Subsequences of automatic sequences and uniform distribution

Michael Drmota

Abstract. Automatic sequences and their number theoretic properties have been intensively studied during the last 20 or 30 years. Since automatic sequences are quite regular (they just have linear subword complexity) they cannot be used as quasi-random sequences. However, the situation changes drastically when one uses proper subsequences, for example the subsequence along primes or squares. It is conjectured that the resulting sequences are normal sequences which could be already proved for the Thue-Morse sequence along the subsequence of squares.

This kind of research is very challenging and was mainly motivated by the Gelfond problems for the sum-of-digits function. In particular during the last few years there was a spectacular progress due to the Fourier analytic method by Mauduit and Rivat. In this article we survey these recent developments, comment on the proof methods and formulate quite general conjectures. We also present a new result on the subsequence along primes of so-called invertible automatic sequences.

Keywords. Automatic sequences, Gelfond problems, uniform distribution, exponential sums.

AMS classification. 11A63, 11L03, 11N05, 11N60.

1 Introduction

An automatic sequences $\mathbf{u} = (u(n))_{n \ge 0}$ is the output sequence of a finite automaton, where the input is the q-ary digital expansion of n. For example the Thue-Morse sequence is automatic (with respect to base q = 2). These kind of sequences have gotten a lot of attention during the last 20 or 30 years, we just mention here the book *Automatic Sequences* [1] by Allouche and Shallit that provides a systematic treatment of this subject. Moreover there are very interesting recent transcendency results related to automatic sequences. For example, a result of Bugeaud [2] says that a real number α with continued fraction expansion $\alpha = [a_0, a_1, a_2, \ldots]$, where the sequence $(a_n)_{n \ge 0}$ is automatic, is either a quadratic irrational number (when a_n is ultimatively periodic) or transcendental.

A very well studied class of automatic sequences is directly related to the q-ary digital expansion of $n = \sum_{j=0}^{\nu} \varepsilon_j(n) q^j$ (with digits $\varepsilon_j(n) \in \{0, 1, \dots, q-1\}$ and $\nu = \nu(n) = \lfloor \log_q n \rfloor$). A function $f : \mathbb{N} \to \mathbb{Z}$ is called strongly q-additive if f(0) = 0

and

$$f(n) = \sum_{j=0}^{\nu} f(\varepsilon_j(n))$$

The most prominent example of strongly q-additive functions is the q-ary sum-of-digits function

$$s_q(n) = \sum_{j=0}^{\nu} \varepsilon_j(n).$$

It is easy to see that for every strongly q-additive function f the sequence

$$u(n) := f(n) \bmod m$$

is an automatic sequence (with respect to base q) for any integer $m \ge 1$. The Thue-Morse sequence

$$T(n) = s_2(n) \bmod 2$$

is a very special case. For several distributional properties of q-additive (and even more generally defined functions) we refer to the book chapter "Analysis of digital functions and applications. Combinatorics, automata and number theory" by Drmota and Grabner [7]. Im particular the sequence $\alpha f(n) \mod 1$ is analyzed there with the help of several different methods ranging from ergodic methods over probabilistic to analytic methods.

Actually the first result on distributional properties of the sequence $u(n) = s_q(n) \mod m$ goes back to Gelfond [13] who proved that for every $\ell \in \{0, 1, \dots, m-1\}$

$$\#\{n < N : s_q(an+b) \equiv \ell \mod m\} = \frac{N}{m} + O\left(N^{1-\eta}\right)$$

for some $\eta > 0$ (provided that (q - 1, m) = 1), that is, linear subsequences of the q-automatic sequence $u(n) = s_q(n) \mod m$ are asymptotically uniformly distributed on the values $E = \{0, 1, \dots, m - 1\}$.

What is even more interesting, in the same paper [13] Gelfond formulated three problems, which are usually called **Gelfond Problems**:

(i) If $q_1, q_2 \ge 2$ are coprime integers and $(q_1 - 1, m_1) = (q_2 - 1, m_2) = 1$ then

$$\#\{n < N : s_{q_1}(n) \equiv \ell_1 \mod m_1, \ s_{q_2}(n) \equiv \ell_2 \mod m_2\} = \frac{N}{m_1 m_2} + O\left(N^{1-\eta}\right)$$

for some $\eta > 0$.

(ii) If $q \ge 2$ with (q-1, m) = 1 then

$$\#\{p < N : p \in \mathbb{P}, \ s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O\left(N^{1-\eta}\right)$$

for some $\eta > 0$. ($\pi(x)$ denotes the number of primes $\langle x$.)

(iii) If $q \ge 2$ with (q - 1, m) = 1 then for every integer polynomial P(x)

$$\#\{n < N : s_q(P(n)) \equiv \ell \mod m\} = \frac{N}{m} + O\left(N^{1-\eta}\right)$$

for some $\eta > 0$.

Whereas the first problem was almost immediately solved by Besineau [3] (without an explicit error term; the error term was finally proved by Kim [15]) it took more than 40 years till the other two problems were solved or came close to a solution. Actually, the second problem on the subsequence along the primes was solved by Mauduit and Rivat [25]. The third problem was completely solved for quadratic polynomials by Mauduit and Rivat [24] and partially solved for general polynomials by Drmota, Mauduit and Rivat [8] (it is assumed that the base q is prime and sufficiently large with respect to the degree of P(x)). Most probably Gelfond's paper was the first encounter between (special) automatic sequences and the question of uniform distribution.

