On the elimination of the bounded universal quantifier for Diophantine predicates

Aran Nayebi
anayebi@stanford.edu

Logic Seminar, Stanford

January 22, 2013

Definitions

- Recall that a *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0, \tag{1}$$

where D is a polynomial with integer coefficients.

Definitions

- Recall that a *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0, \tag{1}$$

where D is a polynomial with integer coefficients.

- We will be concerned with *families* of Diophantine equations, understood as a relation of the form

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0, \tag{2}$$

where $a_1, \ldots, a_n$ are *parameters* and $x_1, \ldots, x_m$ are *unknowns*.

Definitions

- Recall that a *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0, \tag{1}$$

where D is a polynomial with integer coefficients.

- We will be concerned with *families* of Diophantine equations, understood as a relation of the form

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0, \tag{2}$$

where $a_1, \ldots, a_n$ are *parameters* and $x_1, \ldots, x_m$ are *unknowns*.

- For different values of the parameters, one can obtain equations that do have solutions as well as equations that do not.

Definitions

- The parametric equation (2) defines a set $\mathfrak{M}$ consisting of n-tuples of values of the parameters $a_1, \ldots, a_n$ for which there are values of the unknowns $x_1, \ldots, x_m$ satisfying (2):

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Leftrightarrow \exists x_1 \ldots x_m \, [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0].$$

Definitions

- The parametric equation (2) defines a set $\mathfrak{M}$ consisting of n-tuples of values of the parameters $a_1, \ldots, a_n$ for which there are values of the unknowns $x_1, \ldots, x_m$ satisfying (2):

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Leftrightarrow \exists x_1 \ldots x_m \, [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0].$$

- $\mathfrak{M}$ is called a *Diophantine set*, n is called the *dimension* of $\mathfrak{M}$ and above is its *Diophantine representation*.

Basic operations

- The *union* of two Diophantine sets of the same dimension is Diophantine, namely

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) \cdot D_2(a_1, \ldots, a_n, x_1, \ldots, x_{m_2}) = 0,$$

if $D_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) = 0$ and $D_2(a_1, \ldots, a_n, x_1, \ldots, x_{m_2}) = 0$ are Diophantine representations of two sets.

Basic operations

- The *intersection* of two Diophantine sets of the same dimension is Diophantine, namely

$$D_1^2(a_1,\ldots,a_n,x_1,\ldots,x_{m_1})+D_2^2(a_1,\ldots,a_n,y_1,\ldots,y_{m_2})=0,$$

if $D_1(a_1,\ldots,a_n,x_1,\ldots,x_{m_1})=0$ and $D_2(a_1,\ldots,a_n,y_1,\ldots,y_{m_2})=0$ are Diophantine representations of two sets.

Developing a logical language

- Although Diophantine sets, the operations of their unions and intersections, and the relation of set membership are sufficiently expressive, it is often more convenient to use an equivalent language of properties and relations.
- **Example:** Instead of considering the *set* with the representation

$$a - x^2 = 0,$$

we can say that the *property* (over natural numbers) "is a perfect square" is Diophantine.

Developing a logical language

- A relation $\mathcal{R}$ among n natural numbers is called a *Diophantine relation* if the set of all n-tuples for which the relation holds is Diophantine.

Developing a logical language

- A relation $\mathcal{R}$ among n natural numbers is called a *Diophantine relation* if the set of all n-tuples for which the relation holds is Diophantine.
- An equivalence of the form

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \exists x_1, \ldots, x_m \; [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]$$

is called a Diophantine representation of the relation $\mathcal{R}$.

Connectives

- **Disjunction:** If $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine relations then the relation $\mathcal{R}$ such that for all $a_1, \ldots, a_n$

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \mathcal{R}_1(a_1, \ldots, a_n) \vee \mathcal{R}_2(a_1, \ldots, a_n)$$

is also Diophantine.

Connectives

- **Disjunction:** If $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine relations then the relation $\mathcal{R}$ such that for all $a_1, \ldots, a_n$

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \mathcal{R}_1(a_1, \ldots, a_n) \vee \mathcal{R}_2(a_1, \ldots, a_n)$$

  is also Diophantine.
- **Conjunction:** The relation $\mathcal{R}$ such that for all $a_1, \ldots, a_n$

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \mathcal{R}_1(a_1, \ldots, a_n) \wedge \mathcal{R}_2(a_1, \ldots, a_n)$$

  is also Diophantine, provided of course that $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine.

