A Remark on Acceptable Sets of Numbers

MARCEL PAUL SCHÜTZENBERGER*

The RAND Corporation, Santa Monica, California

ABSTRACT. Two negative results concerning the so-called acceptable sets of numbers are extended to the case of arbitrary context-free languages with the help of conventional analytic techniques.

KEY WORDS AND PHRASES: acceptable sets, automata, context-free languages, regular sets, finite automata

CR CATEGORIES: 5.22, 5.23, 5.29

Introduction

In what follows, X^* denotes the free monoid with neutral element e that is generated by a fixed finite nonempty set X, $\mathbf{N}$ denotes the nonnegative integers, and $\mathbf{L}$ is the family of all context-free languages on X [4, 7]. We consider a fixed crossed homomorphism ρ of X^* into the ring $\mathbf{Z}$ of rational integers; ρ is defined by its restriction to X and by the identity

$$\rho ff' = \rho f \cdot \alpha f' + \rho f', \qquad f, f' \in X^*, \tag{1}$$

where α is a homomorphism of X^* into the multiplicative structure of $\mathbf{Z}$. Thus $\rho e = 0$ by definition. We make the assumption that $|\alpha x| > 1$ for all $x \in X$. This condition is satisfied when $X = \{0, 1\}$, $\alpha 0 = \alpha 1 = 2$, $\rho 0 = 0$, and $\rho 1 = 1$, in which case ρf is the number whose binary expansion is f.

The problem of showing that certain remarkable subsets of $\mathbf{Z}$ cannot have the form $\rho L = \{\rho f : f \in L\}$ for $L \in \mathbf{L}$, or for L in some given subfamily of $\mathbf{L}$, was first attacked by Elgot [6] using metamathematical methods. Recently, Minsky and Papert [8] have considerably generalized these results by a delicate analysis of the asymptotic properties of the function **Card** $\{f \in L : |\rho f| < n\}$ of the nonnegative integer n. Being concerned with the subfamily of the so-called "regular sets," they indicated the possibility of extending their method to arbitrary languages $L \in \mathbf{L}$. (See also [2, 5, 10].) We show here two applications of the techniques of classical analysis to examples already discussed by other authors.

We rely on the following result [1]:

THEOREM [Bar-Hillel, Shamir, and Perles]. *Let $L \in \mathbf{L}$. Except for the members of a finite subset L_0 of L, every word $f \in L$ admits at least one factorization $f = g''h'g'hg$ such that $h' \neq e$ and that $H = \{h_n = g''h'^n g'h^n g : n \in \mathbf{N}\}$ is contained in L.*

This work was supported in part by contract with the US Air Force, AF 61(052)945. Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of the RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors.

* Present address: Faculté des Sciences de Paris, Paris, France

Journal of the Association for Computing Machinery, Vol. 15, No. 2, April 1968, pp. 300–303.

Without loss of generality we always assume $g = e$ when $h = e$. A straightforward computation gives

$$\rho h_n = b'' + b'(\alpha h)^n + b(\alpha hh')^n \tag{2}$$

where, setting $\beta f = \rho f(1 - \alpha f)^{-1}$ when $f \neq e$, and $\beta e = 0$, we have

$$b'' = \rho g + \beta h \cdot \alpha g;$$

$$b' = \beta h' \cdot \alpha g' g + \rho g' \cdot \alpha g - \beta h \cdot \alpha g;$$

$$b = \rho g'' \cdot \alpha g' g - \beta h' \cdot \alpha g' g.$$

In particular, $b'' = 0$ when $h = e$. Further, ρH is finite if and only if it reduces to $\{\rho h_0\} = \{\rho g'' g' g\}$.

First Example

Let $L \in \mathbf{L}$ and $k \in \mathbf{N}$ be such that no member of ρL has more than k different prime divisors. Then the set $\mathbf{Prm}(\rho L)$ of all prime divisors of the members of ρL is a finite set contained in $\mathbf{Prm}(\rho L_0 \cup \alpha X)$.

