Variations on a theme of K. Mahler

Attila Pethő

Department of Computer Science
University of Debrecen
Debrecen, Hungary

Uniform Distribution Theory
CIRM Marseille-Luminy, October 3, 2018.

Talk is base on the paper

Variations on a theme of K. Mahler, I., Annales Univ. Sci. Budapest., Sect. Comp. 48 (2018) 137–149.

The volume is dedicated - among others - to the 80th birthday of **Imre Kátai**.

1. Introduction and notations

Let $g, h \geq 2$. Denote $(n)_g$ the sequence of digits of the g-ary representation of n, e.g. $(2018)_{10} = 2018, (2018)_5 = 31033$. K. Mahler, 1981, proved that the number $0.(1)_g(h)_g(h^2)_g \ldots$ is irrational, equivalently: the infinite word $(1)_g(h)_g(h^2)_g \ldots$ is not periodic. Refinements, generalizations and new methods by

- P. Bundschuh, 1984
- H. Niederreiter, 1986
- Z. Shan, 1987
- Z. Shan and E. Wang, 1989: Let $(n_i)_{i=1}^{\infty}$ be a strictly increasing sequence of integers. Then $0.(g^{n_1})_h(g^{n_2})_h \ldots$ is irrational. In the proof they used the theory of Thue equations.

Generalizations for numeration systems based on linear recursive sequences:

- P.G. Becker, 1991
- P.G. Becker and J. Sander 1995
- G. Barat, R. Tichy and R. Tijdeman, 1997
- G. Barat, C. Frougny and A. Pethő, 2005

2. Radix representation in number fields

Let $\mathbb{K}$ an algebraic number field with ring of integers $\mathbb{Z}_{\mathbb{K}}$
$\mathbb{L}$ a finite extension of $\mathbb{K}$ with ring of integers $\mathbb{Z}_{\mathbb{L}}$
The pair $(\gamma, \mathcal{D})$, where $\gamma \in \mathbb{Z}_{\mathbb{L}}$ and $\mathcal{D}$ is a complete residue system modulo γ in $\mathbb{Z}_{\mathbb{K}}$ is called a GNS in $\mathbb{Z}_{\mathbb{L}}$ if for any $0 \neq \beta \in \mathbb{Z}_{\mathbb{L}}$ there exist an integer $\ell \geq 0$ and $a_0, \ldots, a_\ell \in \mathcal{D}, a_\ell \neq 0$ such that

$$\beta = a_\ell \gamma^\ell + \cdots + a_1 \gamma + a_0. \tag{1}$$

Denote the sequence or word of the digits $a_\ell \ldots a_1 a_0$ by $(\beta)_\gamma$.

The GNS concept was initiated by D. Knuth, and developed further by Penney, I. Kátai, J. Szabó, B. Kovács, etc.

3. Results on power sums

Let $0 \notin \mathcal{A}, \mathcal{B} \subset \mathbb{Z}_{\mathbb{L}}$ be finite, and Γ, Γ^{+} be the semigroup, group generated by $\mathcal{B}$. Put

$$S(\mathcal{A}, \mathcal{B}, s) = \{\alpha_1\mu_1 + \cdots + \alpha_s\mu_s \ : \ \alpha_j \in \mathcal{A}, \mu_j \in \Gamma\}.$$

Example: $\mathbb{L} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{2, 3\}$ then

$$S(\mathcal{A}, \mathcal{B}, 2) = \{2^a 3^b + 2^c 3^d \ : \ a, b, c, d \geq 0\}.$$

Theorem 1. *Let* $s \geq 1$ *and* $\mathcal{A}, \mathcal{B}$ *as above. Let* (c_n) *be such that* $c_n \in S(\mathcal{A}, \mathcal{B}, s)$*. If* $(\gamma, \mathcal{D})$ *is a GNS in* $\mathbb{Z}_{\mathbb{L}}$*,* $\gamma \notin \Gamma^+$ *and* (c_n) *has infinitely many distinct terms then the infinite word* $(c_1)_\gamma (c_2)_\gamma \ldots$ *is not periodic.*

Let $(c_1)_\gamma (c_2)_\gamma \ldots = f_0 f_1 \ldots$. Then

$$g = \sum_{j=0}^{\infty} f_j \gamma^{-j}$$

is a well defined complex number. A result of B. Kovács and I. Környei, 1992 implies $g \notin \mathbb{Q}$. We expect at least $g \notin \mathbb{L}$, but we are unable to prove this.