Permitted quantifiers

- Thus, any formula constructed from parametric Diophantine equations by using, in whatever order, disjunction, conjunction, and existential quantification can be regarded as constituting a generalized Diophantine representation.

Permitted quantifiers

- Thus, any formula constructed from parametric Diophantine equations by using, in whatever order, disjunction, conjunction, and existential quantification can be regarded as constituting a generalized Diophantine representation.
- In fact, we can do better and show that the bounded universal quantifier is a part of our language. Namely, if P is a polynomial then the set S such that

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

is Diophantine.

Importance?

- Many number-theoretic properties can be written in the form $\forall n \; P(n)$, where P is a decidable property over natural numbers.

Importance?

- Many number-theoretic properties can be written in the form $\forall n\ P(n)$, where P is a decidable property over natural numbers.
- For example, it is obvious that the set of primes is defined by the formula:

$$a > 1\ \&\ \forall x < a\ \forall y < a\ \exists v\ [(a-(x+2)(y+2))^2 - v - 1 = 0].$$

Importance?

- Many number-theoretic properties can be written in the form $\forall n\ P(n)$, where P is a decidable property over natural numbers.
- For example, it is obvious that the set of primes is defined by the formula:

$$a > 1 \ \&\ \forall x < a\ \forall y < a\ \exists v\ [(a-(x+2)(y+2))^2 - v - 1 = 0].$$

- Other examples include Goldbach's conjecture, Riemann hypothesis, and the four color theorem.

Importance?

- Many number-theoretic properties can be written in the form $\forall n\ P(n)$, where P is a decidable property over natural numbers.
- For example, it is obvious that the set of primes is defined by the formula:

$$a > 1\ \&\ \forall x < a\ \forall y < a\ \exists v\ [(a-(x+2)(y+2))^2 - v - 1 = 0].$$

- Other examples include Goldbach's conjecture, Riemann hypothesis, and the four color theorem.
- An important step towards proving the recursive unsolvability of Hilbert's tenth problem, namely, that every recursively enumerable set is Diophantine.

Eliminating the bounded universal quantifier

- Davis, Putnam, Robinson technique using the Chinese remainder theorem
- Matiyasevich's technique via Turing machines
- Matiyasevich's technique via summations of generalized geometric progressions
- Given the size of the polynomials we will be dealing with, the Davis, Putnam, and Robinson technique is the most useful for our purposes.

Bovykin and De Smet's Project

- A prefixed polynomial equation (or "a polynomial expression with a quantifier prefix") is an equation of the form $P(x_1, \ldots, x_n) = 0$, where the variables $x_1, \ldots, x_n$ range over natural numbers, preceded by quantifiers over some, if not all, of its variables.

Bovykin and De Smet's Project

- Bovykin and De Smet want to study the collection of all prefixed polynomial equations, with the equivalence of relation of being "EFA-provably equivalent" on its members.

Bovykin and De Smet's Project

- Bovykin and De Smet want to study the collection of all prefixed polynomial equations, with the equivalence of relation of being "EFA-provably equivalent" on its members.
- "Probably every theorem published in Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., an arithmetical statement) can be proved in EFA."
  -Friedman

Bovykin and De Smet's Project

- Bovykin and De Smet want to study the collection of all prefixed polynomial equations, with the equivalence of relation of being "EFA-provably equivalent" on its members.
- "Probably every theorem published in Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., an arithmetical statement) can be proved in EFA." -Friedman
- It is not difficult to obtain a prefixed polynomial representation, but the value of such polynomial expressions is that they provide concrete examples of unprovable statements and explicit illustrations of deep logical phenomena.

Paris-Harrington Theorem

- The following combinatorial principle is unprovable in PA:

Paris-Harrington Theorem

- The following combinatorial principle is unprovable in PA:
- $\forall\ e, r, k,\ \exists\ M$, such that for every coloring f of e-subsets of $[M+1] = \{0, 1, \ldots, M\}$ into r colors, there is an f-homogeneous $Y \subseteq [M+1]$ of size at least $\min(Y) + k - 1$.

Paris-Harrington Theorem

- The following combinatorial principle is unprovable in PA:
- $\forall\ e, r, k,\ \exists\ M$, such that for every coloring f of e-subsets of $[M+1] = \{0, 1, \ldots, M\}$ into r colors, there is an f-homogeneous $Y \subseteq [M+1]$ of size at least $\min(Y) + k - 1$.
- First "natural" example of incompleteness in PA. Many others followed.

