On Diophantine Complexity

and

Statistical Zero-Knowledge Arguments

Helger Lipmaa
Helsinki University of Technology
http://www.tcs.hut.fi/~helger

Overview of This Talk

- Diophantine complexity: definitions
- Noncryptographic result: bounded arithmetic is in $\mathbf{PD}$
- Cryptographic applications:
  - ⋆ Diophantine HVSZK arguments
  - ⋆ “Outsourcing” model

This paper has too many results to even mention all of them in the presentation!

Overview of This Talk

- Diophantine complexity: definitions
- Noncryptographic result: bounded arithmetic is in $\mathbf{PD}$
- Cryptographic applications:
  - ⋆ Diophantine HVSZK arguments
  - ⋆ “Outsourcing” model

Hilbert's 10th Problem

- Hilbert, 1900: find an algorithm that, given a polynomial f, returns its integral solutions

- Solved negatively by Davis, Putnam, Robinson and Matiyasevich (1952...1970) by showing that for any recursively enumerable set $S \subseteq \mathbb{Z}^n$ there exists a representing polynomial $\mathfrak{R}_S \in \mathbb{Z}[X, Y]$, s.t.

$$\mu \in S \iff (\exists \omega \in \mathbb{Z}^m)[\mathfrak{R}_S(\mu; \omega) = 0] \ .$$

- Set S is called *Diophantine* if it has such a representing polynomial. Thus every r.e. set is Diophantine.

Example: Primality

Jones etc:

- Constructed a representing polynomial $\mathfrak{R}_{\mathsf{Primes}} \in \mathbb{Z}[X, Y]$, s.t.

$$\mu \in \mathsf{Primes} \iff (\exists \omega \in \mathbb{Z}^{26})[\mathfrak{R}_S(\mu; \omega) = 0] \ .$$

- However, some of the witnesses are either hard to compute or plainly too long

Diophantine Theory: Nice But Nonpractical

- Positive: there are representing polynomials for any r.e. set
  - ⋆ There is also a “universal” polynomial (similar to the universal TM)
- Negative: the witnesses have nonpractical length or are difficult to compute
- A really nice area of mathematics (full of real gems)...
- ...without almost any practical applications

Adleman-Manders's Conjecture: Step to Practicality

- Adleman-Manders 1976: Define the complexity class $\mathbf{D}$ as follows: $S \in \mathbf{D}$ iff there exists a representing polynomial $\mathfrak{R}_S \in \mathbb{Z}[X, Y]$, s.t.

$$\mu \in S \iff (\exists \omega \in \mathbb{Z}^m)[\mathfrak{R}_S(\mu; \omega) = 0 \ \wedge \ |\omega| = \mathsf{poly}(|\mu|)] \ .$$

- Clearly, a much more "applicable" (and restricted class) than r.e. (See [AM76] for possible applications.)

- Adleman-Manders conjecture (76): $\mathbf{D} = \mathbf{NP}$

- A conjecture that is believed to be true but not much is known about the power of $\mathbf{D}$

Overview of This Talk

- Diophantine complexity: definitions
- Noncryptographic result: bounded arithmetic is in $\mathbf{PD}$
- Cryptographic applications:
  - ⋆ Diophantine HVSZK arguments
  - ⋆ “Outsourcing” model

Let's Get Really Practical

- Assume that there is an efficient witness algorithm $\mathfrak{P}_S$, so that

$$\mu \in S \Rightarrow \mathfrak{R}_S(\mu; \mathfrak{P}_S(\mu)) = 0 \ ,$$

and

$$\mu \notin S \Rightarrow (\neg\exists\omega)[\mathfrak{R}_S(\mu;\omega) = 0 \wedge |\omega| = \mathsf{poly}(|\mu|)] \ .$$

Then we say that $S \in \mathbf{PD}$

- Interested in the case when $|\omega|$ is *sub-quadratic* in $|\mu|$

- Which languages in $\mathbf{PD}$ are guaranteed to have $|\mathfrak{P}_S(\mu)| = |\mu|^{2-o(1)}$?

