reversible.
2. Update matrix A is unimodular so that $\det(A) = \pm 1$.[3]
3. char poly $f(x) := \det(xI - A) \in \mathbb{Z}[x]$ has $f(0) = \pm 1$.
4. The extension $\langle u_n \rangle_{n=-\infty}^{\infty}$ is $\mathbb{Z}$-valued.

[3] A induces a linear toral automorphism $T_A \colon \mathbb{R}^d/\mathbb{Z}^d \to \mathbb{R}^d/\mathbb{Z}^d$.

Reversible LRS

An LRS with

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_1 u_{n+1} \pm u_n$$

is reversible.

Examples and a Non-Example

$\langle \ldots, 2, -1, 1, 0, 1, 1, 2, 3, \ldots \rangle$	$u_{n+2} = u_{n+1} + u_n$
$\langle \ldots, 0, 1, 0, 1, 0, 1, 0, 1, 0, \ldots \rangle$	$u_{n+2} = u_n$
$\langle \ldots, 1/8, 1/4, 1/2, 1, 2, 4, 8, \ldots \rangle$	$u_{n+1} = 2u_n$

Reversible Skolem

Theorem (Lipton et al., 2022)

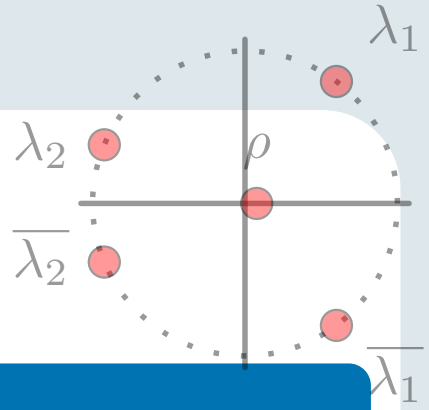
Reversible Skolem is decidable up to order 7.

(H1) f has at least four dominant roots.

(H2) roots of f lead to non-deg $\langle u_n \rangle_n$.

Note: Instances where either hypothesis fails are decidable.

Alternative Proof (at order 5)



Proof.

Assume there exists $f \in \mathbb{Z}[x]$ a monic quintic with $f(0) = \pm 1$ st both of the hypotheses (H1) and (H2) hold.

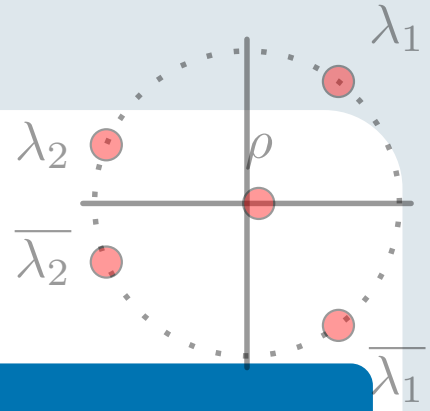
WTS: there is no monic quintic $f \in \mathbb{Z}[x]$ with $f(0) = \pm 1$ st both of the hypotheses (H1) and (H2) hold.

(H1) f has at least four dominant roots.

(H2) roots of f lead to non-deg $\langle u_n \rangle_n$.

Note: Instances where either hypothesis fails are decidable.

Alternative Proof (at order 5)



Proof.

Assume there exists $f \in \mathbb{Z}[x]$ a monic quintic with $f(0) = \pm 1$ st both of the hypotheses (H1) and (H2) hold.
Then f is irreducible and its roots lie on two concentric circles centred at the origin.

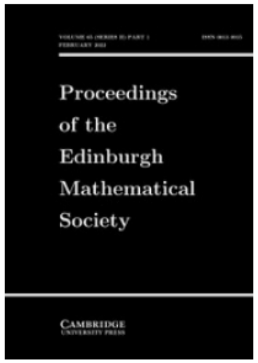
WTS: there is no monic quintic $f \in \mathbb{Z}[x]$ with $f(0) = \pm 1$ st both of the hypotheses (H1) and (H2) hold.

(H1) f has at least four dominant roots.

