

CMPE 210 COMPUTATIONAL MODELS & COMPLEXITY

PROJECT PRESENTATION
Winter 2001

HILBERT'S 10TH PROBLEM IS UNSOLVABLE



Hilbert 1900

10. Entscheidung der Losbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

ISMAIL ARI
ari@cse.ucsc.edu

University of California Santa Cruz

A Roadmap

- A Quick History
- Hilbert's 10th Problem Definition
- Terminology and easy examples
 - Diophantine sets
 - Diophantine functions
- Exponential Function $h(n,k) = n^k$ is Diophantine
- Language of Diophantine predicates
- Bounded quantifiers
- Recursive functions
- Universal (all) Diophantine Set(s) (D_n)
- $g(n,x)$ a non-recursive function
 - its recursiveness would imply $\exists x \in D_n$
 - algorithm to test $P(n, x, z_1, \dots, z_k) = 0$
 - algorithm to test $\exists x \in D_n$
 - algorithm to compute $g(n,x)$

A Quick History

1900 Hilbert states his 10th problem among the 23 problems, “problems from the discussion of which an advancement of science may be expected.”

1930s: The notion of computability and algorithm
K. Gödel, A. Church, Stephen Kleene and Alan Turing.

1931 Gödel existence of undecidable statements in formal systems. (...Every recursive function + r.e. set - can be defined by a Diophantine equation preceded by a finite number of existential and bounded universal quantifiers.)

1936 Turing Invention of Universal Turing Machine and the discovery of basic unsolvable problems.

1953 Davis shows bounded universal quantifiers could be eliminated, so that every r.e. set S could be defined as:

$$S = \{x \mid (\exists y)(\forall k)_{\leq y} (\exists y_1..y_m) [P(k, x, y, y_1, \dots, y_m) = 0]\}$$

1950s Julia Robinson Hypothesis :

There exists a Diophantine set D such that:

- (1) $\langle u, v \rangle \in D$ implies $v \leq u^u$
- (2) For each k there is $\langle u, v \rangle \in D$ such that $v > u^k$

1970 Matyasevich proves Julia Robinson's Hypothesis using Fibonacci Numbers.

$$(5/4)^n < a_n < 2^{n-1} \quad \text{for } n \geq 3$$

a_n is the n th Fibonacci number

if we define $a_1 = a_2 = 1$, $a_{n+1} = a_n + a_{n-1}$

a_{2n} (function) is Diophantine.

The set $D = \{ \langle u, v \rangle \mid v = a_{2u} \ \& \ u \geq 2 \}$ satisfies Julia Robinson's Hypothesis.

PROBLEM DEFINITION

- Hilbert's 10th problem is to give a computing algorithm, which will tell of a given polynomial Diophantine equation with integer coefficients whether or not it has a solution in *integers*.
- Hilbert's 10th Problem is a decision problem where an answer YES or NO is to be given.
- Hilbert asked for a universal method for recognizing the solvability of Diophantine equations.
- Matyasevich proved that there is no such algorithm.
- Would Hilbert be satisfied with this unsolvability answer?

YES, because Hilbert's address: "Sometimes ... therefore unable to reach our goal. The task arises of proving the impossibility of solving the problem..."

Definitions of Diophantine Sets and Easy Examples

n -tuple $\langle x_1, \dots, x_n \rangle$ (*parameters*) belong to Diophantine set S iff there exists positive integers $\langle y_1, \dots, y_m \rangle$ (*unknowns*) $m \geq 0$, such that there is a polynomial:

$$P(x_1, \dots, x_n, y_1, \dots, y_m) = 0.$$

Logic Representation:

$$\langle x_1, \dots, x_n \rangle \in S \Leftrightarrow \exists y_1 \dots y_m [P(x_1, \dots, x_n, y_1, \dots, y_m) = 0]$$
$$S = \{ \langle x_1, \dots, x_n \rangle \mid (\exists y_1 \dots y_m) [P(x_1, \dots, x_n, y_1, \dots, y_m) = 0] \}$$

EXAMPLES (of Diophantine Sets)

$$x - y^2 = 0$$

The numbers which are not powers of 2:

$$x \in S \Leftrightarrow (\exists y, z) [x = y(2z+1)]$$

The composite numbers :

$$x \in S \Leftrightarrow (\exists y, z) [x = (y+1)(z+1)]$$

The ordering relations:

$$x < y \Leftrightarrow (\exists z) [x + z = y]$$

$$\text{Divisibility: } a \mid b \Leftrightarrow \exists x [ax = b]$$

Others, $h(n, k) = n^k$, primes, ALL RECURSIVE!!