More Background: Bounded Arithmetic

- Bounded arithmetic is a first-order theory of the natural numbers with non-logical symbols

$$0, \sigma, +, \cdot, \leq, \dot{-}, \lfloor x/2 \rfloor, |x|, \mathsf{MSP}(x, i), \sharp \ .$$

- Here, $\sigma(x) = x + 1$, $x \dot{-} y = \max(x - y, 0)$, $|x| = \lfloor \log_2(x + 1) \rfloor$, $\mathsf{MSP}(x, i) = \lfloor x/2^i \rfloor$, $x \sharp y = 2^{|x| \cdot |y|}$

- We assume that the underlying domain is $\mathbb{Z}$ (and not $\mathbb{N}$)

- Let L_2 be the set of terms of the quantifier-free bounded arithmetic (over $\mathbb{Z}$)

More Background: Bounded Arithmetic

- Some predicates in bounded arithmetic: $[\mu_1 > \mu_2]$, $[\mu$ is a perfect square$]$, $[\mu_2 = \mathsf{bit}(\mu_1, i)]$, $[\mu_1 = \mathsf{max}(\mu_2, \mu_3)]$, $[\mu_1$ is not a power of $2]$, ...

- A relatively small set of languages that contains however sufficiently many arithmetic and number-theoretic predicates

- Pollet 2003: bounded arithmetic is in $\mathbf{D}$

Main Result: Bounded Arithmetic is in $\mathbf{PD}$

Theorem. Bounded arithmetic is in $\mathbf{PD}$, with $|\omega| = |\mu|^{2-o(1)}$.

Proof. By induction on length of structure of the term. For example,

$$[\mu_2 = \lfloor \mu_1/2 \rfloor] \equiv [(\mu_2 = 2\mu_1) \vee (\mu_2 = 2\mu_1 + 1)] \ .$$

The proof follows from the two nontrivial theorems that construct representing polynomials (and witness algorithms) for nonnegativity and exponential relationship.

Efficient Witness Algorithm for Nonnegativity

- Lagrange 1770: $\mu \geq 0$ iff $\mu = \omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2$ for $\omega_i \in \mathbb{Z}$
- Thus $\mathbb{N}_0 \in \mathbf{D}$ with $|\omega| = \Theta(|\mu|)$
- Rabin, Shallit 1986: corresponding ω_i can be found in probabilistic polynomial time
- Thus $\mathbb{N}_0 \in \mathbf{PD}$
- This paper: slight improvement over Rabin-Shallit (a slightly faster algorithm for computing ω_i)

Exponential Relation is in $\mathbf{PD}$

- Matiyasevich 1970: e.r. has representing polynomial
- Adleman-Manders 1976: e.r. is in $\mathbf{PD}$
- Current paper: more efficient representing polynomial for the exponential relation

Theorem Assume $\mu_1 > 1$, $\mu_3 > 0$ and $\mu_2 > 2$. The exponential relation $[\mu_3 = \mu_1^{\mu_2}]$ belongs to $\mathbf{PD}$. More precisely, let $E(\mu_1, \mu_2, \mu_3)$ be the next equation:

$$
\begin{aligned}
&[(\exists \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6)(\exists_b \omega_7, \omega_8)] \\
&\quad [(\omega_2 = \omega_1 \mu_1 - \mu_1^2 - 1) \wedge (\omega_2 - \mu_3 - 1 \geq 0) \wedge && (E1 - E2) \\
&\quad (\mu_3 - (\mu_1 - \omega_1)\omega_7 - \omega_8 = \omega_2 \omega_3)) \wedge (\omega_1 - 2 \geq 0) \wedge && (E3 - E4) \\
&\quad ((\omega_1 - 2)^2 - (\mu_1 + 2)(\omega_1 - 2)\omega_5 - \omega_5^2 = 1) \wedge && (E5) \\
&\quad (\omega_1 - 2 = \mu_2 + \omega_6(\mu_1 + 2)) \wedge (\omega_7 \geq 0) \wedge (\omega_7 < \omega_8) \wedge && (E6 - E8) \\
&\quad (\omega_7^2 - \omega_1 \omega_7 \omega_8 - \omega_8^2 = 1) \wedge (\omega_7 = \mu_2 + \omega_4(\omega_1 - 2)] \ , && (E9 - E10)
\end{aligned}
$$

