Fragments of Hilbert's Program

Joël Ouaknine

Max Planck Institute for Software Systems, Germany

(joint work with Valérie Berthé, Florian Luca, James Worrell,
Toghrul Karimov, Joris Nieuwveld, Mihir Vahanwala)

Workshop on recurrence, transcendence, and Diophantine approximation
Lorentz Center, Netherlands, 14–18 July 2025

Funded by the European Union

Funded by DFG Deutsche Forschungsgemeinschaft German Research Foundation

Calculemus!

Calculemus!

If I have seen farther than others, it is because I have stood on the shoulders of giants;

Calculemus!

If I have seen farther than others, it is because I have stood on the shoulders of giants;
You, my dear Hooke, have not.

Leibniz's Dream: reducing mathematics to mere computation

Leibniz visited the Royal Society in 1673 where he demonstrated a calculating machine that he had designed and had been building since 1670. The machine was able to execute all four basic operations (adding, subtracting, multiplying, and dividing), and the Royal Society promptly elected him as external member.

Leibniz's Dream: reducing mathematics to mere computation

Leibniz visited the Royal Society in 1673 where he demonstrated a calculating machine that he had designed and had been building since 1670. The machine was able to execute all four basic operations (adding, subtracting, multiplying, and dividing), and the Royal Society promptly elected him as external member.

But in fact, Leibniz's boyhood "wonderful idea" went much further: to devise *an alphabet representing all fundamental concepts*.

Leibniz's Dream: reducing mathematics to mere computation

Leibniz visited the Royal Society in 1673 where he demonstrated a calculating machine that he had designed and had been building since 1670. The machine was able to execute all four basic operations (adding, subtracting, multiplying, and dividing), and the Royal Society promptly elected him as external member.

But in fact, Leibniz's boyhood "wonderful idea" went much further: to devise *an alphabet representing all fundamental concepts*.

Each symbol would represent some definite idea in a natural and appropriate way. His *calculus ratiocinator* (algebra of symbolic logic) would then bring under mathematical laws human reasoning, "which is the most excellent and useful thing we have".

Leibniz's Dream: reducing mathematics to mere computation

Leibniz visited the Royal Society in 1673 where he demonstrated a calculating machine that he had designed and had been building since 1670. The machine was able to execute all four basic operations (adding, subtracting, multiplying, and dividing), and the Royal Society promptly elected him as external member.

But in fact, Leibniz's boyhood "wonderful idea" went much further: to devise *an alphabet representing all fundamental concepts*.

Each symbol would represent some definite idea in a natural and appropriate way. His *calculus ratiocinator* (algebra of symbolic logic) would then bring under mathematical laws human reasoning, "which is the most excellent and useful thing we have".

``In large language models (LLMs), a *token* is a chunk of text used as a basic unit for processing -- typically a word, subword, or even character, depending on the language and tokenizer. The model reads and generates text in terms of these tokens, not full words or sentences, enabling it to handle diverse languages and structures efficiently.''

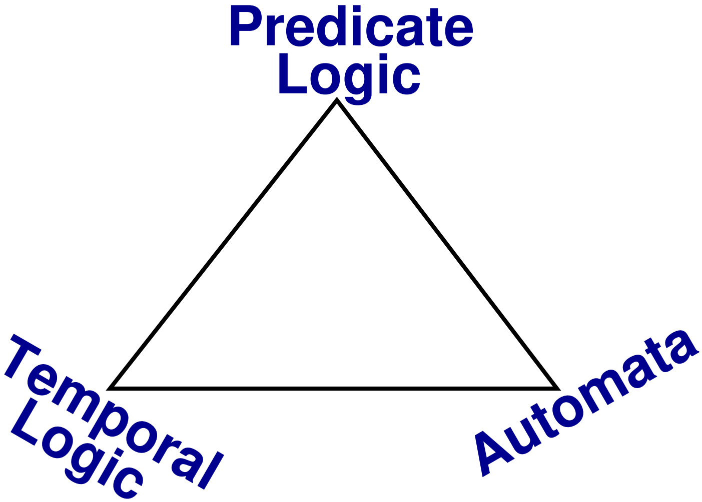
Hilbert's Program and the Entscheidungsproblem