Although automatic sequences have the property that the (logarithmic) densities of output letters exist – so that we have a kind of limiting distribution – they are certainly no quasi-random sequences (even if the output letters are uniformly distributed). The subword complexity $p_{\mathbf{u}}(n)$, that is, the number of different subwords of \mathbf{u} of length n, is either uniformly bounded (if \mathbf{u} is ultimatively periodic) or of linear order. For a (quasi-)random sequence we should certainly have $p_{\mathbf{u}}(n) = |E|^n$ (when E denotes the output alphabet). Thus, we are actually far away from a (quasi-)random sequence.

The idea of taking subsequences of automatic sequences it to *re-introduce* randomness to such sequences without destroying the original density structure. The purpose of this article is to survey some recent developments into this directions, some of them are quite spectacular – and many problems are still unsolved. In particular the Fourier theoretic method that has been developed by Mauduit and Rivat [24, 25] was a break-through in this field. (We will discuss several aspects of this method in the sequel.)

The structure of this survey paper is the following one. First we recall the definition (and some properties) of automatic sequences (Section 2). Then we discuss recent results on subsequences along $\lfloor n^c \rfloor$ (Section 3), polynomial subsequences (Section 4) and the subsequence of primes (Section 5). In particular we also present a new result (Theorem 5.5) on subsequences along primes of invertible automatic sequences.

We also want to mention that there are other kinds of relations between automatic sequences and uniform distribution. For example Mauduit [17, 18, 19, 20] discussed in a series of papers the problem, whether the sequence (αu_n) is uniformly distributed modulo 1 (for irrational α) when the sequence u_n is recognized by an finite automaton. However, we will not discuss such kind of questions in this paper.

2 Automatic Sequences

The notion of q-automata and q-automatic sequences was standardized in the monograph by Allouche and Shallit [1]. We just give here the minimal information for the reader who is not acquainted with those notions (we follow here the presentation of [6]).

Definition 2.1. Let $q \ge 2$. A q-automaton \mathcal{M} with values in a finite set E is given by:

- a finite non-empty set $\mathcal{R} = \{r_1, \dots, r_d\}$, the elements of which are called states,
- one element of \mathcal{R} , which is singled out and called the initial state; we will use the notation r_1 for this element,
- a map $\delta : \mathcal{R} \times \{0, 1, \dots, q-1\} \rightarrow \mathcal{R}$,
- a map $\tau : \mathcal{R} \to E$.

Let us explain, how we associate to the q-automaton \mathcal{M} a sequence of elements of E, say $\mathbf{v}_{\mathcal{M}}$, via a sequence $\mathbf{r}_{\mathcal{M}}$ of elements of \mathcal{R} .

- (i) We let $\mathbf{r}_{\mathcal{M}}(0) = r_1$ and $\mathbf{v}_{\mathcal{M}}(0) = \tau(r_1)$
- (ii) For $n \ge 1$, we consider the proper representation of n in base q and we let

$$\mathbf{r}_{\mathcal{M}}(n) = \delta(\cdots \delta(\delta(r_1, \varepsilon_{\nu}(n)), \varepsilon_{\nu-1}(n)), \dots, \varepsilon_0(n))$$

and $\mathbf{v}_{\mathcal{M}}(n) = \tau(\mathbf{r}_{\mathcal{M}}(n)).$

It is convenient to consider the oriented graph where the vertices are \mathcal{R} and the oriented arrows are given by the map δ . In order to calculate $\mathbf{v}_{\mathcal{M}}(n)$, we start at r_1 and sequentially read the digits of n from the left to right, i.e. starting with $\varepsilon_{\nu}(n)$, going from one state to another on following the arrows numbered $\varepsilon_{\nu}, \varepsilon_{\nu-1}, \ldots, \varepsilon_0$. We thus arrive at a certain state $\mathbf{r}_{\mathcal{M}}(n)$ and the value of $\mathbf{v}_{\mathcal{M}}(n)$ is simply $\tau(\mathbf{r}_{\mathcal{M}}(n))$.

Definition 2.2. We say that a sequence $\mathbf{u} = (u(n))_{n \ge 0}$ with values in E is q-automatic, if there exists a q-automaton \mathcal{M} with values in E such that we have $u(n) = \mathbf{v}_{\mathcal{M}}(n)$ for all $n \ge 0$.

As already mentioned the most prominent automatic sequence (with q = 2) is the **Thue-Morse sequence**. Let us consider the 2-automaton \mathcal{T} defined by:

•
$$E = \{0, 1\}, \mathcal{R} = \{r_1, r_2\},\$$

- $\delta(r_1, 0) = \delta(r_2, 1) = r_1, \, \delta(r_2, 0) = \delta(r_1, 1) = r_2,$
- $\tau(r_1) = 0, \tau(r_2) = 1.$

Its graph (as described in the previous remark) is given in Figure 1. It is readily seen that the state denoted by $\mathbf{r}_{\mathcal{M}}(n)$ is r_1 if we have read an even number of 1's in the expansion of n in base 2, and is r_2 otherwise. Thus, due to the definition of τ we have

$$\mathbf{v}_{\mathcal{M}}(n) = s_2(n) \bmod 2,$$

which proves that T(n) is a 2-automatic sequence.



Figure 1. Automaton for the Thue-Morse sequence.

Another famous 2-automatic sequence is the **Rudin-Shapiro sequence** that can be defined by

$$R(n) = \sum_{j=0}^{\nu-1} \varepsilon_j(n) \varepsilon_{j+1}(n) \mod 2.$$

The corresponding automaton is depicted in Figure 2.



Figure 2. Automaton for the Rudin-Shapiro sequence.

