Syntactic Methods in Solving Linear Diophantine Equations

Presenter: Dmitry G. Korzun

Department of Computer Science

University of Petrozavodsk

Contents of the Presentation

1. **Introduction to NLDE**
   - What is NLDE? (**N**onnegative **L**inear **D**iophantine **E**quation)
   - Hilbert basis
   - Problem of solving NLDE, the complexity
2. **NLDE and Syntactic Analysis**
   - Interrelationship
   - Associated NLDE systems (ANLDE systems)
   - Solutions of ANLDE and Derivations in a grammar
3. **Syntactic solvers**
   - Algorithms
   - Complexity
   - Web-SynDic system

What is Nonnegative Linear Diophantine Equation (NLDE)?

n **equations,** m **unknowns:** $\boxed{Ax = b}$ $\quad A \in \mathbb{Z}^{n\times m},\ b \in \mathbb{Z}^n,\ x \in \mathbb{Z}^m$

$$\begin{cases} a_{11}x_1 + \cdots + a_{1m}x_m = b_1 \\ \quad\cdots \\ a_{n1}x_1 + \cdots + a_{nm}x_m = b_n \end{cases}$$

Diophantness: solutions are integer, $x_i \in \{0,1,2,\ldots\} = \mathbb{Z}_+$

Nonnegativness: solutions are nonnegative, $x_i \geq 0$

Example:

$$\begin{cases} x_1 - x_2 + 3x_3 = 1 \\ x_1 + 2x_2 - x_4 = -1 \end{cases} \qquad \begin{cases} x_1 - x_2 + 3x_3 = 0 \\ x_1 + 2x_2 - x_4 = 0 \end{cases}$$

$$x = \begin{pmatrix} 2 \\ 4 \\ 1 \\ 11 \end{pmatrix} \qquad h = \begin{pmatrix} 1 \\ 4 \\ 1 \\ 9 \end{pmatrix}$$

Hilbert basis of NLDE system

Consider NLDE system: $Ax = b$. There exist finite sets $\mathcal{N}$ and $\mathcal{H}$:

$$\mathcal{N} = \{x^{(1)}, x^{(2)}, \ldots, x^{(p)}\}, \quad \mathcal{H} = \{h^{(1)}, h^{(2)}, \ldots, h^{(q)}\}$$

$$\boxed{\mathcal{S} = \mathcal{N} + \mathcal{H}^*}$$

$$x \in \mathcal{S} \iff x = x^{(l)} + \alpha_1 h^{(1)} + \cdots + \alpha_q h^{(q)} = x^{(0)} + \sum_{s=1}^{q} \alpha_s h^{(s)}$$

for some $x^{(l)} \in \mathcal{N}$ and $\alpha_s \in \mathbb{Z}_+$

Solution x is *minimal* if there is no solution x' such that $x' \leq x$ (component-wise partial order: $x'_i \leq x_i$, $i = 1,2,\ldots,m$)

$\mathcal{N}$	all minimal solutions of $Ax = b$,
$\mathcal{H}$	all minimal solutions of $Ax = 0$ (homogenous system),
$\mathcal{H}^*$	all solutions of the homogenous system,
$\mathcal{N} + \mathcal{H}^*$	all solutions of the original system

An Example

NLDE system of 2 equations in 4 unknowns and its homogenous case:

$$\begin{cases} x_1 - x_2 + 3x_3 = 1 \\ x_1 + 2x_2 - x_4 = -1 \end{cases} \qquad \begin{cases} x_1 - x_2 + 3x_3 = 0 \\ x_1 + 2x_2 - x_4 = 0 \end{cases}$$

$$\mathcal{N} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 5 \end{pmatrix} \right\}, \quad \mathcal{H} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 1 \\ 6 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 2 \\ 4 \\ 1 \\ 11 \end{pmatrix} = \underset{\mathcal{N}}{\underset{\Cap}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \end{pmatrix}}} + \underset{\mathcal{H}^*}{\underset{\Cap}{\begin{pmatrix} 1 \\ 4 \\ 1 \\ 9 \end{pmatrix}}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 3 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 3 \\ 1 \\ 6 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 5 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 3 \end{pmatrix}$$

Problem of Solving NLDE

Solvability: has NLDE a solution?