Hilbert's Program and the Entscheidungsproblem

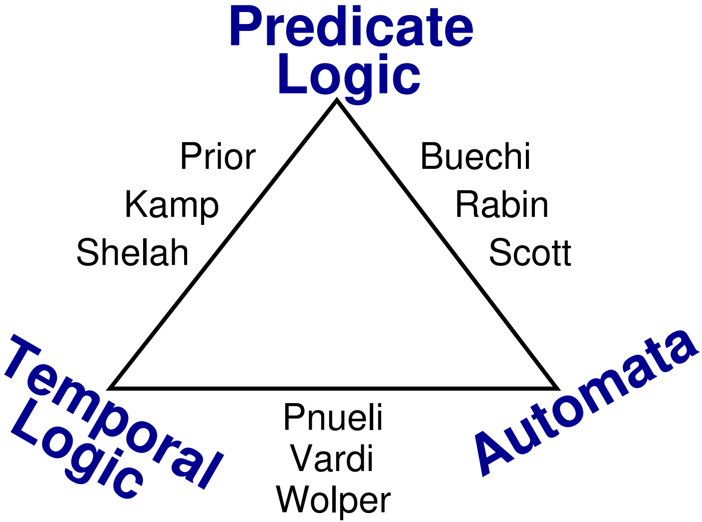
Wir müssen wissen. Wir werden wissen.

Fast forward about a hundred years. . .

The Holy Trinity of Theoretical Computer Science



The Holy Trinity of Theoretical Computer Science



Theorem (Euclid, c. 300 BC)

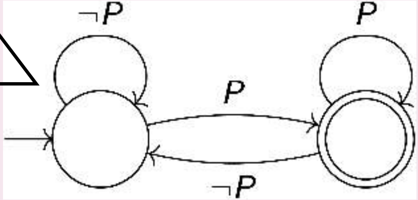
Let P denote the set of prime numbers. Then the following holds:

Theorem (Euclid, c. 300 BC)

Let P denote the set of prime numbers. Then the following holds:

$$\forall x \, \exists y \, (y > x \wedge P(y))$$

$$\mathbf{G} \, \mathbf{F} \, P$$



The Monadic Second-Order Logic of Order

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

Examples:

- $y = x + 1$ iff $x < y \wedge \forall z\, (x < z \Rightarrow (y < z \vee y = z))$

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

Examples:

- $y = x + 1$ iff $x < y \wedge \forall z\, (x < z \Rightarrow (y < z \vee y = z))$
- Q is the set of integers congruent to 1 mod 4 iff

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

Examples:

- $y = x + 1$ iff $x < y \wedge \forall z\, (x < z \Rightarrow (y < z \vee y = z))$
- Q is the set of integers congruent to 1 mod 4 iff

$$\neg Q(0) \wedge Q(1) \wedge \neg Q(2) \wedge \neg Q(3) \wedge \forall x\, (Q(x) \Leftrightarrow Q(x+4)) \qquad (*)$$

The Monadic Second-Order Logic of Order

The syntax of **MSO**$\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

Examples:

- $y = x + 1$ iff $x < y \wedge \forall z\, (x < z \Rightarrow (y < z \vee y = z))$
- Q is the set of integers congruent to 1 mod 4 iff

$$\neg Q(0) \wedge Q(1) \wedge \neg Q(2) \wedge \neg Q(3) \wedge \forall x\, (Q(x) \Leftrightarrow Q(x+4)) \qquad (*)$$

Theorem (Dirichlet, 1837)

Let PRIMES denote the set of prime numbers. Then

$$\forall x\, \exists y\, (y > x \wedge PRIMES(y) \wedge \exists Q\, .\, ((*) \wedge Q(y)))\, .$$

The Monadic Second-Order Logic of Order

The syntax of $\mathbf{MSO}\langle \mathbb{N}; < \rangle$

$$\varphi ::= x < y \mid P(x) \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid \forall P\, \varphi \mid \exists P\, \varphi$$

Examples:

- $y = x + 1$ iff $x < y \wedge \forall z\, (x < z \Rightarrow (y < z \vee y = z))$
- Q is the set of integers congruent to 1 mod 4 iff

$$\neg Q(0) \wedge Q(1) \wedge \neg Q(2) \wedge \neg Q(3) \wedge \forall x\, (Q(x) \Leftrightarrow Q(x+4)) \qquad (*)$$

Theorem (Dirichlet, 1837)

Let PRIMES denote the set of prime numbers. Then

$$\forall x\, \exists y\, (y > x \wedge PRIMES(y) \wedge \exists Q\,.\, ((*) \wedge Q(y)))\,.$$

- Above formula is an example of a sentence in the MSO theory of $\langle \mathbb{N}; <, PRIMES \rangle$

Question (Büchi and Landweber, 1969)

Is the MSO theory of $\langle \mathbb{N}; <, \mathit{PRIMES} \rangle$ decidable?