(H2) roots of f lead to non-deg $\langle u_n \rangle_n$.

Note: Instances where either hypothesis fails are decidable.

(Kronecker, 1857) handles the case where the roots all lie on one circle.



Proceedings of the Edinburgh Mathematical Society

Article contents

Abstract

ON THE REMAK HEIGHT, THE MAHLER MEASURE AND CONJUGATE SETS OF ALGEBRAIC NUMBERS LYING ON TWO CIRCLES

Published online by Cambridge University Press: **20 January 2009**

A. Dubickas and C. J. Smyth

Show author details

Article | Metrics

Save PDF | Share | Cite | Rights & Permissions

Abstract

HTML view is not available for this content. However, as you have access to this content, a full PDF is available via the 'Save PDF' action button.

We define a new height function $\mathcal{R}(\alpha)$, the *Remak height* of an algebraic number α. We give sharp upper and lower bounds for $\mathcal{R}(\alpha)$ in terms of the classical Mahler measure $M(\alpha)$. Study of when one of these bounds is exact leads us

The Mahler measure and Remak height give root separation bounds for irreducible polynomials. Equality between these functions occurs when the roots of an irreducible polynomial lie on two circles. . .

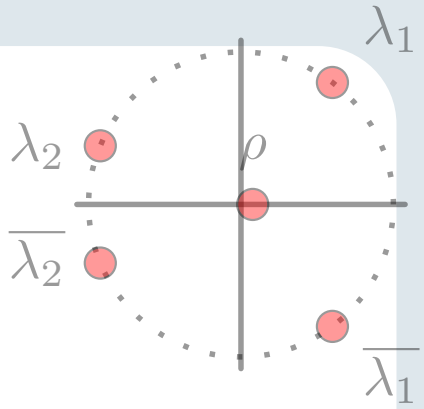
Theorem 2.1. Suppose that a unit-norm α of degree d lies, with all its conjugates on two circles $|z| = r$ and $|z| = R$, but not just on one, with (without loss of generality) at most half of the conjugates on $|z| = r$. Then one of the following holds.

(a) d is a multiple of 3, $R = r^{-1/2}$ with α having $d/3$ conjugates on $|z| = r$ and $2d/3$ conjugates on $|z| = r^{-1/2}$. Assuming (without loss of generality) that $|\alpha| = r$, we have that for some positive integer n, r^n ($= \sigma$ say) is a real, but non-totally real, cubic unit-norm, and $\alpha^n = \rho\sigma$, where ρ is unit-circular.

(b) d is even, $R = r^{-1}$ where $R > 1$ without loss of generality, and $d/2$ conjugates of α lie on each circle. Furthermore, for some positive integer n, R^n ($= \tau$ say) is either an extended Salem number or is reciprocal quadratic, and $\alpha^n = \rho\psi$, where ψ is a Salem half-norm defined by τ, and ρ is unit circular.

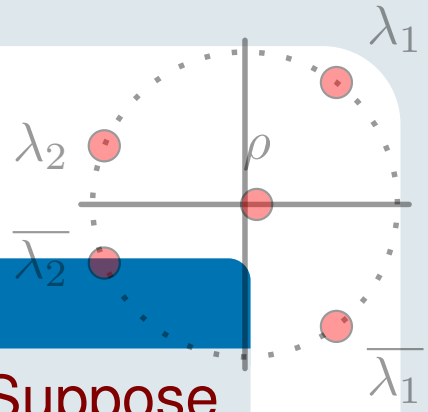
...

coup de grâce



. . . A weaker version of Theorem 2.1:

coup de grâce

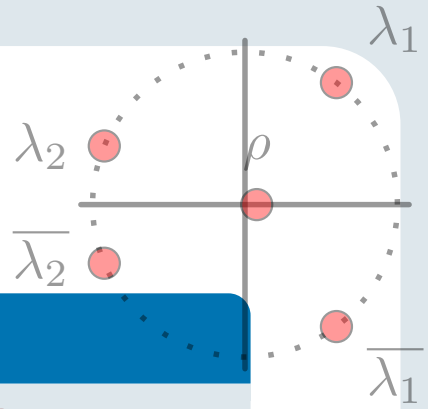


Theorem (Dubickas and Smyth, 2001)

Let $f \in \mathbb{Z}[x]$ be irreducible, monic, and $f(0) = \pm 1$. Suppose that the roots of f lie on two concentric circles centred at the origin. Then $\deg(f)$ is either even, or a multiple of three.

