Polynomial Generators of Recursively Enumerable Languages

Juha Kortelainen

Department of Information Processing Science
University of Oulu

9th International Conference
Developments in Language Theory
July 4-8, 2005, Mondello, Italy

Outline

Simple Generators of the Family $\mathcal{L}_{RE}$

We study languages L that are

- generators of $\mathcal{L}_{RE}$ with respect to the full AFL operations and intersection (i.e., $\mathcal{L}_{RE} = \hat{\mathcal{F}}_{\cap}(L)$); and
- of the type $L = \{a^{P(n)} \mid n \in \mathbb{N}\}$ where P is a polynomial of n with nonnegative integer coefficients;

In the 1970's

- Hartmanis J. and Hopcrroft J. (1970) [4]: $\mathcal{L}_{RE} = \hat{\mathcal{F}}_{\cap}(DUP)$ where $DUP = \{a^n b^n \mid n \in \mathbb{N}\}$.
- Ginsburg S. and Goldstine J. (1973) [3]:
  1. $\mathcal{L}_{RE} \subseteq \hat{\mathcal{F}}_{\cap}(L)$ for each infinite language $L = \{a^{n_i} \mid i \in \mathbb{N}\}$ such that
  $$lim\ inf_{i \to \infty} \frac{n_{i+1}}{n_i} > 1 \text{ ; and}$$
  2. $\mathcal{L}_{RE} \not\subseteq \hat{\mathcal{F}}_{\cap}(L)$ for each language $L \subseteq a^*$ such that
  $$lim_{n \to \infty} \frac{|\{a^i \mid a^i \in L, 0 \leq i < n\}|}{n} = 1 .$$

In the 1980's

Turakainen P. (1981) [6]:

- the smallest intersection closed full trio generated by $PROD = \{a^n b^n c^{n\,m} | n, m \in \mathbb{N}\}$ (denoted by $\hat{\mathcal{C}}_\cap(PROD)$) contains all recursively enumerable one-letter languages
- for the sets $REP = \{(a^n b)^m |\ n, m \in \mathbb{N}\}$ and $BREP = \{(a^n b)^n |\ n \in \mathbb{N}\}$ the following inclusion relations hold

$$\hat{\mathcal{C}}_\cap(DUP) \subsetneq \hat{\mathcal{C}}_\cap(PROD) \subsetneq \hat{\mathcal{C}}_\cap(BREP) \subseteq \hat{\mathcal{C}}_\cap(REP)$$

Definitions

- A (*full*) *trio* is a family of languages closed under nonerasing morphism (arbitrary morphism), inverse morphism and intersection with regular sets
- A (*full*) *AFL* (acronym for Abstract Family of Languages) is a (full) trio closed under union, concatenation and Kleene+

Notations

For each language L, let

- $\mathcal{C}_\cap(L)$ be the smallest intersection-closed trio;
- $\mathcal{F}_\cap(L)$ be the smallest intersection-closed AFL;
- $\hat{\mathcal{C}}_\cap(L)$ be the smallest intersection-closed full trio; and
- $\hat{\mathcal{F}}_\cap(L)$ be the smallest intersection-closed full AFL

containing (or generated by) the language L

Facts:

- each (full) trio is closed under union with e-free regular sets

Main Results

We show that

- $\mathcal{L}_{RE} = \hat{\mathcal{F}}_{\cap}(P_k)$ for all $k \geq 2$ where $P_k = \{a^{n^k} | n \in \mathbb{N}\}$ (i.e., for all $k \geq 2$, the family of all recursively enumerable languages coincides with the smallest intersection-closed full AFL generated by the polynomial language P_k)
- REP is in $\hat{\mathcal{C}}_{\cap}(BREP)$ (thus $\hat{\mathcal{C}}_{\cap}(BREP) = \hat{\mathcal{C}}_{\cap}(REP)$)

Celebrated Results from Number Theory I

- Wiles, A. (1995) [7] (Fermat's Last Theorem): The Diophantine equation $x^n + y^n = z^n$ has no solutions in nonzero integers x, y and z when n is an integer greater than 2.
- Darmon, H. and Merel, L. (1997) [2]: The Diophantine equation $x^n + y^n = 2\,z^n$ has no solutions in integers x, y and z such that $x \neq y$ when n is an integer greater than 2.
- Nagell, T. (1951) [1]: Parametric solutions to Diophantine equations of the type $a\,x^2 + b\,y^2 = c\,y^2$.

