BULLETIN

of the

European Association for Theoretical Computer Science

EATCS

Number 12 October 1980

Example: Consider the four state mouse whose program is described by: $q_0 \xrightarrow{E} q_1 \xrightarrow{N} q_2 \xrightarrow{N} q_3 \xrightarrow{N} q_0$; the essential states are q_0 and q_3 ; one has $V = 3$, $H = 1$, so $c = 2$, $b = 1$, and $y_0 = 0$, $y_1 = 1$. This example yields the recurrence sequence whose initial fragment was given above.

Discussion: One might compare the problem above to the problem about the Collatz "even-odd" game : define the function g by :

g(n) = if even n then n/2 else 3n+1 fi ;

It is an open conjecture that for each n there exists a k such that iterating g for k times on input n will transform n into 1 :

$g^k(n) = 1$.

J.H. Conway has shown that some generalisation of this type of iterations leads to an undecidable problem. If one considers functions g defined by

$$g(n) = a_{n \bmod q} * n + b_{n \bmod q}$$

where a_i and b_i are rational numbers selected in such a way that g(n) is integral for each value of n, then the problem of deciding whether $g^k(n) = 1$ for some k becomes undecidable; this holds even for the case that all $b_i = 0$; the proof uses an encoding of a Minsky machine, whose register contents together with its memory state are encoded by exponents in the prime factorisation of the argument n . (for this reduction it is even crucial that the b_i are zero !).

The sequences arising out of the Mouse-in-first-Octant-problem are in one aspect more restricted than the sequences considered by Conway - the multiplier a_i is a fixed number which is moreover larger than 1 ; however we have the new effect of the finite memory (state q_i) which influences the additive terms b_i , and which is in its turn determined by the residue class mod c of the sum of all previous values in the sequence. Will it still be possible to encode a Minsky machine with these restricted tools ?

REFERENCES

L. Budach, problem 63, FCT-problem Book of Computing, Poznań, Sep 1977

J.H. Conway, *Unpredictable Iterations, in* N.N. (ed.), *Proceedings of the 1972 Number Theory Conference, University of Colorado, Boulder, Colorado Aug 14-18, 1972,* Publ. Univ. of Colorado (1973), pp. 49-52.

Some remarks on PCP(k) and related problems

by

Volker C l a u s (University of Dortmund, FRG)

1. Examples and definitions

Consider the integer-valued matrix

$$M = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 1 & 5 \\ 14 & -9 & 0 \end{pmatrix}$$

Does there exist a power M^n of $M (n \geq 1)$ such that the right upper element of M^n is zero ? For testing we calculate:

$$M^2 = \begin{pmatrix} 43 & -26 & 5 \\ 71 & -43 & 8 \\ -9 & 5 & -3 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 44 & -28 & -1 \\ 69 & -44 & -2 \\ -37 & 23 & -2 \end{pmatrix},$$

$$M^4 = \begin{pmatrix} -42 & 25 & -8 \\ -72 & 43 & -13 \\ -5 & 4 & 4 \end{pmatrix}$$

and this gives us the right upper elements of M^n for n = 1,2,...,8:

3, 5, -1, -8, -1, 14, 8, -21.

The reader may verify that the right upper element of M^{14} is zero.

Let RU be the right upper element of a matrix. Our example belongs to the unsolved problem of SKOLEM (1933):

> Does there exist an algorithm, which decides for every natural number m and for every matrix over the integers $M \in \mathbb{Z}^{m,m}$ of order m, whether there exists a power M^n of $M (n \geq 1)$ with $RU(M^n) = 0$?

The similar problem of KARPINSKI asks for positive right upper elements $(RU(M^n) > 0)$, and is unsolved, too. The generalization leads to problems (which I called NUGAMOR- and POGAMOR-problem [1]):

> Does there exist an algorithm which decides for every natural numbers k and m and for every set $M = \{M_1, \dots, M_k\} \subset \mathbb{Z}^{m,m}$ of k integer-valued matrices of order m, whether there exists a sequence of indices $i_1, \dots, i_n$ $(n \geq 1)$ such that
> $RU(M_{i_1} \cdot M_{i_2} \cdot \dots \cdot M_{i_n}) \neq 0$ (respectively greater zero).

We abbreviate the restriction of this problem to fixed k and m by NUG(m,k), resp. POG(m,k). Then NUG(m,1) is equal to the SKOLEM-problem, and POG(m,1) to the KARPINSKI-problem. The problems NUG(m,k) andPOG(m,k) turn out to be unsolvable for some m and k, and therefore we'll ask for the limit between the areas of decidability and undecidability (with respect to the parameters m and k).