Related to the graph representations of finite automata it is natural to consider the corresponding $d \times d$ transition matrices $M(k) = (m_{i,j}(k)), k \in \{0, 1, ..., q - 1\}$, such that

$$m_{ij}(k) = \begin{cases} 1 & \text{if } \delta(r_j, k) = r_i, \\ 0 & \text{otherwise.} \end{cases}$$

For example, for the Thue-Morse sequence, we have

$$M(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } M(1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The dynamics of the automaton \mathcal{M} , i.e. the sequence can be obtained in the following

way: For $n \ge 1$ with the digital representation $n = \sum_{i=0}^{\nu} \varepsilon_i(n) q^i$ in base q we have

$$M(\varepsilon_0(n))M(\varepsilon_1(n))\cdots M(\varepsilon_\nu(n))\mathbf{e}_1 = \mathbf{e}_{\mathbf{r}_\mathcal{M}(n)}$$

where \mathbf{e}_j , $1 \leq j \leq d$, denotes the canonical basis $(\mathbf{e}_j)_i = \delta_{ij}$. In the sequel, it will turn out to be convenient to introduce the notation

$$S(n) = M(\varepsilon_0(n))M(\varepsilon_1(n))\cdots M(\varepsilon_\nu(n)) \quad \text{for } n \ge 1 \text{ and } S(0) = \mathbf{I} = (\delta_{ij}).$$
(2.1)

In order to check whether $v_{\mathcal{M}}(n)$ is equal to a given value $a \in E$, we simply have to compute the product

$$\mathbf{z}_a^T \mathbf{e}_{r_{\mathcal{M}}(n)} = \mathbf{z}_a^T S(n) \mathbf{e}_1,$$

where the vector \mathbf{z}_a is defined by

$$(\mathbf{z}_a)_i = \begin{cases} 1 & \text{if } \tau(r_i) = a, \\ 0 & \text{otherwise.} \end{cases}$$

It is equal to 1 if $v_{\mathcal{M}}(n) = a$ and 0 otherwise. The advantage of this matrix representation is that, as shown by Peter [28], it permits to give a criterion for the existence of the asymptotic density with which the element $a \in E$ is recognized by $\mathbf{v}_{\mathcal{M}}$. We consider the matrix $M = (M(0) + \cdots + M(q-1))/q$ which is a stochastic matrix and, thus, there exists a positive integer m such that the sequence $(M^{km})_{k\geq 0}$ converges. In particular, Peter showed that the density

$$\operatorname{dens}(\mathbf{v}_{\mathcal{M}}, a) = \lim_{N \to \infty} \frac{1}{N} \# \{ 1 \le n < N : \mathbf{v}_{\mathcal{M}}(n) = a \}$$

exists if and only if for all $1 \le j \le d$ the limit

$$\lim_{k\to\infty} \mathbf{z}_a^T M^{mk} \mathbf{e}_1$$

exists. A special case of importance is the positive regular case, where M admits a power all the entries of which are positive: in this case $(M^k)_{k\geq 0}$ tends towards a matrix, where all the columns are equal and Peter's criterion is trivially satisfied.

In general the density dens($\mathbf{v}_{\mathcal{M}}, a$) needs not exist. Nevertheless the so-called logarithmic density

$$\log\text{-dens}(\mathbf{v}_{\mathcal{M}}, a) = \lim_{N \to \infty} \frac{1}{\log N} \sum_{1 \le n < N, \ \mathbf{v}_{\mathcal{M}}(n) = a} \frac{1}{n}$$

exists for all automatic sequences (see [1]).

For more properties of automatic sequences we refer to [1]. We only mention here that linear subsequences of q-automatic sequences $\mathbf{u} = (u(n))_{n\geq 0}$, that is, sequences of the form $(u(an + b))_{n\geq 0}$, are q-automatic, too. Thus, it is not necessary to consider linear subsequences of automatic sequences.

3 Subsequences along the sequence $\lfloor n^c \rfloor$

We start the discussion with subsequences of the form $\mathbf{v}_{\mathcal{M}}(\lfloor n^c \rfloor)$. There is a quite general theorem for c < 7/5 by Deshoulliers, Drmota, and Morgenbesser [6] (see also [22, 23]).

Theorem 3.1 ([6]). Let $q \ge 2$ and $\mathbf{u} = (u(n))_{n\ge 0}$ be a q-automatic sequence with values in a finite set E and 1 < c < 7/5. Then we have for every $a \in E$:

- (i) The quantity log-dens $(u(\lfloor n^c \rfloor), a)$ exists and is equal to log-dens (\mathbf{u}, a) .
- (ii) The quantity dens(u([n^c], a) exists if and only if dens(u, a) exists, and in this case, they are equal.

This means that the overall behavior does not change if we consider subsequences of this form. The condition c < 7/5 looks artificial and is certainly an Artifact of the proof method. Therefore the following conjecture is quite natural.

Conjecture 3.2. The statement of Theorem 3.1 holds for all non-integers c > 1.

Actually there are some partial results into this direction. For example it was shown by Morgenbesser [27] that for every non-integer c > 0 there exists $q_0(c) \ge 2$ such that for all $q \ge q_0(c)$

$$\sum_{\leq n < N} e\left(\alpha s_q(\lfloor n^c \rfloor)\right) \ll \left(\log N\right) N^{1 - \sigma_{c,q} \| (q-1)\alpha \|^2}$$
(3.1)

for some $\sigma_{c,q} > 0$; as usual $e(x) = e^{2\pi i x}$ and $||x|| = \min\{|x - k| : k \in \mathbb{Z}\}$. As a corollary he obtains the following theorem.