The bicycle numbers are precisely those natural numbers n where $\gcd(n, 6) > 1$.

coup de grâce

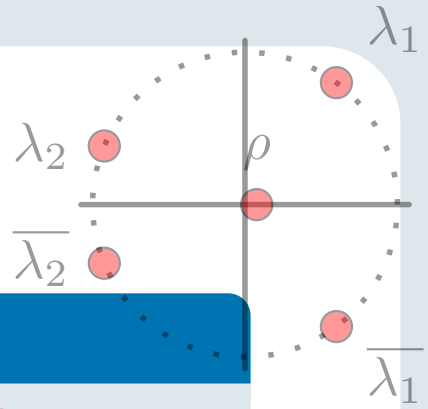


Theorem (Dubickas and Smyth, 2001)

Let $f \in \mathbb{Z}[x]$ be irreducible, monic, and $f(0) = \pm 1$. Suppose that the roots of f lie on two concentric circles centred at the origin. Then $\deg(f)$ is either even, or a multiple of three.

Proof (contradiction continued)

coup de grâce



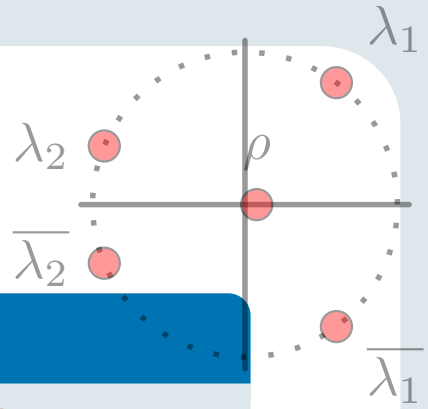
Theorem (Dubickas and Smyth, 2001)

Let $f \in \mathbb{Z}[x]$ be irreducible, monic, and $f(0) = \pm 1$. Suppose that the roots of f lie on two concentric circles centred at the origin. Then $\deg(f)$ is either even, or a multiple of three.

Proof (contradiction continued)

f is a quintic that satisfies the above assumptions.

coup de grâce



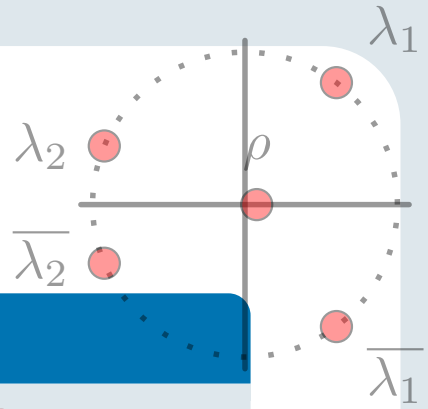
Theorem (Dubickas and Smyth, 2001)

Let $f \in \mathbb{Z}[x]$ be irreducible, monic, and $f(0) = \pm 1$. Suppose that the roots of f lie on two concentric circles centred at the origin. Then $\deg(f)$ is either even, or a multiple of three.

Proof (contradiction continued)

f is a quintic that satisfies the above assumptions.
Thus five is either even, or a multiple of three. ↯ □

coup de grâce



Theorem (Dubickas and Smyth, 2001)

Let $f \in \mathbb{Z}[x]$ be irreducible, monic, and $f(0) = \pm 1$. Suppose that the roots of f lie on two concentric circles centred at the origin. Then $\deg(f)$ is either even, or a multiple of three.