There are connections to the reachability problem (decide, whether there exists an n such that $M^n x = y$ for given vectors $x, y \in \mathbb{Z}^{m,1}$ and matrix $M \in \mathbb{Z}^{m,m}$), which were pointed out by KARPINSKI. A related problem is the mortality-problem, which asks for indices $i_1, \dots, i_n$ such that $M_{i_1} \dots M_{i_n} = 0$ ([5],[6]).

The emptiness-problem for rational probabilistic acceptors asks for an algorithm , which decides to every natural numbers k and m, to every rational number λ , and to every rational probabilistic acceptor $\mathcal{A} = (X, S, \{P(x) | x \in X\}, \pi, f)$ with an k-elementary input-set X, an m-elementary set of states S, a rational probabilistic distribution π on the states, a 0-1-vector of final states f,and k stochastic matrices $P(x_1), \dots, P(x$ over the rational numbers of order m, whether the accepted language $L(\mathcal{A}, \lambda)$ is empty or not. We abbreviate the restriction of this problem to fixed m and k by EMPTY(m,k). In general this problem is unsolvable.

The undecidability is often proven by reducing the problem to Post's correspondence problem (PCP). Let X be an alphabet of 2 elements. The k-bounded PCP asks for an algorithm which decide for a fixed natural number k and for every k-elementary set of pairs of words over X

$$Y = \{(u_1, v_1), \dots, (u_k, v_k)\} \subset X^* \times X^*,$$

whether there is a correspondence,i.e. whether there exists a sequence of indices $i_1, \dots, i_n$ $(n \geq 1)$ such that

$u_{i_1} u_{i_2} \dots u_{i_n} = v_{i_1} v_{i_2} \dots v_{i_n}$. We denote this problem by PCP(k).

2. PCP(10) is undecidable

We need a theorem of MATIJASEVIC ([4]) and a corollary.

<u>Theorem 1</u>: The wordproblem for semigroups over a 2-elementary alphabet is undecidable, even if it is restricted to 3 relations.

For defining the equivalence of words the relation can be used symmetrically. For carrying over this result to Semi-Thue-system (or grammars) every relation has to be read from left to right and from right to left. Therefore, we get 6 productions from the 3 relations.

Corollary: There exists no algorithm which decides for every Semi-Thue-system U (or grammar) with 6 productions over a 2-elementary alphabet X and for every two words $u,v \in X^*$ whether $u \overset{*}{\to} v$ (i.e. v is derivable from u with respect to U) or not.

This corollary says that the wordproblem for Semi-Thue-systems with at most 6 productions is undecidable.

Theorem 2: If the word problem for Semi-Thue-systems with j productions is undecidable, then PCP(j+4) is unsolvable.

Proof: Let $U_0 = (X_0, P_0)$ be a Semi-Thue-system with the 2-elementary alphabet $X_0 = \{x_1, x_2\}$ and the j-elementary set of productions $P_0 = \{u_1 \to v_1, \dots, u_j \to v_j\}$. Let γ be a new symbol.

Define $X_1 := X_0 \cup \{\gamma\}$ and $U_1 = (X_1, P_0)$, then for all $u,v \in X_0^*$:

$$u \overset{*}{\to} v \quad \text{w.r.t.} \quad U_0 \iff \gamma u \gamma \overset{*}{\to} \gamma v \gamma \quad \text{w.r.t.} \; U_1.$$

Let $X_2 := \{0,1\}$, and define a homomorphism $h: X_1^* \to X_2^*$ by $h(x_1) = 01$, $h(x_2) = 011$, $h(x_3) = 0111$. h is injective.
Let $P_2 = \{h(u_1) \to h(v_1), \dots, h(u_j) \to h(v_j)\}$ and $U_2 = (X_2, P_2)$. Then we get for all $u,v \in X_0^*$:

$$\gamma u \gamma \overset{*}{\to} \gamma v \gamma \quad \text{w.r.t.} \quad U_1 \iff h(\gamma u \gamma) \overset{*}{\to} h(\gamma v \gamma) \quad \text{w.r.t.} \; U_2.$$

Let β be a new symbol, and $X_3 := X_2 \cup \{\beta\}$. We define two monomorphismus $\rho, \lambda: X_2^* \to X_3^*$ by

$$\rho(x) = x\beta \quad \text{and} \quad \lambda(x) = \beta x \quad \text{for all } x \in X_2.$$