Theorem 3.3 ([27]). For every non-integer c > 0 there exists $q_0(c) \ge 2$ such that for all $q \ge q_0(c)$

$$\#\{1 \le n < N : s_q(\lfloor n^c \rfloor) \equiv \ell \mod m\} = \frac{N}{m} + O\left(N^{1 - \eta_q/m^2}\right)$$
(3.2)

for some $\eta_q > 0$ and all integers ℓ, m .

1

On the other hand if we fix the base q and search for those c > 1 for which Theorem 3.1 holds there is no general improvement. Only recently Spiegelhofer [29] could improve the upper bound 7/5 = 1.4 to 1.42 in the case of the Thue-Morse sequence. We add that it was pointed out by Mauduit (see [21, Section II.4]), that (3.2) holds for almost all $c \in [1, 2)$ (and this follows from a result of Harman and Rivat [14]).

The next problem concerns the distribution of consecutive blocks of the sequence $u(\lfloor n^c \rfloor)$. The only known result into this direction is the following one due to Deshoulliers, Drmota, and Morgenbesser [6].

Theorem 3.4 ([6]). Let $c \in (1, 10/9)$ and let T(n) denote the Thue-Morse sequence. Then for every pair $(a, b) \in \{0, 1\}^2$ we have

$$\lim_{N \to \infty} \frac{1}{N} \# \{ 1 \le n < N : (T(\lfloor n^c \rfloor), T(\lfloor (n+1)^c \rfloor)) = (a,b) \} = \frac{1}{4}.$$

This means that all blocks of length 2 appear with the *right frequency*. It is natural to ask whether this property could be improved.

Conjecture 3.5. For every non-integer c > 1 the sequence $T(\lfloor n^c \rfloor)$ is normal, that is, every block of length L appears with asymptotic frequency 2^{-L} .

Unfortunately there is no single c > 1 for which this conjecture could be proved so far. We just mention that by extending the methods of [6] it is possible to prove that for every $L \ge 1$ there exists $c_L > 0$ such that every block of length L appears with asymptotic frequency 2^{-L} in the sequence $T(\lfloor n^c \rfloor)$, provided that $1 < c \le c_L$. The problem is that $c_L \to 1$ as $L \to \infty$.

In order to obtain results like Theorems 3.1-3.4 several proof methods have been established. For example the proof of Theorem 3.1 is an extension of the methods of Mauduit and Rivat [23], who have shown that for all q-multiplicative functions f, that is, f(aq + b) = f(a)f(b) for $a \ge 1$ and $0 \le b < q$, we have

$$\left| \sum_{1 \le n < N} f(\lfloor n^c \rfloor) - \frac{1}{c} \sum_{1 \le m < N^c} m^{1/c - 1} f(m) \right| \ll N^{1 - \delta}$$
(3.3)

for $c \in (1, 7/5)$ and all $\delta \in (0, (7-5c)/9)$. The proof relies on Vaaler's approximation method and on a proper application of the double large sieve of Bombieri and Iwaniec.

Of course, a function of the form $f(n) = e(\alpha s_q(n))$ is q-multiplicative and so (3.3) can be applied and proves the result in this case (after partial summation). In order to handle general automatic sequences one has to generalize (3.3) to matrix valued sequences of the form S(n) which behave like q-multiplicative functions.

It is, however, very unlikely that an inequality of the form (3.3) should hold for arbitrarily large *c*. Therefore it is probably impossible to settle Conjecture 3.2 by this method. As already mentioned Mauduit and Rivat [24, 25] introduced a Fourier analytic method (in order to settle some parts of the Gelfond problems). We indicate next how this Fourier analytic method can be used to prove (3.1) and consequently Theorem 3.3.

For every integer $\lambda \geq 0$ let $s_{q,\lambda}$ be defined by

$$s_{q,\lambda}(n+kq^{\lambda}) = s_2(n), \quad 0 \le n < q^{\lambda}, \ k \ge 0.$$

So $s_{q,\lambda}$ is periodic with period q^{λ} and we are led to introduce the discrete Fourier transform

$$F_{\lambda}(h,\alpha) = \frac{1}{q^{\lambda}} \sum_{0 \le u < q^{\lambda}} e(\alpha s_{q,\lambda}(u) - huq^{-\lambda})$$

of the function $n \mapsto e(\alpha s_{q,\lambda}(n))$. With the help of these terms we can rewrite the exponential sum (3.1) to

$$\sum_{0 \le n < N} e(\alpha s_q(\lfloor n^c \rfloor)) = \sum_{0 \le h < q^{\lambda}} F_{\lambda}(h, \alpha) \sum_{0 \le n < N} e(h \lfloor n^c \rfloor) q^{-\lambda}),$$

where λ is defined by $q^{\lambda-1} < N^c \leq q^{\lambda}$. Now the problem can be split into two (almost) independent parts.

First, there are exponential sums of the form

$$\sum_{0 \leq n < N} e(\beta \lfloor n^c \rfloor))$$

that can be handled by standard tools (see [27]) and usually lead to upper bounds of the form $\ll N^{1-\eta}$ for some $\eta > 0$ (that depends on β and c).