Unprovability in $I\Sigma_1$

- The following combinatorial principle is unprovable in $I\Sigma_1$:

Unprovability in $I\Sigma_1$

- The following combinatorial principle is unprovable in $I\Sigma_1$:
- $\forall\ k$, $\exists\ M$ such that for every coloring f of 2-subsets of $[M+1] = \{0, \ldots, M\}$ into r colors, there is an f-homogeneous $Y \subseteq [M+1]$ of size at least $\min(Y) + k - 1$.

Unprovability in $I\Sigma_1$

- The following combinatorial principle is unprovable in $I\Sigma_1$:
- $\forall\ k$, $\exists\ M$ such that for every coloring f of 2-subsets of $[M+1] = \{0, \ldots, M\}$ into r colors, there is an f-homogeneous $Y \subseteq [M+1]$ of size at least $\min(Y) + k - 1$.
- We will call this PH^2, as it is a special case of the original Paris-Harrington theorem (Erdös-Mills).

Prefixed polynomial equation for PH^2

- For $r > 2$, (where r is the only free variable which represents the colors), PH^2 is equivalent to the following prefixed polynomial equation (Bovykin and De Smet):

Prefixed polynomial equation for PH^2

- $$\forall k\ \exists M\ \forall ab\ \exists cdAX\ \forall xy\ \exists BCF\ \forall fg\ \exists ehilnpq$$
$$[x \cdot (y + B - x) \cdot (A + k + B - y) \cdot (((((f - A)^2(g - 1)^2)$$
$$\cdot ((f - B)^2 + (g - x)^2) \cdot ((f - C)^2 + (g - y)^2) - h - 1)$$
$$\cdot ((dgi + i - c + f)^2 + (f + h - dg)^2) + (B + l + 1 - C)^2$$
$$+ (C + n - M)^2 + (F + e - b(B + C^2))^2 + (bp(B + C^2)$$
$$+ p - a + F)^2 + ((F - X)^2 - qr)^2)] = 0.$$

Challenges for the Atlas

- Although in the case of PH^2 covers only a few lines, the challenge comes when transforming this polynomial from its Π^0_6 form to its EFA-provably equivalent Diophantine form.

Challenges for the Atlas

- Although in the case of PH^2 covers only a few lines, the challenge comes when transforming this polynomial from its Π^0_6 form to its EFA-provably equivalent Diophantine form.
- Here, bounding the universal quantifiers and then eliminating them introduces a drastic increase in the number of variables of the original prefixed polynomial representation, to the point that the resulting Diophantine form is too long to be practical to write (or include in the Atlas).

Challenges for the Atlas

- Although in the case of PH^2 covers only a few lines, the challenge comes when transforming this polynomial from its Π^0_6 form to its EFA-provably equivalent Diophantine form.
- Here, bounding the universal quantifiers and then eliminating them introduces a drastic increase in the number of variables of the original prefixed polynomial representation, to the point that the resulting Diophantine form is too long to be practical to write (or include in the Atlas).
- Thus, naive attempts to obtain Diophantine representations (namely, a direct application of the results of DPRM and possibly with some slight modifications but with no drastic tricks) for PH^2 (and certainly other unprovable statements) yields unwriteable representations.

Our results

- Our results: A 138 variable exponential Diophantine representation or a 347 variable Diophantine representation.

Our results

- Our results: A 138 variable exponential Diophantine representation or a 347 variable Diophantine representation.
- DPRM method: A 233 variable exponential Diophantine representation or a 1055 variable Diophantine representation.

Our results

- Our results: A 138 variable exponential Diophantine representation or a 347 variable Diophantine representation.
- DPRM method: A 233 variable exponential Diophantine representation or a 1055 variable Diophantine representation.
- Conservation of 95 variables and 708 variables for each case, respectively.

Diophantine coding

- To code a tuple $\langle a_1, \ldots, a_n \rangle$ of *arbitrary* length we use Gödel coding.