Let $f \in L \backslash L_0$ and assume that $\mathbf{Prm}(\rho f') \subseteq \mathbf{Prm}(\rho L_0 \cup \alpha X)$ is already verified for every $f' \in L$ strictly shorter than f. Since $f \notin L_0$, we can write $f = h_1 = g'' h' g' h g$ as indicated in the Introduction; and the result is still true for f if ρH is finite since then we know that $\rho f = \rho h_0$ where $h_0 = g'' g' g$ is strictly shorter than f. Thus we can assume that ρH is infinite. According to (2), ρh_n is the coefficient of t^n in the Taylor series expansion of the rational function

$$r(t) = b'' \cdot (1 - t)^{-1} + b' \cdot (1 - t \cdot \alpha h)^{-1} + b \cdot (1 - t \cdot \alpha hh')^{-1}$$

of the variable t. Noting that $r(t)$ has a zero for $t = \infty$, a well-known theorem of Polyá [9, p. 14, Satz II] indicates that $\mathbf{Prm}(\rho H)$ is infinite unless $r(t)$ has the form

$$\sum_{0 \leq i < m} c_i t^i \cdot (1 - c_i t^m)^{-1}$$

for some finite m. Now this condition is satisfied only if $b'' = b'b = 0$, and then ρH has the form

$$\{b' \cdot (\alpha h)^n : n \in \mathbf{N}\} \quad \text{or} \quad \{b \cdot (\alpha hh')^n : n \in \mathbf{N}\}.$$

Furthermore, $\rho h_0 = b'$ or b; and since α is a homomorphism, $\mathbf{Prm}(\alpha h)$ and $\mathbf{Prm}(\alpha hh')$ are contained in $\mathbf{Prm}(\alpha X)$. Thus $\mathbf{Prm}(\alpha H)$ is contained in $\mathbf{Prm}(\rho h_0) \cup \mathbf{Prm}(\alpha X)$ and the verification is concluded.

Second Example

Let $L \in \mathbf{L}$ and the polynomial π be such that $\mathbf{Card}\ \rho L = \infty$ and $\rho L \subseteq \pi \mathbf{Z} (= \{\pi z : z \in \mathbf{Z}\}) \subseteq \mathbf{Z}$. Then π is a trinomial, i.e., $\pi t = c(t + s)^d + c'(t + s)^{d'} + c''$ for some constant s.

We can assume $\pi t = \sum_{0 \leq j \leq d} c_j t^{d-j}$ where the degree d of π is at least 3, since otherwise π is automatically a trinomial. Since ρL is infinite, L must contain a subset H of the type described in the introduction for which ρH is infinite. We set $a' = \alpha h, \quad a = \alpha hh'$.

The hypothesis $\rho L \subseteq \pi \mathbf{Z}$ implies the existence of a map, denoted by ζ_n, of $\mathbf{N}$ into $\mathbf{Z}$ such that $\pi\zeta_n = \rho h_{nd} = ba^{nd} + b'(a')^{nd} + b''$ identically.

Let ζ_n' satisfy $c_0\zeta_n' = \rho h_{nd} - b'' = ba^{nd} + b'a'^{nd}$. We have

$$\zeta_n' = a^n(r_0 + \sum_{0<i} r_i(a'^{dn}/a^{dn})^1)$$

where $r_0 = (bc_0^{-1})^{1/d}$. Thus letting $\zeta_n = \zeta_n'(1 + \epsilon_n')$, it follows from $\zeta_n = \rho h_{nd}$ that

$$(1 + \epsilon_n')^d + \sum_{0<j\leq d} \zeta'^{-j}_n(1 + \epsilon_n')^{d-j} c_j c_0^{-1} = 1 + b''\zeta'^{-d}_n c_0^{-1},$$

showing that $\epsilon_n' = r'\zeta'^{-1}_n + \epsilon_n'' \zeta'^{-2}_n$ where r' is a constant and ϵ_n'' has bounded modulus. Accordingly, if $| a'^d | \leq | a^{d-1} |$ we can write $\zeta_n = r_0a^n + r' + \epsilon_n$ where $| \epsilon_n |$ tends to zero at least as fast as $\max \{ | a^{-n} |, | a'^{dn} a^{-dn+n} | \}$. If $| a'^d | > | a^{d-1} |$ there exists a finite integer k such that $| a'^{kd}/a^{kd-1} | > 1 \geq | a'^{kd+d}/a^{kd+d-1} |$, and then we can write $\zeta_n = r_0a^n + \sum_{0<i\leq k} r_i a'^{idn} a^{-idn+n} + r' + \epsilon_n$ where $| \epsilon_n |$ tends to zero at least as fast as $| a'^{(kd+d)n} a^{-(kd+d)n+n} |$.

In the first case, we have $\zeta_{n+1} - a\zeta_n = r'(a - 1) + (\epsilon_{n+1} - a\epsilon_n)$. Since the left member of this relation is an integer and since $| \epsilon_{n+1} - a\epsilon_n |$ tends to zero for $n \to \infty$ we have in fact that, for all large enough $n \in \mathbf{N}$, $\epsilon_{n+1} - a\epsilon_n$ is equal to some fixed $r'' \in \mathbf{Z}$. Thus, for all large enough n, ζ_n satisfies a linear recurrence relation $\zeta_{n+1} - a\zeta_n = r'(a - 1) + r''$; hence $\zeta_n = sa^n + s'$ where s and s' are constant rational numbers. Bringing this expression into the relation $\pi\zeta_n = \rho h_{nd}$ and identifying terms, we see instantly that π must have the form $c(t + s'')^d + c'(t + s'')^{d'} + c''$, and further that a' and d' must be such that $a'^d = a^{d'}$. This concludes the verification in this case.