Second there is a remarkable L_1 estimate for the Fourier terms $F_{\lambda}(h, \alpha)$ of the form (see [24, 8])

$$\sum_{0 \le h < q^{\lambda}} |F_{\lambda}(h, \alpha)| \le q^{\eta_q \lambda}, \tag{3.4}$$

where η_q satisfies

$$\eta_q \le \frac{\log\left(\frac{2}{q\sin\frac{\pi}{2q}} + \frac{2}{\pi}\log\frac{2q}{\pi}\right)}{\log q}.$$
(3.5)

In particular $\eta_q \to 0$ as $q \to \infty$. Thus, if q is sufficiently large then by combining the estimates for the exponential sums and (3.4) leads to (3.1). (Of course we have over simplified the proof but the main ideas should be clear).

We remark that this method only works if q is sufficiently large (so that the Fourier part is small) or if c is close to 1 (so that that the exponential sums are small). For the proof of Theorem 3.3 we applied the first variant whereas the second variant can be used to prove Theorem 3.4.

As above the exponential sum

$$\sum_{0 \le n < N} e\left(\alpha_0 s_2(\lfloor n^c \rfloor) + \alpha_1 s_2(\lfloor (n+1)^c \rfloor)\right)$$

is replaced by the sum

$$\sum_{0 \le h_0, h_1 < 2^{\lambda}} F_{\lambda}(h_0, \alpha_0) F_{\lambda}(h_1, \alpha_1) \sum_{0 \le n < N} e\left((h_0 \lfloor n^c \rfloor + h_1 \lfloor (n+1)^c \rfloor) 2^{-\lambda} \right)$$

By assuming that c < 10/9 it is possible to obtain proper estimates for the exponential sums so that it is sufficient to estimate the Fourier part by (3.4) with 0.4428 $< \eta_2 < 0.4429$, see [6].

4 Polynomial subsequences

In Section 3 we have excluded the integer case for c. Actually, there are several differences between the integer and the non-integer case. On the one hand functions like $P(n) = n^2$ are easier to handle than functions of the form $\lfloor n^{3/2} \rfloor$. For example, the difference $P(n+r) - P(n) = (n+r)^2 - n^2 = 2nr + r^2$ is a linear polynomial whereas the exact behaviour of the difference $\lfloor (n+r)^{3/2} \rfloor - \lfloor n^{3/2} \rfloor$ is quite erratic. On the other hand the *irregularity* of $\lfloor n^c \rfloor$ for non-integers c might be also an advantage. For example the distribution of $\lfloor n^c \rfloor$ mod m is always asymptotically uniform modulo mwhich is not true for integer exponents (as the example $n^2 \mod 4$ shows).

It is therefore not that unexpected that we have to apply a different method for $\mathbf{u}(n^2)$ (and other polynomial subsequences).

We start with a quite general result on so-called invertible automatic sequences.

Definition 4.1. Let $\mathbf{u} = (u(n))_{n\geq 0}$ be a *q*-automatic sequence. Then we call \mathbf{u} an invertible *q*-automatic sequence if there exists an automaton such that all transition matrices are invertible and such that the transition matrix of zero is given by the identity matrix.

For example, the Thue-Morse sequence is an invertible 2-automatic sequence but the Rudin-Shapiro sequence is not invertible.

It is easy to show that the densities $dens(\mathbf{u}, a)$ exist for invertible automatic sequences. However, it is a non-trivial result that the same property holds for the subsequence along squares (this is a result by Drmota and Morgenbesser [10]).

Theorem 4.2 ([10]). Let $q \ge 2$ and $\mathbf{u} = (u(n))_{n\ge 0}$ an invertible q-automatic sequence. Then the densities dens $(u(n^2), a)$ exist for each letter $a \in E$.

In general it is not true that the densities dens(u(n), a) and $dens(u(n^2), a)$ coincide. Nevertheless it is always possible to calculate them explicitly. (They depend on the structure of representation of the group that is generated by the matrices $M(0), M(1), \ldots, M(q-1)$, for details see [10]). However, if q = 2 then they always coincide. In particular this applies to the Thue-Morse sequence T(n) and so we get

dens
$$(T(n^2), 0) = dens(T(n^2), 1) = \frac{1}{2}$$

Actually this is part of the Gelfond problems (since $T(n^2) = s_2(n^2) \mod 2$) and has been first proved by Mauduit and Rivat [25]. (By the way it was already shown by Dartyge and Tenenbaum [5] that the lower densities of the letter 0 and 1 of the sequence $T(n^2)$ are strictly positive but their method could not be extended to settle the Gelfond conjecture). More precisely Mauduit and Rivat have shown that

$$\sum_{1 \le n < N} e\left(\alpha s_q(n^2)\right) \ll (\log N)^{c_q} N^{1 - \sigma_q \| (q-1)\alpha \|^2}$$
(4.1)

for some positive constants c_q, σ_q . In particular this implies that

$$\#\{1 \le n < N : s_q(n^2) \equiv \ell \mod m\} = \frac{N}{m}Q(\ell, d) + O\left(N^{1 - \sigma_q/m^2}\right),$$

where d = (q - 1, m) and $Q(\ell, d) = \#\{0 \le m < d : m^2 \equiv \ell \mod d\}.$

The next question is of course, the distribution of consecutive blocks. Recently, Drmota, Mauduit and Rivat [9] could handle the case of the Thue-Morse sequence.

Theorem 4.3 ([9]). Let $(T(n))_{n\geq 0}$ denote the Thue-Morse sequence. Then the sequence $(T(n^2))_{n>0}$ is normal on the alphabet $\{0, 1\}$.

It is easy to extend Theorems 4.2 and 4.3 to arbitrary integer polynomials of degree 2. However, for polynomials of higher degree there is only a partial result (similarly to Theorem 3.3).