Question (Büchi and Landweber, 1969)

Is the MSO theory of $\langle \mathbb{N}; <, \mathit{PRIMES} \rangle$ *decidable?*

Theorem (Bateman, Jockusch, and Woods, 1993)

Yes, assuming Schinzel's Hypothesis H.

A glimpse of the Hilbert Landscape

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

Solution requires Baker's theorem on linear forms in logarithms!

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ *is decidable.*

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ *is decidable.*

The genesis of the grand love affair between logic and automata!

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ *is decidable.*

The genesis of the grand love affair between logic and automata!

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 4^{\mathbb{N}} \rangle$
- $\ldots$

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ *is decidable.*

The genesis of the grand love affair between logic and automata!

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 4^{\mathbb{N}} \rangle$
- $\ldots$

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ is decidable.

The genesis of the grand love affair between logic and automata!

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 4^{\mathbb{N}} \rangle$
- $\ldots$

But can these predicates be combined??

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ is decidable.

The genesis of the grand love affair between logic and automata!

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 4^{\mathbb{N}} \rangle$
- $\ldots$

But can these predicates be combined??

Theorem (Büchi, 1962)

The MSO theory of $\langle \mathbb{N}; < \rangle$ is decidable.

The genesis of the grand love affair between logic and automata!

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 4^{\mathbb{N}} \rangle$
- $\ldots$

. . . much subsequent work over the ensuing decades (Landweber, Semenov, Thomas, Rabinovich, Carton, . . .)

But can these predicates be combined??

RESEARCH-ARTICLE | OPEN ACCESS

On the Decidability of Monadic Second-Order Logic with Arithmetic Predicates

Authors: Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell | Authors Info & Claims

LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science

(LICS 2024 Distinguished Paper Award)

RESEARCH-ARTICLE | OPEN ACCESS

On the Decidability of Monadic Second-Order Logic with Arithmetic Predicates

Authors: Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell | Authors Info & Claims

LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science

(LICS 2024 Distinguished Paper Award)

Theorem (Berthé *et al.*, 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, {a_1}^{\mathbb{N}}, \ldots, {a_k}^{\mathbb{N}} \rangle$ *assuming Schanuel's Conjecture*

RESEARCH-ARTICLE | OPEN ACCESS

On the Decidability of Monadic Second-Order Logic with Arithmetic Predicates

Authors: Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell | Authors Info & Claims

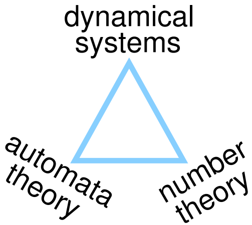
LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science

(LICS 2024 Distinguished Paper Award)

Theorem (Berthé *et al.*, 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, {a_1}^{\mathbb{N}}, \ldots, {a_k}^{\mathbb{N}} \rangle$ *assuming Schanuel's Conjecture*



RESEARCH-ARTICLE | OPEN ACCESS

On the Decidability of Monadic Second-Order Logic with Arithmetic Predicates

Authors: Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell | Authors Info & Claims

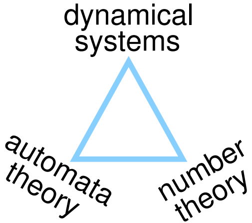
LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science

(LICS 2024 Distinguished Paper Award)

Theorem (Berthé *et al.*, 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, {a_1}^{\mathbb{N}}, \ldots, {a_k}^{\mathbb{N}} \rangle$ *assuming Schanuel's Conjecture*



We are planning to implement this algorithm!

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

There are 26 pairs in total;
the last one is $(m = 8, n = 5)$,
with $|2^8 - 3^5| = 13$

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

A glimpse of the Hilbert Landscape

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

There are 26 pairs in total;
the last one is $(m = 8, n = 5)$,
with $|2^8 - 3^5| = 13$

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Yes, there are infinitely many.
The first pair is
$(m = 1788, n = 1128)$;
3^{1128} has 539 digits!