ρ attaches one β to every symbol on the right side and λ on the left side. To two given words $\bar{u}, \bar{v} \in X_0^*$ define

$$Y = \{ (\rho(w_1), \lambda(w_2)) \mid \text{for all } w_1 \to w_2 \in P_2 \}$$
$$\cup \{ (\rho(x), \lambda(x)) \mid \text{for all } x \in X_2 \}$$
$$\cup \{ (h(\gamma)\beta \,,\, h(\gamma)\lambda(h(\bar{u}\gamma))) \,,\, (\rho(h(\gamma\bar{v}))h(\gamma) \,,\, \beta h(\gamma)) \}.$$

If there exists a derivation with respect to U_2

$$h(\gamma\bar{u}\gamma) = h(\gamma z_0 \gamma) \to h(\gamma z_1 \gamma) \to h(\gamma z_2 \gamma) \to \dots \to h(\gamma z_n \gamma) = h(\gamma \bar{v} \gamma),$$

then

$$h(\gamma)\lambda(h(z_0\gamma))\lambda(h(z_1\gamma))\dots\lambda(h(z_{n-1}\gamma))\lambda(h(z_n))\beta h(\gamma)$$

is a correspondence of Y. Conversely, if there exists a correspondence, this must begin with $h(\gamma)\lambda(h(\bar{u}\gamma))$ ... and end with $\lambda(h(\gamma\bar{v}))\beta h(\gamma)$. The reader may verify that any correspondence of Y defines a derivation from $h(\gamma\bar{u}\gamma)$ to $h(\gamma\bar{v}\gamma)$. It follows:

$$h(\gamma\bar{u}\gamma) \overset{*}{\to} h(\gamma\bar{v}\gamma) \quad \text{w.r.t.} \; U_2 \iff Y \text{ has a correspondence.}$$

By coding X_3 into a 2-elementary alphabet and coding Y analogously, we get a set of j+4 pairs of words $\bar{Y}$ over a 2-elementary alphabet such that:

$$\bar{u} \overset{*}{\to} \bar{v} \quad \text{w.r.t.} \; U_0 \iff \bar{Y} \text{ has a correspondence.}$$

Hence, theorem 2 is proven.

The proof is a variant of a proof given in [2].

Collary: PCP(10) is unsolvable

To my knowledge, k = 10 is the best proven bound of undecidability of PCP(k). PCP(1) is solvable. For k = 2,3,...,9 the question is open, but because of the investigations of K.CULIK, J.KARHUMAKI and others it is supposed that PCP(2) is solvable, but PCP(3) is not.

(Remark: The mortality-problem for 12 3×3-matrices is undecidable. Use the proof of [5].)

3. Related problems

Let X = {1,2} be the 2-elementary alphabet and let $g: X^* \to \mathbb{N}_0$ be the 3-adic interpretation of every word over X. g is injective, but no homonorphism. Then, the mapping $\psi: X^* \times X^* \to \mathbb{Z}^{3,3}$ defined by

$$\psi(u,v) = \begin{pmatrix} 1 & g(v) & g(u) - g(v) \\ 0 & 3^{|v|} & 3^{|u|} - 3^{|v|} \\ 0 & 0 & 3^{|u|} \end{pmatrix}$$

is an injective homomorphism ($|u|$ denotes the length of u). Therefore PCP(k) can be transformed into NUG(3,k). Using another injective homomorphism PCP(k) can be transformed into POG(7,k). By combining the matrices and adding a suitable permutation matrix several results can be derived, for example ([1]):

Theorem 3: The following problems are unsolvable:
NUG(3,10), NUG(32,2), NUG(6,6),

POG(7,10), POG(70,2), POG(14,6).

This theorem is based on the unsolvability of PCP(10), and will be automatically sharpened, if the corollary of theorem 2 will be.

There is a strong connection between EMPTY(m,k) and POG(m,k). Inspecting the proof of TURAKAINEN([7]) carefully one gets

Lemma: If POG(m,k) is unsolvable, then so is EMPTY(m+2,k).
If EMPTY(m,k) is unsolvable, then so is POG(m+1,k).

Therefore, EMPTY(9,10), EMPTY(72,2),... are unsolvable. Though, we do not know anything about POG(2,k), it has been proven that EMPTY(2,k) is solvable ([1]).