Theorem 4.4 ([8]). For every $d \ge 2$ there exists $q_0(d) \ge 2$ such that for all prime $q \ge q_0(c)$ and all integer polynomials P(x) of degree d (where the leading coefficient if coprime to q)

$$\#\{1 \le n < N : s_q(P(n)) \equiv \ell \mod m\} = \frac{N}{m} + O\left(N^{1-\eta}\right)$$
(4.2)

for some $\eta > 0$ and all integers m with (m, q - 1) = 1.

This leads us to the following conjecture that is an extension of the corresponding Gelfond problem.

Conjecture 4.5. Suppose that (q-1,m) = 1. Then for every integer polynomial P(x) of degree ≥ 2 the sequence $s_q(P(n)) \mod m$ is normal on the alphabet $\{0, 1, \ldots, q-1\}$.

For the sake of shortness we only indicate how exponential sums of the form

$$S_0 = \sum_{0 \le n < N} e\left(\alpha s_q(n^2)\right)$$

can be handled. With the help of two applications of Van-der-Corput type inequalities the original problem is reduced to finding an upper bound of the exponential sum

$$S_1 = \sum_{0 \le n < N} e\left(\alpha \left(s_q(n^2) - s_q((n+r)^2) - s_q((n+t2^{\mu})^2) + s_q((n+r+t2^{\mu})^2)\right)\right),$$

where $q^{\mu} < N$, $1 \le r \le q^{\lambda}/N$, $1 \le t \le N/q^{\mu}$ (and λ satisfies $q^{\lambda} > N$).

Let $s_{q,\mu,\lambda}(n) = s_{q,\lambda}(n) - s_{q,\mu}(n)$ the partial sum of digits $\sum_{\mu \leq j < \lambda} \varepsilon_j(n)$. The first (elementary) observation is that the double differences of s_q and $s_{q,\mu,\lambda}$ coindice with at most $O(N\sqrt{N/q^{\lambda}}) = o(N)$ exceptions:

$$s_q(n^2) - s_q((n+r)^2) - s_q((n+t2^{\mu})^2) + s_q((n+r+t2^{\mu})^2)$$

= $s_{q,\mu,\lambda}(n^2) - s_{q,\mu,\lambda}((n+r)^2) - s_{q,\mu,\lambda}((n+t2^{\mu})^2) + s_{q,\mu,\lambda}((n+r+t2^{\mu})^2).$

Thus, it is sufficient to consider the exponential sum

$$S_{2} = \sum_{0 \le n < N} e \left(\alpha \left(s_{q,\mu,\lambda} (n^{2}) - s_{q,\mu,\lambda} ((n+r)^{2}) - s_{q,\mu,\lambda} ((n+t2^{\mu})^{2}) + s_{q,\mu,\lambda} ((n+r+t2^{\mu})^{2}) \right) \right)$$

The second step is to use a proper Fourier analysis in order to relate S_2 with

$$S_{3} = \sum_{|h_{1}|,|h_{2}|,|h_{3}|,|h_{4}| \leq H} F_{\lambda-\mu}(h_{1},\alpha) \overline{F_{\lambda-\mu}(h_{2},\alpha)F_{\lambda-\mu}(h_{3},\alpha)} F_{\lambda-\mu}(h_{4},\alpha)$$
$$\times \sum_{0 \leq n < N} e\left(\left(h_{1}n^{2} + h_{2}(n+r)^{2} + h_{3}(n+tq^{\mu})^{2} + h_{4}(n+r+tq^{\mu})^{2}\right) q^{-\lambda} \right),$$

where $H = q^{\lambda - \mu + \rho}$ (for some $\rho > 0$). As in Section 3 the problem is now to deal with the exponential sum part and a Fourier part in a proper way. The exponential sums are either quadratic or linear and, thus, easy to handle (one just has to take more or less care of the trivial sums – but this part is more subtle that it looks at a first glance). Finally we have to apply proper estimates for the Fourier terms. We do not go into details but the main ingredient is that there is a bound of the form

$$|F_{\lambda-\mu}(h,\alpha)| \le 2^{-c_q \|(q-1)\alpha\|^2 (\lambda-\mu)}$$

for a proper constant $c_q > 0$. This leads to a proof of (4.1).

The proof of Theorem 4.3 is much more involved than that of (4.1) but uses related ideas. One essential difference is that one has to use more general Fourier terms of the form

$$G_{\lambda}(h,d) = \frac{1}{2^{\lambda}} \sum_{0 \le u < 2^{\lambda}} e\left(\sum_{\ell=0}^{k-1} \alpha_{\ell} s_{2,\lambda}(u+\ell d) - h 2^{-\lambda}\right)$$

Finally, a proof of Theorem 4.4 can be worked out in a way similar to the proof of Theorem 3.3.

5 Subsequences along the primes

The second Gelfond problem was recently solved by Mauduit and Rivat [24] (see also [16]). However, the approach of [16, 24] is limited to those kind of sequences, where a

non-trivial L_1 bound for the Fourier terms of type (3.4) is satisfied for some $\eta_q < 1/2$. In particular this kind of bounds is not valid for the Rudin-Shapiro sequence (where the best exponent equals the trivial exponent 1/2), so this approach is certainly not applicable for general automatic sequences. Nevertheless there is a very interesting (recent) variant by Mauduit and Rivat [26] that we describe next.