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

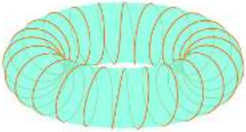
RESEARCH-ARTICLE | OPEN ACCESS

On the Decidability of Monadic Second-Order Logic with Arithmetic Predicates

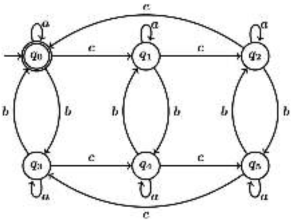
Authors Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell   Authors Info & Claims

LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science

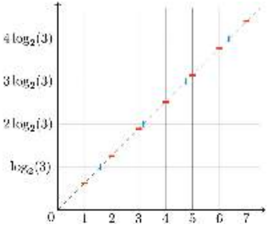
toric words



logic & automata theory



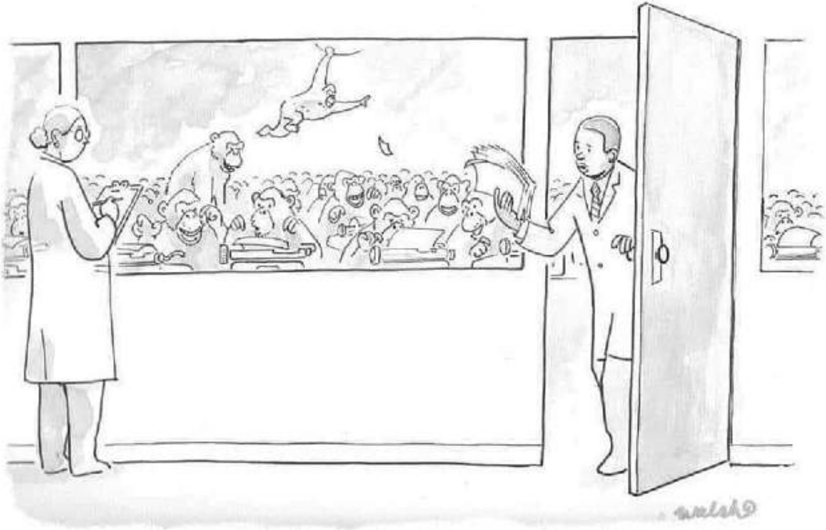
Diophantine geometry



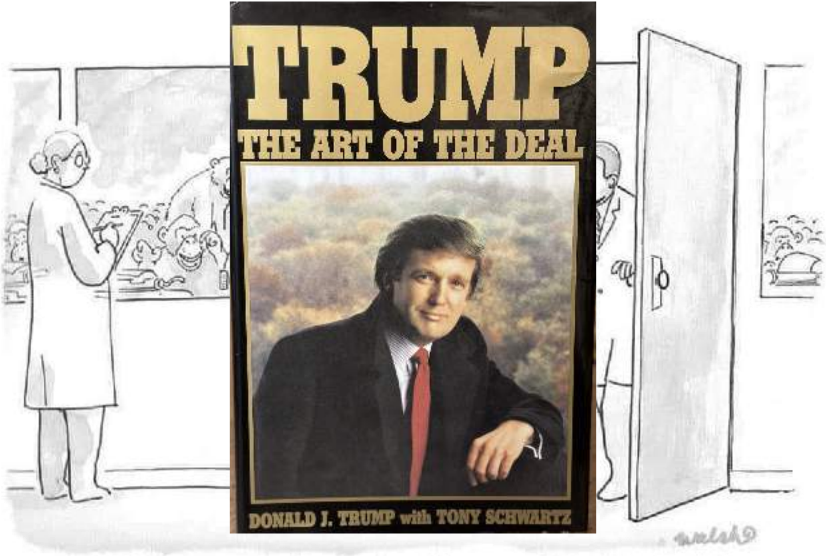
Normality and Disjunctivity

Normality and Disjunctivity

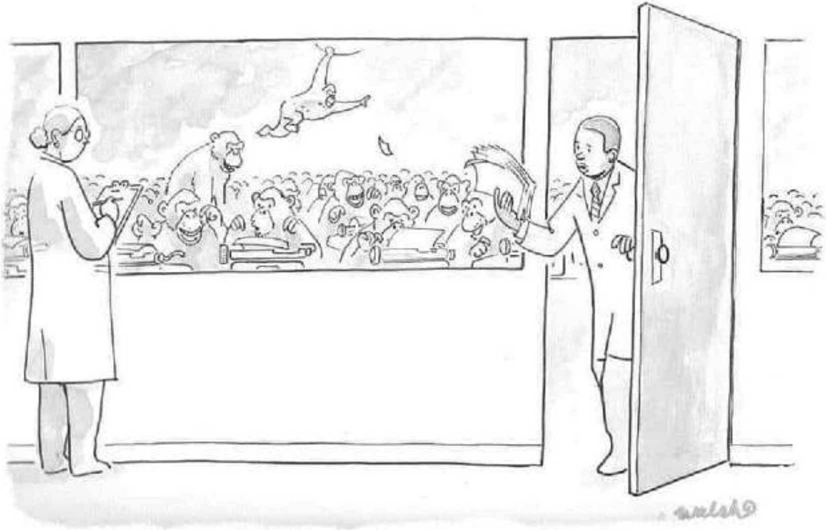
$\sqrt{2} = 1.41421356237309504880168872420969807856967187537694807317667973799$0
7324784621070388503875343276415727350138462309122970249248360558507372126
4412149709993583141322266592750559275579995050115278206057147010955997160
5970274534596862014728517418640889198609552329230484308714321450839762603
6279952514079896872533965463318088296406206152583523950547457502877599617
2983557522033753185701135437460340849884716038689997069900481503054402779
0316454247823068492936918621580578463111596668713013015618568987237235288
5092648612494977154218334204285686060146824720771435854874155657069677653
7202264854470158588016207584749226572260020855844665214583988939443709265
9180031138824646815708263010059485870400318648034219489727829064104507263
6881313739855256117322040245091227700226941127573627280495738108967504018
3698683684507257993647290607629969413804756548237289971803268024744206292
6912485905218100445984215059112024944134172853147810580360337107730918286
9314710171111683916581726889419758716582152128229518488472089694633862891
5628827659526351405422676532396946175112916024087155101351504553812875600
5263146801712740265396947024030051749531886292563138518816347800156936 9...



"No Shakespeare yet, but here's another copy of 'Art of the Deal'."



"No Shakespeare yet, but here's another copy of 'Art of the Deal'."



"No Shakespeare yet, but here's another copy of 'Art of the Deal'."

Back to the Elgot-Rabin paper . . .

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- . . .
- $\langle \mathbb{N}; <, \mathit{SQUARES} \rangle$
- $\langle \mathbb{N}; <, \mathit{CUBES} \rangle$
- . . .
- $\langle \mathbb{N}; <, \mathit{FIB} \rangle$
- $\langle \mathbb{N}; <, \mathit{FACT} \rangle$
- . . .

Back to the Elgot-Rabin paper ...

Theorem (Elgot and Rabin, 1966)