Diophantine coding

- To code a tuple $\langle a_1, \ldots, a_n \rangle$ of *arbitrary* length we use Gödel coding.
- If we let $b_1, \ldots, b_n$ be any pairwise coprime numbers such that

$$a_i < b_i, \; i = 1, \ldots, n. \tag{3}$$

Diophantine coding

- To code a tuple $\langle a_1, \ldots, a_n \rangle$ of *arbitrary* length we use Gödel coding.
- If we let $b_1, \ldots, b_n$ be any pairwise coprime numbers such that

$$a_i < b_i, \;\; i = 1, \ldots, n. \tag{3}$$

- By the CRT, we can find a number a such that

$$a_i = \mathrm{rem}(a, b_i), \;\; i = 1, \ldots, n.$$

Diophantine coding

- To code a tuple $\langle a_1, \ldots, a_n \rangle$ of *arbitrary* length we use Gödel coding.
- If we let $b_1, \ldots, b_n$ be any pairwise coprime numbers such that

$$a_i < b_i, \;\; i = 1, \ldots, n. \tag{3}$$

- By the CRT, we can find a number a such that

$$a_i = \mathrm{rem}(a, b_i), \;\; i = 1, \ldots, n.$$

- We will take $b_i = bi + 1$, where b is a multiple of $n!$ large enough to imply the inequalities in (3).

Diophantine coding

- To code a tuple $\langle a_1, \ldots, a_n \rangle$ of *arbitrary* length we use Gödel coding.
- If we let $b_1, \ldots, b_n$ be any pairwise coprime numbers such that

$$a_i < b_i, \;\; i = 1, \ldots, n. \tag{3}$$

- By the CRT, we can find a number a such that

$$a_i = \mathrm{rem}(a, b_i), \;\; i = 1, \ldots, n.$$

- We will take $b_i = bi + 1$, where b is a multiple of $n!$ large enough to imply the inequalities in (3).
- All the elements of $\langle a_1, \ldots, a_n \rangle$ are uniquely determined by $a, b_1, \ldots, b_n$.

PH^2 representation

- Let $[M+1]^2$ represent the set of all the 2-subsets of $[M+1]$. Moreover, $f(\{x_1,\ldots,x_n\})$ will be shortened to $f(x_1,\ldots,x_n)$ with the assumption that the x_i's are increasing.

PH^2 representation

- Let $[M+1]^2$ represent the set of all the 2-subsets of $[M+1]$. Moreover, $f(\{x_1,\ldots,x_n\})$ will be shortened to $f(x_1,\ldots,x_n)$ with the assumption that the x_i's are increasing.
- The main idea is to represent the colorings $f:[M+1]^2 \to r$ as sequences $\langle a_1,\ldots,a_n\rangle$ such that if $h<l\in[M+1]$ and $h+l^2=i$, then
$$a_i \equiv f(h,l) \mod r.$$

PH^2 representation

- Let $[M+1]^2$ represent the set of all the 2-subsets of $[M+1]$. Moreover, $f(\{x_1, \ldots, x_n\})$ will be shortened to $f(x_1, \ldots, x_n)$ with the assumption that the x_i's are increasing.
- The main idea is to represent the colorings $f : [M+1]^2 \to r$ as sequences $\langle a_1, \ldots, a_n \rangle$ such that if $h < l \in [M+1]$ and $h + l^2 = i$, then
$$a_i \equiv f(h, l) \mod r.$$
- Observe that if $h < l$, then the function that associates (h, l) with $h + l^2$ is injective.

PH^2 representation

- Let $[M+1]^2$ represent the set of all the 2-subsets of $[M+1]$. Moreover, $f(\{x_1, \dots, x_n\})$ will be shortened to $f(x_1, \dots, x_n)$ with the assumption that the x_i's are increasing.
- The main idea is to represent the colorings $f : [M+1]^2 \to r$ as sequences $\langle a_1, \dots, a_n \rangle$ such that if $h < l \in [M+1]$ and $h + l^2 = i$, then
$$a_i \equiv f(h, l) \mod r.$$
- Observe that if $h < l$, then the function that associates (h, l) with $h + l^2$ is injective.
- So we use Gödel coding to code the sequence $\langle a_1, \dots, a_n \rangle$ as the pair (a, b) such that
$$a_i = \mathrm{rem}(a, b_i).$$

PH^2 representation

- If (a, b) codes the sequence $\langle a_1, \ldots, a_n \rangle$ such that $n < M + (M+1)^2$, then not all values of possible 2-subsets of $[M+1]$ will be covered. This can be fixed if we extend the sequence by adding a's at the end until the length of the sequence is at least $M + (M+1)^2$.

PH^2 representation

- If (a, b) codes the sequence $\langle a_1, \ldots, a_n \rangle$ such that $n < M + (M+1)^2$, then not all values of possible 2-subsets of $[M+1]$ will be covered. This can be fixed if we extend the sequence by adding a's at the end until the length of the sequence is at least $M + (M+1)^2$.
- This extended sequence now defines a function $f : [M+1]^2 \to r$ as previously described.