Let $\mathbf{u} = (u(n))_{n \ge 0}$ be an automatic sequence on the alphabet $E = \{0, 1, \dots, m-1\}$. In order to study the densities $dens((u(p))_{p \in \mathbb{P}}, a)$ of the subsequence of primes it is sufficient to study the exponential sums

$$\sum_{\langle N, \ p \in \mathbb{P}} e(\alpha u(p)), \tag{5.1}$$

where $\alpha \in \{0, 1/m, 2/m, \dots, (m-1)/m\}$. This means that we are led to consider sums of the form $\sum_{p \in \mathbb{P}} f(p)$, where |f(n)| = 1. Actually, in the context of sums over primes it is convenient to study first the sum

$$\sum_{1 \le n < N} \Lambda(n) e(\alpha u(n)), \tag{5.2}$$

where $\Lambda(n)$ denotes the Von Mangoldt function (that is defined by $\Lambda(n) = \log p$ if $n = p^k$ for some prime p and some integer $k \ge 1$, and $\Lambda(n) = 0$ otherwise). By partial summation it follows (for example) that

$$\left|\sum_{p < N, \ p \in \mathbb{P}} e(\alpha u(p))\right| \leq \frac{2}{\log N} \max_{M \leq N} \left|\sum_{n \leq M} \Lambda(n) e(\alpha u(n))\right| + O(\sqrt{N}).$$

Thus, upper bounds for (5.2) imply upper bounds for (5.1), too.

Mauduit and Rivat [26] formulated two conditions on a sequence f(n) (with |f(n)| = 1) that should be satisfied in order to estimate (5.2) in a non-trivial way.

Let $q \ge 2$ and $(f(n))_{n\ge 0}$ be a sequence with |f(n)| = 1 for all $n \ge 0$. Furthermore for a non-negative integer λ let f_{λ} denote the q^{λ} -periodic function defined by

$$f_{\lambda}(n+kq^{\lambda}) = f(n), \quad 0 \le n < q^{\lambda}, \ k \ge 0$$

(i) We say that f has the carry property if, uniformly for λ, κ, ρ ≥ 0 with ρ < λ, the number of integers 0 ≤ ℓ < q^λ such that there exists k₁, k₂ ∈ {0, 1, ..., q^κ − 1} with

$$f(\ell q^{\kappa} + k_1 + k_2)\overline{f(\ell q^{\kappa} + k_1)} \neq f_{\kappa+\rho}(\ell q^{\kappa} + k_1 + k_2)\overline{f_{\kappa+\rho}(\ell q^{\kappa} + k_1)}$$

is at most $O(q^{\lambda-\rho})$, where the implied constant may depend on q and f.

(ii) Second, we say that f has the Fourier property if there exists a non-decreasing real function γ with lim_{λ→∞} γ(λ) = +∞ and a constant c > 0 such that for all non-negative integers λ, κ ≥ 0 with κ ≤ cλ and real t

$$\left|\frac{1}{q^{\lambda}}\sum_{0 \le u < q^{\lambda}} f(uq^{\kappa})e(-ut)\right| \le q^{-\gamma(\lambda)}$$

It turns out that the Fourier property is (usually) more difficult to establish. Nevertheless there are several interesting examples for which it holds. If $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$ then it follows from [25, Lemme 9] that the sequence

$$f(n) = e(\alpha s_q(n))$$

satisfies the Fourier property (for any c > 0) with

$$\gamma(\lambda) = \frac{\pi^2}{12\log q} \left(1 - \frac{2}{q+1} \right) \|(q-1)\alpha\|^2 \lambda - \frac{\pi^2}{48\log q}.$$

Since the carry properly holds, too, these two properties are satisfied in the context of the sum-of-digits function.

The main result of [26] is the following one.

Theorem 5.1 ([26]). Suppose that f has the carry and the Fourier property (for some $c \ge 10$) Then we have for real ϑ

$$\left|\sum_{n < N} \Lambda(n) f(n) e(\vartheta n)\right| \ll c_1(q) (\log N)^{c_2(q)} N q^{-\gamma(2\lfloor (\log N)/(80 \log q) \rfloor)/20}$$

for some (explicit) positive constants $c_1(q), c_2(q)$.

Theorem 5.1 applies directly to the sequence $f(n) = e(\alpha s_q(n))$ and solves the second Gelfond problem.

Corollary 5.2. Let $q \ge 2$ and (q - 1, m) = 1. Then we have

$$\#\{p < N : p \in \mathbb{P}, \ s_q(p) \equiv \ell \mod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

for some $\eta > 0$.

It should be mentioned that there are earlier but not that strong results on the subsequence of P_2 -numbers (that are either prime or the product of two primes) [11, 12] and on numbers with precisely k prime factors (with $k \ge 2$) [4].

As already mentioned the original method by Mauduit and Rivat [24] does not apply to the Rudin-Shapiro sequence R(n). However, it can be shown (see [26]) that R(n)satisfies the carry and the Fourier property. Thus, we also obtain the following result.

Corollary 5.3. Let R(n) denote the Rudin-Shapiro sequence. Then we have

$$\operatorname{dens}((R(p))_{p\in\mathbb{P}},0) = \operatorname{dens}((R(p))_{p\in\mathbb{P}},1) = \frac{1}{2}.$$

We get the same relation for Rudin-Shapiro sequences $R_d(n)$ of higher degree, too, that are defined by

$$R_d(n) = \sum_{j=0}^{\mu-d} \varepsilon_j(n) \varepsilon_{j+1}(n) \cdots \varepsilon_{j+d}(n).$$

It is quite natural to conjecture that similar relations hold for general automatic sequences (at least for the logarithmic density).