The MSO theory of each of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}} \rangle$
- $\langle \mathbb{N}; <, 3^{\mathbb{N}} \rangle$
- $\ldots$
- $\langle \mathbb{N}; <, SQUARES \rangle$
- $\langle \mathbb{N}; <, CUBES \rangle$
- $\ldots$
- $\langle \mathbb{N}; <, FIB \rangle$
- $\langle \mathbb{N}; <, FACT \rangle$
- $\ldots$

Which predicates can one combine?

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

There are 26 pairs in total;
the last one is $(m = 8, n = 5)$,
with $|2^8 - 3^5| = 13$

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Yes, there are infinitely many.
The first pair is
$(m = 1788, n = 1128)$;
3^{1128} has 539 digits!

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

Theorem (Berthé *et al.*, LICS 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *assuming* $\sqrt{2}$ *is disjunctive in binary*

Theorem (Berthé *et al.*, LICS 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *assuming* $\sqrt{2}$ *is disjunctive in binary*
- $\langle \mathbb{N}; <, 4^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *(unconditionally)*

Theorem (Berthé *et al.*, LICS 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *assuming* $\sqrt{2}$ *is disjunctive in binary*
- $\langle \mathbb{N}; <, 4^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *(unconditionally)*
- $\langle \mathbb{N}; <, b^{\mathbb{N}}, \mathit{FIB} \rangle$ *(unconditionally)*

Theorem (Berthé *et al.*, LICS 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *assuming* $\sqrt{2}$ *is disjunctive in binary*
- $\langle \mathbb{N}; <, 4^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *(unconditionally)*
- $\langle \mathbb{N}; <, b^{\mathbb{N}}, \mathit{FIB} \rangle$ *(unconditionally)*
- $\ldots$ *(see paper!)*

Theorem (Berthé *et al.*, LICS 2024)

The MSO theory of the following structures is decidable:

- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *assuming* $\sqrt{2}$ *is disjunctive in binary*
- $\langle \mathbb{N}; <, 4^{\mathbb{N}}, \mathit{SQUARES} \rangle$ *(unconditionally)*
- $\langle \mathbb{N}; <, b^{\mathbb{N}}, \mathit{FIB} \rangle$ *(unconditionally)*
- $\ldots$ *(see paper!)*

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

There are 26 pairs in total;
the last one is $(m = 8, n = 5)$,
with $|2^8 - 3^5| = 13$

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Yes, there are infinitely many.
The first pair is
$(m = 1788, n = 1128)$;
3^{1128} has 539 digits!