where "$\exists_b$" signifies a bounded quantifier in the following sense: if $\mu_3 = \mu_1^{\mu_2}$ then $E(\mu_1, \mu_2, \mu_3)$ is true with $|\omega| = \Theta(\mu_2^2 \log \mu_1) = o(|\mu|^2)$. On the other hand, if $\mu_3 \neq \mu_1^{\mu_2}$ then either $E(\mu_1, \mu_2, \mu_3)$ is false, or it is true but the intermediate witnesses ω_7 and ω_8 have length $\Omega(\mu_3 \log \mu_3)$, which is equal to $\Omega(2^{|\mu|} \cdot |\mu|)$ in the worst case.

16 additional witnesses are hidden in 4 inequalities

Overview of This Talk

- Diophantine complexity: definitions
- Noncryptographic result: bounded arithmetic is in $\mathbf{PD}$
- Cryptographic applications:
  - ⋆ Diophantine HVSZK arguments
  - ⋆ “Outsourcing” model

Integer commitment schemes

- Integer commitment scheme [FO97,DF02]: a function $C(\mu; \rho)$, $\mu \in \mathbb{Z}$, that has the next two properties:
  - ⋆ Statistically hiding: for any $\mu_1, \mu_2 \in \mathbb{Z}$, the distributions $C(\mu_1; \cdot)$ and $C(\mu_2; \cdot)$ are statistically close
  - ⋆ Computationally binding: for any μ_1, it is hard to find an *integer* $\mu_2 \neq \mu_1$, ρ_1 and ρ_2, such that $C(\mu_1; \rho_1) = C(\mu_2; \rho_2)$
- A nonstandard primitive that has many applications...

Diophantine SZK arguments

- Goal: show that a committed integer tuple $\mu = (\mu_1, \ldots, \mu_n)$ belongs to set S, where S belongs to bounded arithmetic

- Method: Let C be an integer commitment scheme. Then

  1. Apply $\mathfrak{P}_S(\mu)$ to find $\omega = (\omega_1, \ldots, \omega_m)$, s.t. $\mathfrak{R}_S(\mu; \omega) = 0$

  2. Commit to ω_i, and send the commitments to the verifier

  3. Argue by using the methodology of Fujisaki and Okamoto that $\mathfrak{R}_S(\mu; \omega) = 0$

- Results in practical *statistical ZK arguments* for all languages in bounded arithmetic

Example: Nonnegativity

- Goal: for a committed integer μ, argue that $\mu \geq 0$

  1. Find $(\omega_1, \ldots, \omega_4)$ s.t. $\sum \omega_i^2 = \mu$
  2. Commit to ω_i and send commitments to the verifier
  3. Argue in SZK that $\mu = \sum \omega_i^2$

- This argument system is slightly shorter than Boudot's (Eurocrypt 2000), conceptually much simpler and perfectly complete