The proof of Theorem 1 is based on the following

Lemma 1. *For any* $w \in \mathcal{D}^*$ *there are only finitely many* $U \in S(\mathcal{A}, \mathcal{B}, s)$ *such that* $(U)_\gamma = w_1 w^k$*, where* w_1 *is a suffix of* w*.*

Proof. Let $w = d_0 \ldots d_{h-1}$. If $(U)_\gamma = w_1 w^k$ then $w_1 = \lambda$ or $w_1 = d_t \ldots d_{h-1}$. Set $q_0 = 0$ if $w_1 = \lambda$, and $q_0 = d_t + d_{t+1}\gamma + \ldots + d_{h-1}\gamma^{h-t-1}$ otherwise. Further let $q = d_0 + d_1\gamma + \ldots + d_{h-1}\gamma^{h-1}$. We also have $U = \alpha_1\mu_1 + \cdots + \alpha_s\mu_s$. Then

$$
\begin{aligned}
\alpha_1\mu_1 + \cdots + \alpha_s\mu_s &= q_0 + \gamma^{h-t} \sum_{i=0}^{k-1} q\gamma^{ih} \\
&= q_0 + q\gamma^{h-t} \frac{\gamma^{hk} - 1}{\gamma^h - 1} \\
&= \frac{q\gamma^{h-t}}{\gamma^h - 1}\gamma^{hk} + q_0 - \frac{q\gamma^{h-t}}{\gamma^h - 1}.
\end{aligned}
$$

Setting

$$\alpha_{s+1} = \frac{q\gamma^{h-t}}{\gamma^h - 1}, \qquad \alpha_{s+2} = q_0 - \frac{q\gamma^{h-t}}{\gamma^h - 1}$$

we get the equation

$$\alpha_1\mu_1 + \cdots + \alpha_s\mu_s = \alpha_{s+1}\gamma^{hk} + \alpha_{s+2}. \tag{2}$$

As $(\gamma, \mathcal{D})$ is a GNS $|\gamma| > 1$, hence $\gamma^h \neq 1$ and $\alpha_{s+1}, \alpha_{s+2}$ are well defined. Plainly $\alpha_j \in \mathbb{L}, j = 1, \ldots, s+2$ and $\alpha_j \neq 0, k = 1, \ldots, s$ by assumption. It is easy to see that $\alpha_{s+1} \neq 0$ holds too.

Taking Γ_1 the multiplicative semigroup generated by γ and $b \in \mathcal{B}$ (2) is a Γ_1-unit equation. If there are infinitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ such that $(U)_\gamma = w_1 w^k$ then k can take arbitrary large values and (2) has infinitely many solutions in $(\mu_1, \ldots, \mu_s, \gamma^{hk}) \in \Gamma_1^{s+1}$. By the theory of weighted S-unit equations the assumption $\gamma \notin \Gamma^+$ excluded this. $\square$

Proof of Theorem 1. Let $W = (c_1)_\gamma(c_2)_\gamma\ldots$ and assume that it is eventually periodic. Omitting, if necessary, some starting members of (c_n) we may assume that it is periodic, i.e. $W = H^\infty$ with $H \in \mathcal{D}^h$.

There exist for all $n \geq 1$ a suffix c_{n0} a prefix c_{n1} of H and an integer $e_n \geq 0$ such that $(c_n)_\gamma = c_{n0}H^{e_n}c_{n1}$.

There exist only finitely many, elements of $\mathbb{Z}_\mathbb{K}$ with a $(\gamma, \mathcal{D})$-representation of bounded length. Thus, the length of the words $(c_n)_\gamma, n = 1, 2, \ldots$ is not bounded. Further, there are only $|\mathcal{A}|^s$ possible choices for the s-tuple $(a_{n1}, \ldots, a_{ns})$. Thus, there exists an infinite sequence $k_1 < k_2 < \ldots$ of integers such that $l((c_{k_n})_\gamma) \geq h$ and $l((c_{k_{n+1}})_\gamma) > l((c_{k_n})_\gamma)$ and the s-tuples $(a_{k_n1}, \ldots, a_{k_ns})$ are the same for all $n \geq 1$.

Write $(c_{k_n})_\gamma = c_{k_n0} H^{e_{k_n}} c_{k_n1}$, where c_{k_n0} is a suffix and c_{k_n1} is a prefix of H for all $n \geq 1$. As H has at most $h-1$ proper prefixes and $h-1$ proper suffixes there exists an infinite subsequence of $k_n, n \geq 1$ such that the corresponding words satisfy $c_{k_n0} = C_0$ and $c_{k_n1} = C_1$. In the sequel we work only with this subsequence, therefore we omit the subindexes.

With this simplified notation we have $(c_n)_\gamma = C_0 H^{e_n} C_1$, where C_0 denotes a proper suffix, and C_1 a proper prefix of H and (e_n) tends to infinity. Finally, replacing H by the suffix of length h of HC_1, and denoting it again by H we have $(c_n)_\gamma = C_0 H^{e_n}$. This contradicts Lemma 1. □

Considering for $\mathbb{K} = \mathbb{Q}$ the ordinary g-ary representation of integers we get immediately the following far reaching generalization of Mahler's result.