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

Are there finitely many m and n such that

$$|2^m - 3^n| \leq 100\,?$$

If so, enumerate them.

There are 26 pairs in total;
the last one is $(m = 8, n = 5)$,
with $|2^8 - 3^5| = 13$

Are there infinitely many m and n such that

$$3^n < 2^m < 2^{m+1} < 3^{n+1} < 2^{m+2} < 2^{m+3} < 3^{n+2}$$

and

$$2^m \equiv 3^n \equiv 1 \pmod{13}\,?$$

Yes, there are infinitely many.
The first pair is
$(m = 1788, n = 1128)$;
3^{1128} has 539 digits!

Are there finitely many n such that the number of perfect squares between 2^n and 2^{n+1} is even, *and* the number of perfect squares between 2^{n+1} and 2^{n+2} is divisible by 3?

This is open! However:

- If $\sqrt{2}$ is disjunctive in binary, then there are infinitely many such n;
- If certain specific strings only occur *finitely often* in the binary expansion of $\sqrt{2}$, then there are only finitely many such n

Fragments of Hilbert's Program: More open problems

Open Problems

Is the MSO theory of the following structures decidable?

- $\langle \mathbb{N}; <, \mathit{SQUARES}, \mathit{CUBES} \rangle$
- $\langle \mathbb{N}; <, \mathit{SQUARES}, \mathit{FACT} \rangle$
- $\langle \mathbb{N}; <, \mathit{SQUARES}, \mathit{FIB} \rangle$
- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathit{FACT} \rangle$
- $\ldots$

Fragments of Hilbert's Program: More open problems

Open Problems

Is the MSO theory of the following structures decidable?

- $\langle \mathbb{N}; <, SQUARES, CUBES \rangle$
- $\langle \mathbb{N}; <, SQUARES, FACT \rangle$
- $\langle \mathbb{N}; <, SQUARES, FIB \rangle$
- $\langle \mathbb{N}; <, 2^{\mathbb{N}}, FACT \rangle$
- $\ldots$

The *Brocard-Ramanujan Problem:* Find all integers m and n such that

$$n! + 1 = m^2$$

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Easy alternative proof of decidability of Presburger Arithmetic via the embedding:

$$\mathsf{FO}\langle \mathbb{N}; 0, 1, <, + \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$$

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Easy alternative proof of decidability of Presburger Arithmetic via the embedding:

$$\mathsf{FO}\langle \mathbb{N}; 0, 1, <, + \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$$

- Idea: given a natural number $x = b_0 b_1 \ldots b_k$ encoded in reverse in binary (from least significant to most significant bit), represent x as a finite set $P_x = \{j \in \mathbb{N} : b_j = 1\}$

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Easy alternative proof of decidability of Presburger Arithmetic via the embedding:

$$\mathsf{FO}\langle \mathbb{N}; 0, 1, <, + \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$$

- Idea: given a natural number $x = b_0 b_1 \ldots b_k$ encoded in reverse in binary (from least significant to most significant bit), represent x as a finite set $P_x = \{j \in \mathbb{N} : b_j = 1\}$
- Perform addition using the primary-school technique, with the help of an auxiliary existentially quantified "carry" predicate, etc.

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Easy alternative proof of decidability of Presburger Arithmetic via the embedding:

$$\mathsf{FO}\langle \mathbb{N}; 0, 1, <, + \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$$

- Idea: given a natural number $x = b_0 b_1 \ldots b_k$ encoded in reverse in binary (from least significant to most significant bit), represent x as a finite set $P_x = \{j \in \mathbb{N} : b_j = 1\}$
- Perform addition using the primary-school technique, with the help of an auxiliary existentially quantified "carry" predicate, etc.

For free: $\mathsf{FO}\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}} \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$

Presburger Arithmetic and non-linear expansions

- Aka *linear arithmetic*: the first-order theory of the structure $\langle \mathbb{N}; 0, 1, <, + \rangle$
- Shown *decidable* in 1929 by Presburger, a student of Tarski, with the explicit aims of advancing both Hilbert's Program and the Entscheidungsproblem
- Presburger's decision procedure was through quantifier elimination

Easy alternative proof of decidability of Presburger Arithmetic via the embedding:

$$\mathsf{FO}\langle \mathbb{N}; 0, 1, <, + \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle$$

- Idea: given a natural number $x = b_0 b_1 \ldots b_k$ encoded in reverse in binary (from least significant to most significant bit), represent x as a finite set $P_x = \{j \in \mathbb{N} : b_j = 1\}$
- Perform addition using the primary-school technique, with the help of an auxiliary existentially quantified "carry" predicate, etc.