If $| a'^d/a^{d-1} | > 1 \geq | a^{2d}/a^{2d-1} |$ (i.e., if $k = 1$), we have

$$\zeta_n = r_0a^n + r_1 a'^{dn} a^{-dn+n} + r' + \epsilon_n .$$

Thus $a^{d-1}\zeta_{n+2} - (a^d + a'^d)\zeta_{n+1} + aa'^d \zeta_n$ is equal to a constant, plus a term whose modulus tends to zero when $n \to \infty$. As above we conclude that ζ_n satisfies a linear recurrence for all large enough n and, in fact, that $\zeta_n = sa^n + s'a'^{dn}a^{-dn+n} + s''$. More generally, for arbitrary $k > 1$, we replace the polynomial $\omega_1 = a^{d-1}t^2 - (a^d + a'^d)t + aa'^d$ used above by the polynomial ω_k of degree $k + 1$ whose roots are $\{a, a'^da^{-d+1}, a'^{2d}a^{-2d+1}, \ldots, a'^{kd}a^{-kd+1}\}$ and whose coefficient of t^{k+1} is the product $a^{d-1}a^{2d-1} \ldots a^{kd-1}$. Substituting ζ_{n+i} for t^i in ω_k we obtain an expression which is equal to a constant plus a term whose modulus tends to zero for $n \to \infty$, and we conclude that in all cases ζ_n can be expressed as a finite sum

$$s_0a^n + \sum_{0<i\leq k} s_i(a'^{id}/a^{id-1})^n + s_{k+1} .$$

We now show that this is incompatible with the hypothesis $\pi\zeta_n = \rho h_{nd}$. Indeed, bringing the expression of ζ_n which has been obtained into the equation $\pi\zeta_n = \rho h_{nd}$, we can identify terms. Noting that $ba^{nd} + b'a'^{nd}$ is equal to the sum of the first two terms in the expansion of $c_0\zeta_n^d$, we find that all the other nonconstant terms of $\pi\zeta_n$ must cancel between themselves. Let j be the largest index less than d such that $c_j \neq 0$, and let i be the largest index less than $k + 1$ such that $s_i \neq 0$. The term $(a'^{id}/a^{id-1})^n \, s_{k+1}^{j-1}$ (or the term $(a'^{id}/a^{id-1})^{nj}$ if $s_{k+1} = 0$) in $\zeta_n{}^j$ cannot cancel with any other term. Thus the equation $\pi\zeta_n = \rho h_{nd}$ with integral ζ_n is impossible when $k \geq 1$, and the verification is concluded.

REFERENCES

1. Bar-Hillel, Y., Shamir, E., and Perles, M. On formal properties of simple phrase structure grammars. *Z. Phonetik, Sprachwiss. Kommunikationsforsch. 14* (1961), 143–172; in Bar-Hillel, Y., *Language and Information*, Addison-Wesley, Reading, Mass., 1965, pp. 116–150.
2. Buchi, J. R. Weak second order arithmetic and finite automata. *Z. math. Logik Grund. Math. 6* (1961), 66–92.
3. Cantor, D. G. On arithmetic properties of coefficients of rational functions. *Pacific J. Math. 15* (1965), 55–58.
4. Chomsky, N., and Miller, G. A. Finitary models of language users. In Luce, R. D., Bush, R. R., and Galanter, E. (Eds.), *Handbook of Mathematical Psychology, Vol. 2*, Wiley, New York, 1963, Ch. 13, pp. 419–491.
5. Cobham, A. Sets definable by finite automata. IBM Res. Notes #405, #458, #577 (1964, 1965, 1966).
6. Elgot, C. C. Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc. 98* (1961), 21–51.
7. Ginsburg, S. *The Mathematical Theory of Context-Free Languages*. McGraw Hill, New York, 1966.
8. Minsky, M., and Papert, S. Unrecognizable sets of numbers. *J. ACM 13* (1966), 281–286.
9. Polyá, G. Arithmetisch Eigenschaften der Reihenentwicklung rationaler Funktionen. *J. reine angew. Math. 151* (1921), 1–31.
10. Ritchie, R. W. Finite automata and the set of squares. *J. ACM 10* (1963), 528-531.

RECEIVED SEPTEMBER, 1966; REVISED SEPTEMBER, 1967