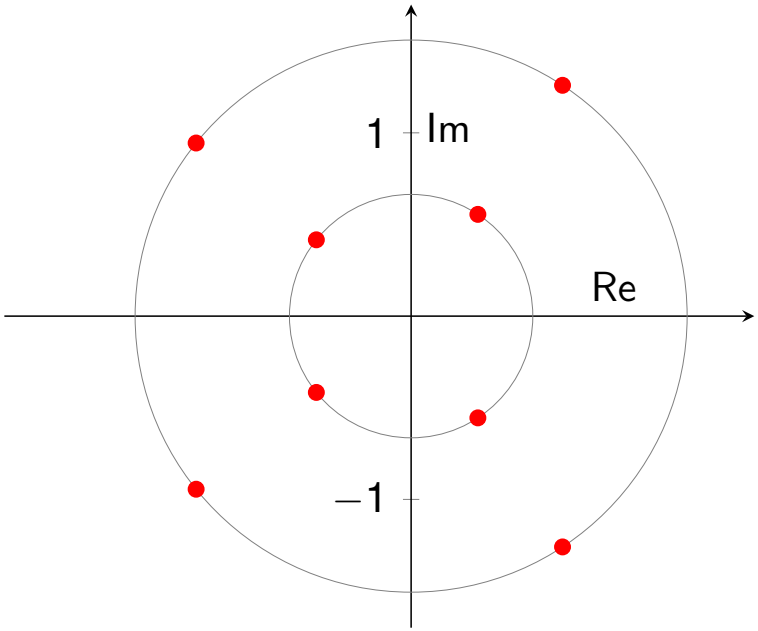
Proof (contradiction continued)

f is a quintic that satisfies the above assumptions.
Thus five is either even, or a multiple of three. ↯ □

So Reversible Skolem is decidable at order 5. (Similar arguments at order 6, 7.)

Reversible Skolem at order 8

Decidability of Reversible Skolem is not known at order 8.[3]



The roots of $x^8 + x^7 + x^6 + 2x^5 + 6x^4 + 2x^3 + x^2 + x + 1$ satisfy (H1) and (H2).

[3] there is an infinite family of LRSs that the state of the art cannot handle.

New Results

The Positivity Problem

For LRS $\langle u_n \rangle_n$, determine whether $u_n \geq 0$ for each $n \in \mathbb{N}_0$.

An LRS is simple if the associated char poly has no repeated roots.

Corollary

Simple Reversible Positivity is decidable up to order 10.

(Ouaknine and Worrell, 2014): simple positivity is decidable up to order 9.

Directions for Future Research

- Apply techniques more widely e.g., Reversible Positivity.
- Extend the state of the art for specialisations such as Palindromic Skolem.

Thank you for listening!

Theorem (Pólya)

n non-attacking queens can be placed on an $n \times n$ toroidal board if and only if $\gcd(n, 6) = 1$

references I

[1] A. Dubickas and C. J. Smyth. “On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles”. In: Proc. Edinb. Math. Soc. (2) 44.1 (2001), pp. 1–17. DOI: 10.1017/S001309159900098X.

[2] L. Kronecker. “Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten.”. In: Journal für die reine und angewandte Mathematik (Crelles Journal) 1857.53 (1857), pp. 173–175. DOI: 10.1515/crll.1857.53.173.

references II

[3] Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. “On the Skolem Problem and the Skolem Conjecture”. In: Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science. LICS ’22. Haifa, Israel: Association for Computing Machinery, 2022. DOI: 10.1145/3531130.3533328.

[4] Maurice Mignotte, Tarlok Shorey, and Robert Tijdeman. “The distance between terms of an algebraic recurrence sequence”. In: Journal für die Reine und Angewandte Mathematik (1984), pp. 63–76.

references III

[5] Joël Ouaknine and James Worrell. “On the Positivity Problem for Simple Linear Recurrence Sequences,” in: Automata, Languages, and Programming. Ed. by Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 318–329.

[6] Nikolai Vereshchagin. “Occurrence of zero in a linear recursive sequence”. In: Mathematical notes of the Academy of Sciences of the USSR 38.2 (1985), pp. 609–615.