Diophantine Functions

A function f of n arguments is called Diophantine if $\{ \langle x_1, \dots, x_n, y \rangle \mid y = f(x_1, \dots, x_n) \}$ is a Diophantine set.

Examples (of Diophantine functions):

Theorem 1.1 Pairing Function Theorem

There are Diophantine functions $P(x,y)$, $L(z)$, $R(z)$ s.t.

- (1) for all x,y $L(P(x,y)) = x$, $R(P(x,y)) = y$
- (2) for all z , $P(L(z), R(z)) = z$, $L(z) \leq z$, $R(z) \leq z$

Theorem 1.2 Sequence Number Theorem

There is a Diophantine function $S(i,u)$ s.t.

- (1) $S(i,u) \leq u$, and
- (2) for each **sequence** a_1, \dots, a_N there is a **number** u s.t. $S(i,u) = a_i$ for $1 \leq i \leq N$.

$$w = L(u) \bmod (1 + iR(u))$$

$$w \leq (1 + iR(u))$$

$1 + iR(u)$ is called the admissible sequence of moduli (*relatively prime*) in Chinese Remainder Theorem.

Why Theorem 1.1 and 1.2?

Used in the elimination of Bounded Quantifiers...

Exponential Function $h(n,k) = n^k$ is Diophantine

Pell Equation (*).

$$x^2 - dy^2 = 1 \quad x, y \geq 0,$$
$$d = a^2 - 1, \quad a > 1$$

$x = x_k(a) \in S$ satisfying this equation is given by the 24 Lemmas.

Consider the following system of equations:

$$(I) \quad x^2 - (a-1)y^2 = 1$$

$$(II) \quad u^2 - (a-1)v^2 = 1$$

$$(III) \quad s^2 - (b-1)t^2 = 1$$

$$(IV) \quad v = ry^2$$

$$(V) \quad b = 1 + 4py = a + qu$$

$$(VI) \quad s = x + cu$$

$$(VII) \quad t = k + 4(d-1)y$$

$$(VIII) \quad y = k + e - 1$$

Theorem 3.1 : System I-VIII has a solution iff $x = x_k(a)$, where,

x as in I and VI; k as in VII and VIII ; a as in I, II and V.

Corollary 3.2: The function $g(z,k) = x_k(z + 1)$ is Diophantine.

$$A) \quad a = z+1$$

System I-VIII has a solution iff $x = x_k(a) = x_k(z+1) = g(z,k)$

Diophantine definition of g can be obtained by summing the squares of 9 polynomials. In addition:

$$(IX) (x - y(a - n) - m)^2 = (f - 1)^2 (2an - n^2 - 1)^2$$

$$(X) m + g = 2an - n^2 - 1$$

$$(XI) w = n + h = k + 1$$

$$(XII) a^2 - (w^2 - 1)^2(w - 1)^2z^2 = 1$$

Lemma 3.5 $m = n^k$ iff equations IX-XII have a solution in the remaining arguments.

Theorem 3.3. The exponential function $h(n,k) = n^k$ is Diophantine.

Theorem 4.1: The following functions are Diophantine

$$(1) f(n,k) = \text{Combination}(n,k)$$

$$(2) g(n) = n!$$

$$(3) h(a,b,y) = \prod (a + bk) \quad , k : 1..y$$

(1) & (2) by Robinson and (3) by Davis by using (1) & (2)

Language of Diophantine predicates:

$+, \cdot, \wedge, \vee, n^k, n!, \exists, \dots$

$$(\exists r_1, \dots, r_n) [P_1 = 0] \vee (\exists s_1, \dots, s_m) [P_2 = 0]$$

\Leftrightarrow

$$(\exists r_1, \dots, r_n, s_1, \dots, s_m) [P_1.P_2 = 0]$$

There are two more operations:

Bounded existential quantifier:

“($\exists y$) $_{\leq x}$ ”, “($\exists y$) ($y \leq x \ \& \dots$)”

Bounded universal (!) quantifier:

“($\forall y$) $_{\leq x}$ ”, “($\forall y$) ($y > x \ \vee \dots$)”

$$S = \{ \langle y, x_1, \dots, x_n \rangle \mid (\forall \mathbf{z})_{\leq y} (\exists y_1 \dots y_m) [P(y, z, x_1, \dots, x_n, y_1, \dots, y_m) = 0] \}$$

Davis Normal Form:

Davis obtained a long expanded but equivalent statement free of *Bounded universal quantifier* to show that, *Bounded universal quantifiers were not destroying the Diophantine property.*

Going for all !!!