Celebrated Results from Number Theory II

Nagell's parametric solutions to Diophantine equations of the type $a\,x^2 + b\,y^2 = c\,y^2$ imply that the only nonnegative integer solutions of the system

$$\begin{cases} x^2 + y^2 = 2\,z^2 \\ x^2 + 2\,y^2 = 3\,u^2 \end{cases} \tag{1}$$

are $x = y = z = u$.

The Role of *DUP*

- The result of Hartmanis J. and Hopcrroft J. [4] imply that $\mathcal{L}_{RE} \subseteq \hat{\mathcal{F}}_{\cap}(L)$ if and only if $DUP \in \hat{\mathcal{F}}_{\cap}(L)$
- Applying the opertions morphism, inverse morphism and intersection we show the following:
  1. the result of Darmon and Merel implies that $DUP \in \mathcal{C}_{\cap}(P_k)$ for $k > 2$; and
  2. the fact that the only nonnegative integer solutions of the system (1) are $x = y = z = u$ implies that $DUP \in \mathcal{C}_{\cap}(P_2)$

$DUP \in \mathcal{C}_\cap(P_k)$ for $k > 2$

Let $k > 2$. Then (by applying suitable morphisms, inverse morphisms and intersection) we see that the languages

- $T_k = \{a^{2^{n^k}} \mid n \in \mathbb{N}\}$
- $B_k = \{w \in \{a,b\}^* \mid \exists m,n \in \mathbb{N}: \ |w|_a = m^k, \text{ and } |w|_b = n^k\}$
- $Q_k = \{w \in \{a,b\}^* \mid \exists n \in \mathbb{N}: \ |w|_a = |w|_b = n^k\}$

are all in $\mathcal{C}_\cap(P_k)$. Certainly DUP is in $\in \mathcal{C}_\cap(Q_k)$ and thus in $\mathcal{C}_\cap(P_k)$.

Open Problems I

Conjectures

- For each $k \geq 2$ the language family $\hat{\mathcal{C}}_{\cap}(P_k)$ does not contain all recursively enumerable one-letter languages.
- The language *PROD* is not in $\hat{\mathcal{C}}_{\cap}(P_k)$ for any integer $k \geq 2$.
- For each pair of integers $j, k \geq 2$ such that $j \neq k$, the language families $\hat{\mathcal{C}}_{\cap}(P_j)$ and $\hat{\mathcal{C}}_{\cap}(P_k)$ are incomparable, i.e., neither $\hat{\mathcal{C}}_{\cap}(P_j) \subseteq \hat{\mathcal{C}}_{\cap}(P_k)$ nor $\hat{\mathcal{C}}_{\cap}(P_k) \subseteq \hat{\mathcal{C}}_{\cap}(P_k)$ holds.
- For each pair of integers $j, k \geq 2$ such that $j \neq k$, we have $\hat{\mathcal{C}}_{\cap}(P_j) \cap \hat{\mathcal{C}}_{\cap}(P_k) = \hat{\mathcal{C}}_{\cap}(DUP)$.

Open Problem

- Is the language family $\hat{\mathcal{C}}_{\cap}(BREP) = \hat{\mathcal{C}}_{\cap}(REP)$ a proper subset of $\mathcal{L}_{RE}$?

References I


Nagell T., *Introduction to Number Theory*, Almqvist & Wiksell, Stockholm, John Wiley & Sons, New York (1951).


Darmon H., Merel L., Winding quotients and some variants of Fermat's Last Theorem, *Journal für die reine und angewandte Mathematik* 490 (1997), 81-100.


Ginsburg S., Goldstine J., Intersection-closed full AFL and the recursively enumerable languages, *Information and Control* 22 (1973), 201-231.


Hartmanis J., Hopcrroft J., What makes some language theory problems undecidable?, *Journal of Computer and System Sciences* 4 (1970), 368-376.

References II


Kortelainen J., On Language Families Generated by Commutative Languages, Annales Academiae Scientiarum Fennicae Series A I. Mathematica Dissertationes 44, Helsinki, 1982.


Turakainen P., On some bounded semiAFLs and AFLs, *Information Sciences* 23 (1981), 31-48.


Wiles A.,Modular elliptic-curves and Fermat's Last Theorem, *Annals of Mathematics* 141 (1995), 443-551.