For free: $\mathsf{FO}\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}} \rangle \hookrightarrow \mathsf{MSO}\langle \mathbb{N}; < \rangle \hookleftarrow \mathsf{FO}\langle \mathbb{N}; 0, 1, <, +, 3^{\mathbb{N}} \rangle$

Question (van den Dries, mid-1980s)

Is the FO theory of $\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ *decidable?*

Question (van den Dries, mid-1980s)

Is the FO theory of $\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ *decidable?*

Theorem (Hieronymi and Schulz, 2022)

No.

Question (van den Dries, mid-1980s)

Is the FO theory of $\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ *decidable?*

Theorem (Hieronymi and Schulz, 2022)

No.

Theorem (Karimov, Luca, Nieuwveld, O., Worrell, 2025)

For any $a, b \in \mathbb{N}$*, the existential fragment of the FO theory of* $\langle \mathbb{N}; 0, 1, <, +, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$ *is decidable.*

Question (van den Dries, mid-1980s)

Is the FO theory of $\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ *decidable?*

Theorem (Hieronymi and Schulz, 2022)

No.

Theorem (Karimov, Luca, Nieuwveld, O., Worrell, 2025)

For any $a, b \in \mathbb{N}$*, the existential fragment of the FO theory of* $\langle \mathbb{N}; 0, 1, <, +, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$ *is decidable.*

Open Problem

What about the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, a_1^{\mathbb{N}}, \ldots, a_k^{\mathbb{N}} \rangle$*?*

Question (van den Dries, mid-1980s)

Is the FO theory of $\langle \mathbb{N}; 0, 1, <, +, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ *decidable?*

Theorem (Hieronymi and Schulz, 2022)

No.

Theorem (Karimov, Luca, Nieuwveld, O., Worrell, 2025)

For any $a, b \in \mathbb{N}$, *the existential fragment of the FO theory of* $\langle \mathbb{N}; 0, 1, <, +, a^{\mathbb{N}}, b^{\mathbb{N}} \rangle$ *is decidable.*

Open Problem

What about the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, a_1^{\mathbb{N}}, \ldots, a_k^{\mathbb{N}} \rangle$*?*

- At the very least, would imply *effective* lower bounds on sums of S-units

Presburger Arithmetic and perfect squares

Theorem (folklore)

The FO theory of $\langle \mathbb{N}; 0, 1, <, +, \mathit{SQUARES} \rangle$ *is undecidable.*

Presburger Arithmetic and perfect squares

Theorem (folklore)

The FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ *is undecidable.*

Question (Büchi, mid-1970s)

What about the existential fragment?

Presburger Arithmetic and perfect squares

Theorem (folklore)

The FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ *is undecidable.*

Question (Büchi, mid-1970s)

What about the existential fragment?

$$\exists x, y, z \begin{pmatrix} x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge \\ S(x) \wedge S(y) \wedge S(z) \wedge \\ S(x+y) \wedge S(x+z) \wedge S(y+z) \wedge \\ S(x+y+z) \end{pmatrix}$$

Presburger Arithmetic and perfect squares

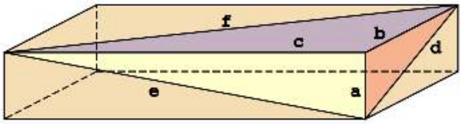
Theorem (folklore)

The FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ *is undecidable.*

Question (Büchi, mid-1970s)

What about the existential fragment?

$$\exists x, y, z \begin{pmatrix} x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge \\ S(x) \wedge S(y) \wedge S(z) \wedge \\ S(x+y) \wedge S(x+z) \wedge S(y+z) \wedge \\ S(x+y+z) \end{pmatrix}$$



Büchi's Problem

Suppose that $\langle s_1, s_2, \ldots, s_M \rangle$ is an increasing sequence of *consecutive* perfect squares. Then for all $1 \leq n \leq M - 2$,

$$s_{n+2} - 2s_{n+1} + s_n = 2 \qquad (\star)$$

Büchi's Problem

Suppose that $\langle s_1, s_2, \ldots, s_M \rangle$ is an increasing sequence of *consecutive* perfect squares. Then for all $1 \leq n \leq M - 2$,

$$s_{n+2} - 2s_{n+1} + s_n = 2 \qquad (\star)$$

Büchi's Problem (mid-1970s)

Does there exist $M \in \mathbb{N}$ such that, whenever $\langle u_1, u_2, \ldots, u_M \rangle$ is a sequence of perfect squares satisfying $(\star)$, then it must necessarily be a sequence of consecutive squares? Büchi's Conjecture is that such an M exists.