With the previous Diophantine predicates and Sequence Number Theorem we can show that almost any set we please is Diophantine:

e.g. The set P of prime numbers

$$x \in P \Leftrightarrow 1 \ \& \ (\forall \mathbf{y}, \mathbf{z})_{\leq x} [yz < x \ \vee \ yz > x \ \vee \ y = 1 \ \vee \ z = 1]$$

“How can any reasonable set or function escape these methods and not be Diophantine?”.

Let’s test the class of *all computable* or *recursive* functions.

Recursive functions:

Initial (base) functions: Zero, Succ, P_i^k ,

Primitive recursive constructions: substitution, primitive recursion and minimalization.

Theorem 6.1. A function is Diophantine if and only if it is recursive.

We consider the list of recursive functions: $x+y$, $x.y$, $c(x)=\text{constant}$, thus polynomials are obtained and we conclude every Diophantine function is recursive.

A Universal Diophantine Set

Claim: Any polynomial with positive integer coefficients can be built from **1** and variables (by successive additions and multiplications). We fix the alphabet:

$$x_0, x_1, x_2, x_3, \dots$$

of the variables and then setup the following enumeration of all such polynomials using the pairing functions:

$$\begin{aligned}P_1 &= 1 \\P_{3i-1} &= x_{i-1} \\P_{3i} &= P_{L(i)} + P_{R(i)} \\P_{3i+1} &= P_{L(i)} \cdot P_{R(i)}\end{aligned}$$

Finally let,

$$D_n = \{x_0 | (\exists x_1 \dots x_m) [P_{L(n)}(x_0, x_1, \dots, x_n) = P_{R(n)}(x_0, x_1, \dots, x_n)]\}$$

by the way sequence P_i is constructed it is seen that the sequence of sets $D_1, D_2, D_3 \dots$ includes all Diophantine sets. Moreover,

Theorem 7.1. Universality Theorem

$\{ \langle n, x \rangle \mid x \in D_n \}$ is Diophantine

Theorem 7.2. $V = \{n/n \notin D_n\}$ is not Diophantine.

Theorem 7.3. The function $g(n, x)$ defined by

$$g(n, x) = 1 \text{ if } x \notin D_n$$

$$g(n, x) = 2 \text{ if } x \in D_n$$

is not recursive.

Proof (will lead to the final conclusion): Towards contradiction let $g(n, x)$ be recursive then it would be Diophantine (by Theorem 6.1), say:

$$y = g(n, x) \Leftrightarrow (\exists y_1 \dots y_m) [P(n, x, y, y_1, \dots, y_m) = 0]$$

But then it would follow that

$$V = \{ x \mid (\exists y_1 \dots y_m) [P(x, x, 1, y_1, \dots, y_m) = 0] \}$$

which contradicts Theorem 7.2.

Using Theorem 7.1, write:

$$x \in D_n \Leftrightarrow (\exists z_1, \dots, z_k)[P(n, x, z_1, \dots, z_k) = 0]$$

If there were an algorithm, this algorithm could be used to test whether or not the equation:

$$P(n, x, z_1, \dots, z_k) = 0$$

has a solution, i.e. whether or not $x \in D_n$. Thus *the algorithm could be used to compute the function $g(n,x)$. Since the recursive functions are just those for which a computing algorithm exists, g would have to be recursive. This would contradict with Theorem 7.3, and this contradiction proves:*

Theorem 7.4 Hilbert's 10th problem is unsolvable !!

Open Problems (listed by Yuri Matyasevich)

We can understand Hilbert's 10th problem in two senses:

- the narrow sense, i.e. literally as the problem was stated originally
- the broader sense, including other problems, solutions of which would easily follow from a positive solution of problem as it was stated originally.

Three outstanding mathematical problems:

- Goldbach's Conjecture
- The Riemann hypothesis
- The four color conjecture

each can be restated as an assertion that particular Diophantine equations have no solutions.

THANK YOU FOR YOUR PATIENCE & TIME !