Corollary 1. *Let $\mathcal{A}, \mathcal{B}$ be finite sets of positive integers and $g \geq 2$ be a positive integer. Let $\Gamma = \Gamma(\mathcal{B})$ and $c_n = a_{n1}u_{n1} + \cdots + a_{ns}u_{ns}$ with $u_{ni} \in \Gamma, a_{ni} \in \mathcal{A}, 1 \leq i \leq s, n \geq 1$. If $g \notin \Gamma$ and (c_n) is not bounded, then $0.(c_1)_g(c_2)_g...$ is irrational.*

To illustrate the power of Theorem 1 we formulate a further corollary.

Corollary 2. *Let γ be an algebraic integer, which is neither rational nor imaginary quadratic. Let $\mathbb{K} = \mathbb{Q}(\gamma)$, $\mathcal{D}$ be a complete residue system modulo γ in $\mathbb{Z}_{\mathbb{K}}$ and $(\gamma, \mathcal{D})$ be a GNS in $\mathbb{Z}[\gamma]$. If (c_n) is a sequence of elements of $\mathbb{Z}[\gamma]$ of given norm, which includes infinitely many pairwise different terms, then the word $(c_1)_\gamma(c_2)_\gamma \ldots$ is not periodic.*

Proof. There exists in $\mathbb{Z}_{\mathbb{K}}$ only finitely many pairwise not associated elements with given norm. Let $\mathcal{A}$ be such a set. There exist by Dirichlet's theorem $\varepsilon_1, \ldots, \varepsilon_r$ such that every unit of infinite order of $\mathbb{Z}_{\mathbb{K}}$ can be written in the form $\varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$. Setting $\mathcal{B} = \{\varepsilon_1, \ldots, \varepsilon_r\}$ apply Theorem 1. $\square$

Notice that in the rational and in the imaginary quadratic fields there are only finitely many elements with given norm, hence there are cases, when $(c_1)_\gamma(c_2)_\gamma\ldots$ is, and other cases, when it is not periodic.

4. Application to solutions of norm form equations

Let $\mathbb{K}$ be an algebraic number field of degree k. It has k isomorphic images, $\mathbb{K}^{(1)} = \mathbb{K}, \dots, \mathbb{K}^{(k)}$ in $\mathbb{C}$. Let $\alpha_1 = 1, \alpha_2, \dots, \alpha_s \in \mathbb{Z}_{\mathbb{K}}$ be $\mathbb{Q}$-linear independent elements and $L(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_s X_s$. Plainly $s \leq k$. Consider the norm form equation

$$N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = \prod_{j=1}^{k} (\alpha_1^{(j)} X_1 + \cdots + \alpha_s^{(j)} X_s) = t, \tag{3}$$

where $0 \neq t \in \mathbb{Z}$, which solutions are searched in $\mathbb{Z}$. Notice that the polynomial $N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X}))$ is invariant against conjugation, thus, it has rational integer coefficients.

Now we are in the position to state our Mahler-type result on the solutions of (3).

Theorem 2. *Let* $(\mathbf{x}_n) = ((x_{n1}, \ldots, x_{ns}))$ *be a sequence of solutions of (3), including infinitely many different ones. Let* $1 \leq j \leq s$ *be fixed and* $g \geq 2$*. If* (x_{nj}) *is not ultimately zero then the infinite word* $(|x_{1j}|)_g(|x_{2j}|)_g \ldots$ *is not periodic.*

Outline of the proof By a deep theorem of W.M. Schmidt there exist a finite set $\mathcal{A} \subset \mathbb{Z}_{\mathbb{K}}$ such that

$$\alpha_1 x_{n1} + \cdots + \alpha_s x_{ns} = \mu u_n$$

with $\mu \in \mathcal{A}$ and with a unit $u_n \in \mathbb{Z}_{\mathbb{K}}$. Taking conjugates we obtain the system of linear equations

$$\alpha_1^{(i)} x_{n1} + \cdots + \alpha_s^{(i)} x_{ns} = \mu^{(i)} u_n^{(i)}, i = 1, \ldots, k,$$

which implies

$$x_{nj} = \nu_1 u_n^{(1)} + \cdots + \nu_k u_n^{(k)}$$

with some constants ν_i belonging to the normal closure of $\mathbb{K}$. The assumption (x_{nj}) is not ultimately zero implies that (x_{nj}) is not bounded. Now we can apply Theorem 1.

Remark 1. *If $\mathbb{K}$ is a real quadratic number field (3) is called Pell equation, which solutions can be expressed by the union of finitely many linear recursive sequences. In this case Theorem 2 is included implicitly in Theorem 1 of Barat, Frougny and Pethő.*

Győry, Mignotte and Shorey, 1990 proved with the notation of Theorem 2 that if the set of the j-th coordinate of the solutions of (3) is not bounded then the greatest prime factor of them tends to infinity. Our Theorem 2 shows that their assumption always holds if (3) has infinitely many solutions, which j-th coordinates is non-zero.