Büchi's Problem

Suppose that $\langle s_1, s_2, \ldots, s_M \rangle$ is an increasing sequence of *consecutive* perfect squares. Then for all $1 \leq n \leq M - 2$,

$$s_{n+2} - 2s_{n+1} + s_n = 2 \qquad (\star)$$

Büchi's Problem (mid-1970s)

Does there exist $M \in \mathbb{N}$ such that, whenever $\langle u_1, u_2, \ldots, u_M \rangle$ is a sequence of perfect squares satisfying $(\star)$, then it must necessarily be a sequence of consecutive squares? Büchi's Conjecture is that such an M exists.

There are infinitely many counterexamples with $M = 4$.
Büchi in fact conjectured that $M = 5$ would suffice.

Büchi's Problem

Suppose that $\langle s_1, s_2, \ldots, s_M \rangle$ is an increasing sequence of *consecutive* perfect squares. Then for all $1 \leq n \leq M - 2$,

$$s_{n+2} - 2s_{n+1} + s_n = 2 \qquad (\star)$$

Büchi's Problem (mid-1970s)

Does there exist $M \in \mathbb{N}$ such that, whenever $\langle u_1, u_2, \ldots, u_M \rangle$ is a sequence of perfect squares satisfying $(\star)$, then it must necessarily be a sequence of consecutive squares? Büchi's Conjecture is that such an M exists.

There are infinitely many counterexamples with $M = 4$.
Büchi in fact conjectured that $M = 5$ would suffice.

Theorem (Büchi, mid-1970s)

Büchi's Conjecture implies that the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ is undecidable.

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Theorem (Vojta, 1999)

The Bombieri-Lang Conjecture implies that Büchi's Conjecture is true. Specifically, with $M = 8$ *there could only be at most finitely many counterexamples.*

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Theorem (Vojta, 1999)

The Bombieri-Lang Conjecture implies that Büchi's Conjecture is true. Specifically, with $M = 8$ there could only be at most finitely many counterexamples.

Theorem (Stanley Yao Xiao, December 2024)

Büchi's Conjecture is true with $M = 5$!

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Theorem (Vojta, 1999)

The Bombieri-Lang Conjecture implies that Büchi's Conjecture is true. Specifically, with $M = 8$ *there could only be at most finitely many counterexamples.*

Theorem (Stanley Yao Xiao, December 2024)

Büchi's Conjecture is true with $M = 5$ *!*
As a consequence, the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ *is undecidable.*

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Theorem (Vojta, 1999)

The Bombieri-Lang Conjecture implies that Büchi's Conjecture is true. Specifically, with $M = 8$ there could only be at most finitely many counterexamples.

Theorem (Stanley Yao Xiao, December 2024)

Büchi's Conjecture is true with $M = 5$!
As a consequence, the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, SQUARES \rangle$ is undecidable.

Open Problem

Is the two-variable existential fragment of $\langle \mathbb{N}; 0, 1, <, +, -, SQUARES \rangle$ decidable?
i.e., is there an algorithm to decide whether a given formula $\exists x, y \,.\, \varphi(x, y)$ is true?

Büchi's Problem

There has been extensive work on Büchi's Problem; see e.g. surveys by Lipshitz (1990), Mazur (1994), Pasten *et al.* (2010), etc.

Theorem (Vojta, 1999)

The Bombieri-Lang Conjecture implies that Büchi's Conjecture is true. Specifically, with $M = 8$ there could only be at most finitely many counterexamples.

Theorem (Stanley Yao Xiao, December 2024)

Büchi's Conjecture is true with $M = 5$!
As a consequence, the existential fragment of the FO theory of $\langle \mathbb{N}; 0, 1, <, +, \mathit{SQUARES} \rangle$ is undecidable.

Open Problem

Is the two-variable existential fragment of $\langle \mathbb{N}; 0, 1, <, +, -, \mathit{SQUARES} \rangle$ decidable?
i.e., is there an algorithm to decide whether a given formula $\exists x, y \,.\, \varphi(x, y)$ is true?

- Note that this fragment is strong enough to express Büchi's Conjecture!

Outlook

Hilbert's legacy continues to be a rich source of inspiration!

Thriving research endeavour at the confluence of computer science and mathematics