Appendix A. Twenty Four Lemma's for proving "exponentiation is Diophantine"

Given Pell's Equations:

$$x^2 - dy^2 = 1 \quad x, y \geq 0,$$

$$d = a^2 - 1, \quad a > 1$$

- 1- $1 < x + y\sqrt{d} < a + \sqrt{d}$ no such (x, y) exists
- 2- $x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d})$
- 3- $x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$
- 4- If x, y are solutions of Pell then for some n
 $x_n = x, y_n = y \Rightarrow (a + \sqrt{d})^n \leq (x + y\sqrt{d}) < (a + \sqrt{d})^{n+1}$
- 5- $x_{m+n} = x_m x_n + d y_m y_n$
 $y_{m+n} = y_m x_n + x_m y_n$
- 6- $x_{m+1} = x_m x_1 + d y_1 y_m = a y_m + x_m$
 $y_{m+1} = y_m x_1 + x_m y_1 = a x_m + d y_m$
- 7- $\gcd(x_n, y_n) = 1$ relatively prime
- 8- $y_n \mid y_{nk}$
- 9- $y_n \mid y_t \Rightarrow n \mid t$
- 10- $y_{nk} = k \cdot x_n^{k-1} y_n \pmod{(y_n)^3}$
- 11- $(y_n)^2 \mid y_n y_n$ set $Y_n = k,$
- 12- $(y_n)^2 \mid y_t \Rightarrow y_n \mid t$

Second order difference equations

$$13- x_{n+1} = 2a \cdot x_n - x_{n-1}$$

$$y_{n+1} = 2a \cdot y_n - y_{n-1}$$

$$14- y_n \equiv n \pmod{(a-1)}$$

$$\text{from } y_{n+1} = 2a \cdot y_n - y_{n-1}$$

$$n + 1 = 2n - (n-1)$$

15- $a = b \pmod{c}$

$$x_n(a) = x_n(b), y_n(a) = y_n(b) \pmod{c}.$$

16- $n \text{ even} \Rightarrow y_n \text{ even}$

$$n \text{ odd} \Rightarrow y_n \text{ odd}$$

17- $x_n(a) - y_n(a)(a-y) \equiv y_n \pmod{(2a \cdot y^2 - y^2 - 1)}$

18- $y_{n+1} > y_n \geq n$

19- $x_{n+1}(a) > x_n(a) \geq a^n$

20- $x_{2n+j} = -x_j \pmod{x_n}$

21- $x_{4n+j} = x_j \pmod{x_n}$

22- If $x_i = x_j \pmod{x_n}$, $i \leq y \leq 2n$, then $i = j$, unless $i=0, j=2, a=2, n=1$

23- $x_j = x_i \pmod{x_n}$, $0 < i \leq n, 0 < j \leq 4n$, either $j=i$ or $j=4n-i$

24- If $(0 \leq i \leq n \ \& \ x_j = x_i \pmod{x_n}) \Rightarrow (j \equiv i \pmod{4n})$

Appendix B. Solving an arbitrary Diophantine equation can be reduced to solving another Diophantine equation (with the same parameters) of degree D in M unknowns where $\langle D, M \rangle$ is any of the following pairs:

$$\langle 4, 58 \rangle, \langle 8, 38 \rangle, \langle 12, 32 \rangle, \langle 16, 29 \rangle, \langle 20, 28 \rangle, \langle 24, 26 \rangle,$$

$$\langle 28, 25 \rangle, \langle 36, 24 \rangle, \langle 96, 21 \rangle, \langle 2668, 19 \rangle, \langle 2 \times 10^5, 14 \rangle,$$

$$\langle 6.6 \times 10^{43}, 13 \rangle, \langle 1.3 \times 10^{44}, 12 \rangle, \langle 4.6 \times 10^{44}, 11 \rangle, \langle 8.6 \times 10^{44},$$

$$10 \rangle, \langle 1.6 \times 10^{45}, 9 \rangle$$

References

[1] Martin Davis, Hilbert's 10th problem is Unsolvable. The American Mathematical Monthly, 80(3):233-269 [1973].

[2] Yuri Matyasevich, Hilbert's 10th problem, The MIT Press, 1993.

[3] Yuri Matyasevich, Online Lecture and Lecture notes, <http://www.pims.math.ca/science/2000/distchair/matyasevich/lecture1/slide1.html>

[4] Martin Davis, Ron Sigal, Elaine Weyuker, Computability, Complexity and Languages, Academic Press 1994.

[5] Martin Davis, Computability and Unsolvability, McGrawHill 1958

[6] Martin Davis, The Undecidable, Raven Press, 1965.

[7] Martin Davis's Letter, <http://www.math.psu.edu/simpson/fom/postings/9802/msg00112.html>