4. Remarks to Skolem's problem

The proof for the undecidability of NUG(32,2) uses two matrices M and Q, where Q is a permutation-matrix and M contains the whole information of PCP(10) for a given Y. It seems impossible to enumerate all products of M and Q with one single matrix, i.e. this proof might be not applicable to SKOLEM's problem.

The SKOLEM-problem is equivalent to the question, whether there exists a zero in a sequence of numbers defined by a linear recursive equation. Let M be an integer-valued matrix of order m with the characteristic polynomial

$p(x) = x^m - \sum_{i=0}^{m-1} \alpha_i x^i$, and let $b_i = RU(M^i)$ for $i \geq 0$. Then the sequence $b_1, b_2, b_3, \ldots$ is characterized by $b_0 := 0, b_1, \ldots, b_{m-1}$, and

$$b_{j+m} = \sum_{i=0}^{m-1} \alpha_i \, b_{j+i} \quad \text{for all } j \geq 0,$$

because M is a root of p. Conversely, from $b_0 = 0, b_1, \ldots, b_{m-1}, \alpha_0, \ldots, \alpha_m$ one can construct an integer-valued matrix M of order m such that: $b_j = 0 \iff RU(M^j) = 0$.

Because of the linearity we may be full of hope that SKOLEM's problem is solvable, though we know the solution only in the case m = 2.

Another characterization uses the eigenvalues of M and gives the result, that SKOLEM's problem becomes only difficult if there exist at least two eigenvalues of the same absolute value. Investigations on the languages

$$L(M) = \{j \mid RU(M^j) = 0\} \subseteq \{1\}^*$$

yield that these languages coincide with the regular languages over an 1-letter alphabet. But this connection is not constructive (until today, [3]).

Anybody, who wants to get a feeling of the problem, may calculate the exponent n, for which $RU(M^n) = 0$ holds with respect to the matrix

$$M = \begin{pmatrix} 113 & 113 & 1469 \\ 1938 & 0 & -7910 \\ 442 & 113 & 113 \end{pmatrix}$$

Literature

[1] V.CLAUS, "The (n,k)-bounded emptiness-problem for probabilistic acceptors and related problems", submitted for publication

[2] G.HOTZ,V.CLAUS, "Automatentheorie und Formale Sprachen", Band III, BI-823a, Mannheim 1972

[3] M.KARPINSKI, "Decidability of 'Skolem-Matrix-Emptiness-Problem' entails constructability of exact regular expression" (a note), IBM: RC 8382, Yorktown Heights, 1980

[4] J.V.MATIJASEVIC, "Simple examples of undecidable associative calculi", Soviet Math. Dokl. 8, 555-557 (1967)

[5] M.S.PATTERSON, "Unsolvability in 3×3-matrixes", Studies in Applied Mathematics, Vol. XLIX, March 1970, MIT.

[6] P.SCHULTZ, "Mortality of 2×2-Matrices", American Math. Monthly, 1977, 463-464

[7] P.TURAKAINEN, "Word functions of stochastic and pseudo-stochastic automata", Annales Academic Scientiarum Fenmicae, Helsinki 1975

A NOTE ON ITERATING INVERSE HOMOMORPHISMS

Matthias Jantzen

Fachbereich 18
Univ. Hamburg
Schlüterstr. 70
D-2000 Hamburg 13

We all know that DOL languages can be defined nicely by iterating some homomorphism $h : X^* \longrightarrow X^*$ on an axiom $w \in X^*$. The DOL language L then is

$$L := \bigcup_{i=0}^{\infty} h^i(w) .$$

Now, thinking backwards, we may define languages of the form

$$h^{-*}(M) := \bigcup_{i=0}^{\infty} h^{-i}(M) ,$$

where M is a single word or a set of words. We see that for L as above we have:

$v \in L$ if and only if $w \in h^{-*}(v)$.

Obviously $h^{-*}(M)$ is a finite set if M is finite and the only interesting case is the one where M is an infinite language of a certain type. For instance, what can we say if M is a context-free language? Well, it is not surprising that $h^{-*}(M)$ need not be context-free if M is context-free.

EXAMPLE

Let h be given by $h(a) := aa$, $h(b) := b$. Then $h^{-*}(\{a^n b^n \mid n \geq 0\})$ is not context- free, since $h^{-*}(\{a^n b^n \mid n \geq 0\}) \cap ab^* = \{a\, b^{2^n} \mid n \geq 0\}$.

Could it happen that $h^{-*}(M)$ is not even recursive for some context-free language M ? We believe that this is the case, but we do not have a proof for this conjecture!