Particular solution: find a solution

Hilbert basis:

- search the basis
- how many elements in the basis?
- given solution = a basis solution ?
- given set of solutions = Hilbert basis?
- ...

Complexity of Solving NLDE

The source of a rich family of complexity problems

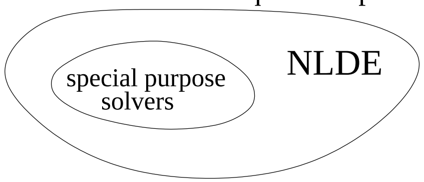
Solvability & Particular solution: has NLDE a solution? find a solution

- Polynomial for homogenous NLDE
- NP-complete in general case

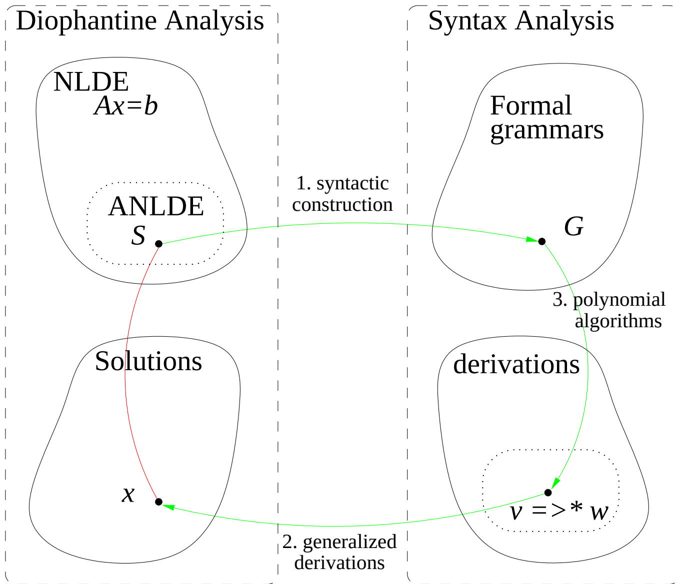
Hilbert basis: over-NP in general case

- search the basis — $|\mathcal{H}|$ depends exponentially on size (n, m, $||A, b||$)
- how many elements in the basis? — #P-hard and in #NP
- given solution = a basis solution? — coNP-complete
- given set of solutions = Hilbert basis? — is the set is basis of some NLDE system?

Universal solvers are not adequate for practical use!



Interrelationship: NLDE ↔ Formal grammars



Associated with formal grammar ANLDE system

Grammar G and strings v, w
m rules (r_i)
n nonterminals (A_k)
t terminals (a_k)

Derivation in G
$v \Rightarrow^* w$

ANLDE system $Ax = b$
m unknowns (x_i)
$n + t$ equations (k)

Solutions
$x \in \mathbb{Z}_+^m$

x — the number of applications of grammar rules in $v \Rightarrow^* w$

A — rules structure (occurrences of symbols)

b — v, w structure (occurrences of symbols)

Associated with formal grammar ANLDE system

$$\sum_{i=1}^{m} \mathrm{occ}(U, \mathrm{lhs}(r_i)) x_i - \sum_{i=1}^{m} \mathrm{occ}(U, \mathrm{rhs}(r_i)) x_i = \mathrm{occ}(U, v) - \mathrm{occ}(U, w) \ , \quad U \in N \cup T$$

$\mathrm{occ}(U, \alpha)$	number of occurrences of symbol U in string α
$\mathrm{lhs}(r)$ or $\mathrm{rhs}(\mathrm{r})$	left or right hand side of rule r

$r_1: \ A \to AAB$
$r_2: \ A \to BB$
$r_3: \ B \to AAAB$
$r_1: \ B \to \varepsilon$

$m = 4$, $n = 2$, $t = 0$
$v = B$, $w = A$
$B \Rightarrow^* A$?
(hom: $A \Rightarrow^+ A$ and $B \Rightarrow^+ B$)

$$A: \ (x_1 + x_2) - (2x_1 + 3x_3) = -1$$
$$B: \ (x_3 + x_4) - (x_1 + x_2 + x_3) = 1$$

$x = (0, 2, 1, 5)$: $\quad B \overset{3}{\Rightarrow} AAAB \overset{4}{\Rightarrow} AAA \overset{2,2}{\Rightarrow} ABBBB \overset{4,4,4,4}{\Rightarrow} A$