PH^2 representation

- If (a, b) codes the sequence $\langle a_1, \ldots, a_n \rangle$ such that $n < M + (M+1)^2$, then not all values of possible 2-subsets of $[M+1]$ will be covered. This can be fixed if we extend the sequence by adding a's at the end until the length of the sequence is at least $M + (M+1)^2$.
- This extended sequence now defines a function $f : [M+1]^2 \to r$ as previously described.
- Observe that the equalities $a_i = \mathrm{rem}(a, bi + 1)$ and $a_i \equiv f(h, l) \mod r$ now hold for all $h < l \in [M+1]$ where $i = h + l^2$.

PH^2 representation

- If (a, b) codes the sequence $\langle a_1, \ldots, a_n \rangle$ such that $n < M + (M+1)^2$, then not all values of possible 2-subsets of $[M+1]$ will be covered. This can be fixed if we extend the sequence by adding a's at the end until the length of the sequence is at least $M + (M+1)^2$.
- This extended sequence now defines a function $f : [M+1]^2 \to r$ as previously described.
- Observe that the equalities $a_i = \mathrm{rem}(a, bi+1)$ and $a_i \equiv f(h,l) \mod r$ now hold for all $h < l \in [M+1]$ where $i = h + l^2$.
- The subset H will be coded as the increasing sequence $\langle c_1, \ldots, c_p \rangle$ such that $c_i \in [M+1]$ for $i = 1, \ldots, p$. This is coded as a pair (c, d) by Gödel coding.

Intermediate representation

- $$\begin{aligned}
&\forall k\ \exists M\ \forall ab\ \exists cdAX\ \forall xy\ \exists BCF \\
&[(0 < x \wedge x < y \wedge y \leq A + k - 1) \rightarrow \\
&(A = \mathrm{rem}(c, d + 1) \wedge B = \mathrm{rem}(c, dx + 1) \wedge C = \mathrm{rem}(c, dy + 1) \\
&\ \wedge B < C \wedge C < M + 1 \wedge F = \mathrm{rem}(a, b(B + C^2) + 1) \\
&\ \wedge F \equiv X \mod r)].
\end{aligned}$$

Intermediate representation

- We will be taking k, M, a, b, r as parameters. Bounding quantifiers we have then that:

Intermediate representation

- We will be taking k, M, a, b, r as parameters. Bounding quantifiers we have then that:
-
$$\exists cdAX\ \forall x \leq A+k-3\ \forall y \leq A+k-2\ \exists BCF$$
$$[x < y \wedge A = \mathrm{rem}(c, d+1) \wedge B = \mathrm{rem}(c, d(x+1)+1)$$
$$\wedge\ C = \mathrm{rem}(c, d(y+1)+1) \wedge B < C$$
$$\wedge\ C < M+1 \wedge F = \mathrm{rem}(a, b(B+C^2)+1) \wedge F \equiv X \mod r].$$

Intermediate representation

- We can reduce the two bounded quantifiers to just one by taking advantage of the fact that if $x \leq A + k - 3$ and $y \leq A + k - 2$, then $J(x, y) \leq J(A + k - 3, A + k - 2)$, where J is Cantor's function defined for natural numbers m and n as $J(m, n) = (m + n)(m + n + 1)/2$.

Intermediate representation

- We can reduce the two bounded quantifiers to just one by taking advantage of the fact that if $x \leq A + k - 3$ and $y \leq A + k - 2$, then $J(x, y) \leq J(A + k - 3, A + k - 2)$, where J is Cantor's function defined for natural numbers m and n as $J(m, n) = (m + n)(m + n + 1)/2$.
- The elimination of the final single bounded universal quantifier then gives us the desired exponential Diophantine representation in 138 variables.

Selected References

- Andrey Bovykin. "A brief introduction to unprovability". http://www.maths.bris.ac.uk/~maaib//new.pdf.
- Andrey Bovykin and Michiel De Smet. "A study of the Atlas of all possible polynomial equations with quantifier-prefixes and the structure of provable-equivalence classes". http://logic.pdmi.ras.ru/~andrey/baby/baby_project.pdf. (Somewhat outdated)
- Paul Erdös and George Mills. "Some bounds for the Ramsey-Paris-Harrington numbers". *J. Comb. Theory Ser. A* **30** (1981): 53-70.
- Yuri Matiyasevich. "Hilbert's Tenth Problem." MIT Press. 1993.