- ZK argument for nonnegativity has many cryptographic applications

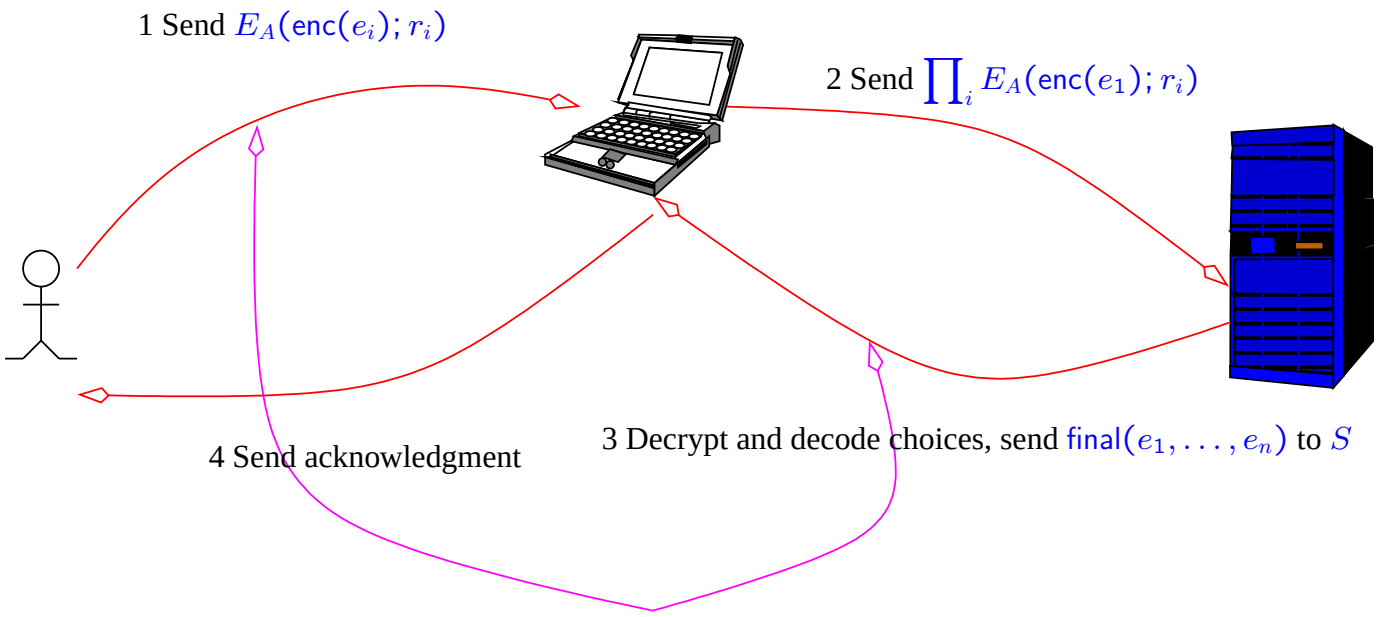
Outsourcing model

- n individuals, 1 interested third party S, one established authority A.
- Individual i has input e_i, her financial or social choice (vote, bid, ...).
- Security: S gets to know $y := \mathsf{final}(e_1, \ldots, e_n)$ for some destination function final.
- Privacy: S will not get any information that cannot be computed from y alone. Individuals will not get any new information at all. A can get to know the vector $(e_1, \ldots, e_n)$.

Why makes sense?

- In voting, it is better to have one tallier: in real life, very hard to have a multiple of completely independent talliers.
- Same in auctions: there is a single seller, all servers are operated by him; why should we trust m machines controlled by the same person more than just one machine, controlled by him?
- OTOH: A can be an established authority who has a reputation to take care off; often S is an occassional party.
- It is also possible to design the system so that we can avoid the limitations of the two-party and multi-party computations, *efficiently*

Outsourcing model: picture



Add SZK correctness arguments for $\mathsf{enc}()$ and final

Details

- There exist $\mathsf{enc}(\cdot)$ in bounded arithmetic and $\mathsf{dec}(\cdot)$, such that $\mathsf{dec}(\sum \mathsf{enc}(e_i)) = (e_1, \ldots, e_n)$ for all e_1 from $[0, V-1]$ and that the corresponding SZK argument is efficient

- Common choice: $\mathsf{enc}(e_i) = V^{e_i}$; $\mathsf{dec}(b)$ returns the vector of V-radix positions of b

- Our proposal: use $\mathsf{enc}(e_i) = Z_V(e_i)$, where $Z_V(e_i)$ is an element of a certain Lucas sequence. Results in more efficient SZK arguments than $\mathsf{enc}(e_i) = V^{e_i}$

- Many cryptographic protocols (voting, auctions, voting with minimal disclosure, ...) can be implemented by using final that belong to bounded arithmetic

Conclusions

- Showed that most of the necessary arguements in this model can be obtained efficiently by using integer commitment schemes
- New algorithm for Lagrange representation, new polynomial for the exponential relationship
- Argued for the outsourcing model for cryptographic protocols
  - ⋆ No threshold trust, efficient arguments of knowledge
  - ⋆ More efficient versions of [DJ01] voting protocol and [LAN02] auction protocol
- Proposed to use Lucas sequences in the SZK arguments

Questions?

?