$x = (1, 0, 0, 2)$: $\quad BA \overset{1}{\Rightarrow} BAAB \overset{4,4}{\Rightarrow} AA$

$h = (1, 1, 0, 3)$: $\quad A \overset{1}{\Rightarrow} AAB \overset{2}{\Rightarrow} ABBB \overset{4,4,4}{\Rightarrow} A$

Solutions and Derivations

[standard derivation $v \Rightarrow^* w$] $\rightarrow$ (by construction) $\rightarrow$ / $\leftarrow$ (?) $\leftarrow$ [solution $x \in \mathbb{Z}_+^m$]

[generalized derivation $\widetilde{v} \Rightarrow^* \widetilde{w}$] $\longleftrightarrow$ [solution $x \in \mathbb{Z}_+^m$]

Three-component solution:

$$x = x^{v,w'} + x^{w \setminus w'} + x^{\varepsilon}$$

Generalized derivation:

$$\begin{array}{ccccccc} \widetilde{v} & = & v & + & v' & + & v^{\varepsilon} \\ & & \Downarrow & & \Downarrow & & \Downarrow \\ \widetilde{w} & = & w' & + & (v' + w \setminus w') & + & v^{\varepsilon} \end{array}$$

Homogenous ANLDE Systems

$$\sum_{i \in H_k} x_i = \sum_{i=1}^{n} \gamma_{ki} x_i \ , \quad k = 1, 2, \ldots, n \ , \quad I_1 \cup \ldots \cup I_n = \{1, 2, \ldots, m\}$$

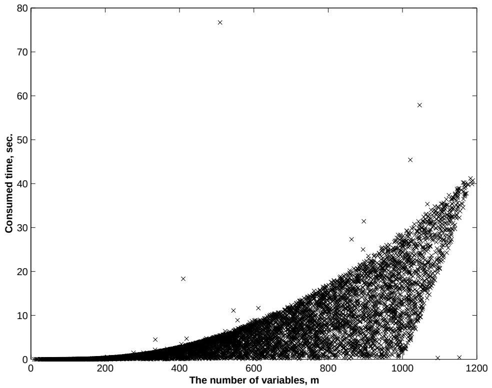
Polynomial complexity ($n \leq m$)**:**

	Hilbert basis	Particular solution
Time	$O(q^3 m^2 n^2) = O(q^3 m^4)$	$O(m^2 n^2) = O(m^4)$
Space	$O(qmn) = O(qm^2)$	$O(mn^2) = O(m^3)$

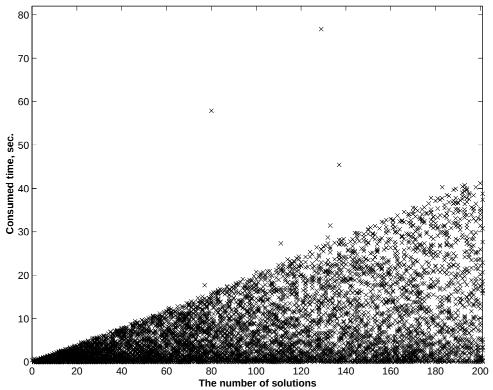
Experimentally: time is $\Theta(qm^2)$ in the most test cases

- more than 1 billion of test ANLDE systems
- coefficients γ_{ki}: $..10^5$
- unknowns and equations: $..10^3$

Experimental plots



Experimental total time complexity as a function on the number of unknowns



Experimental total time complexity as a function on the number of solutions

The dimensions of the generated systems were in range: $n \in [1, 1000]$, $m \in [n, n + 200]$, $\gamma_{ki} \in [0, 500]$. The systems were generated in such a way that each of them has at least one basis solution but not more than 200.

Experimental analysis and testing

1. Think up an ANLDE system and solve it estimating the resources (time&space), test the found solution
2. Construct a generator, generate a system and its solution, . . . , compare the found and original solutions
3. Compare the results with an alternative solver
4. More detailed analysis needs not a system, but a set of them: generate a set and analyze how the solver solves all the systems

COMBINE THESE FEATURES TOGETHER,

MOVE THIS TO THE WEB SPACE . . .

AND YOU GET **THE WEB-SYNDIC** SOFTWARE SYSTEM

Conclusion

THE WEB-SYNDIC SYSTEM IS A TOPIC TO TALK FOR THE NEXT PRESENTATION . . .

Thank you!

Any questions?