Conjecture 5.4. For every automatic sequence $\mathbf{u} = (u(n))_{n \ge 0}$ the logarithmic densities log-dens $(u(p)_{p \in \mathbb{P}}, a)$ exist for all letters $a \in E$.

At the moment we can just say that Conjecture 5.4 is true for invertible automatic sequences. (Actually this is a new result.)

Theorem 5.5. Let $q \ge 2$ and $\mathbf{u} = (u(n))_{n\ge 0}$ an invertible q-automatic sequence. Then the densities dens $((u(p))_{p\in\mathbb{P}}, a)$ exist for each letter $a \in E$.

We will sketch the proof of Theorem 5.5 at the end of this section for which we will need some ideas of the proof of Theorem 5.1. So we discuss this proof first.

The basic idea of the proof of Theorem 5.1 is to use Vaughan's method adapted to the situation (see [24]).

Lemma 5.6. Let $q \ge 2$ $N \ge q^2$, $0 < \beta_1 < 1/3$, $1/2 < \beta_2 < 1$, and f(n) a sequence with |f(n)| = 1. Suppose that for all $M \le N^{\beta_1}$

$$\sum_{M/q < m \le M} \max_{\frac{N}{qm} \le t \le \frac{N}{m}} \left| \sum_{t < n \le \frac{N}{m}} f(mn) \right| \le U$$
(5.3)

and for $N^{\beta_1} \leq M \leq N^{\beta_2}$ and for all sequences a_m , b_n with $|a_m| \leq 1$ and $|b_n| \leq 1$

$$\left| \sum_{\frac{M}{q} < m \le M} \sum_{\frac{N}{qm} < n \le \frac{N}{m}} a_m b_n f(mn) \right| \le U,$$
(5.4)

then we have

$$\left| \sum_{N/q < n \le N} \Lambda(n) f(n) \right| \ll U (\log N)^2.$$

The second (and quite involved) step is to estimate the exponential sums that appear in (5.3) and (5.4) by an approach that is similar to the one for squares. Two applications of the Van-der-Corput inequality (together with the carry property) reduce the problem to functions that depend only on few digits (similarly to the case of squares). Finally by applying a proper Fourier theoretic approach the remaining sums are separated into a Fourier part and a exponential sum part. And these parts can be handled with the help of the Fourier property and by standard exponential sum estimates. (This part is indeed very involved and technical.)

Finally we sketch the proof of Theorem 5.5. By definition the transition matrices M(j), $0 \leq j < q$, are invertible and, thus, permutation matrices. Consequently the group G that is generated by M(j), $0 \leq j < q$, is a (finite) subgroup of the symmetric group S_q . The idea of the proof is to show that the sequence $(S(p))_{p \in \mathbb{P}}$ (recall that S(n) is defined by (2.1)) has a limiting distribution in G, that is, every element $g \in G$ has an asymptotic density along the sequence $(S(p))_{p \in \mathbb{P}}$. Since $\mathbf{v}_{\mathcal{M}}(p)$ can be described with the help of the functionals $\mathbf{z}_a S(p) \mathbf{e}_1$ we obtain then Theorem 5.5 as a corollary.

In order to show that $(S(p))_{p\in\mathbb{P}}$ has a limiting distribution ν on G it is sufficient to show that the limiting relations

$$\lim_{N \to \infty} \frac{1}{\pi(N)} \sum_{p < N, \, p \in \mathbb{P}} D(S(p)) = \int_G D \, d\nu \tag{5.5}$$

hold for all unitary irreducible representations D on G (see [10]).

In the present situation there are two kinds of irreducible representations that we have to consider. First there exists a largest positive integer m = m(G) (a divisor of q - 1) with the property that there is a one-dimensional representation D of G with

$$D(M(j)) = e(-j/m) \quad \text{for } 0 \le j < q.$$

The representations $D_k = D^k$, $0 \le k < m$, form a cyclic group of representations. These representations will be handled separately from the others.

In particular for $D = D_k$ we have (since $s_q(n) \equiv n \mod q - 1$)

$$D(S(n)) = e(-k s_q(n)/m) = e(-kn/m)$$

and consequently

$$\sum_{p < N, p \in \mathbb{P}} D(S(p)) = \sum_{p < N, p \in \mathbb{P}} e(-kp/m) \sim \frac{\pi(N)}{\varphi(m)} \sum_{0 \le u < m, (u,m)=1} e(-ku/m).$$

Finally, let D be a unitary irreducible representation of G that is different from D_k , $0 \le j < m$. Then by [10, Lemma 4] the (matrix valued) Fourier terms

$$\mathbf{F}_{\lambda}(t) = \frac{1}{q^{\lambda}} \sum_{0 \le u < q^{\lambda}} D(S(n)) e^{-ut}$$

satisfy

$$\sup_{t\in\mathbb{R}} \|\mathbf{F}_{\lambda}(t)\| \ll q^{-c\lambda}$$

for some c > 0, where $\|\cdot\|$ denotes any matrix norm. Since $S(q^{\kappa}n) = S(n)$ it follows that the matrix valued function D(S(n)) satisfies a *Fourier property*. The corresponding *carry property* is also satisfied (see [10]). Hence we can mimic the proof of Theorem 5.1 (from [26]), where f(n) is replaced by D(S(n)). The only difference is that the matrix multiplication is not commutative. However, in all relevant estimates (in particular in Van-der-Corput type inequalities for matrices, see [10, Lemma 6]) the right hand side (of the inequalities) depends on the trace of a sum of producs of matrices. Since the trace tr satisfies $tr(A \cdot B) = tr(B \cdot A)$ it is possible to overcome this potential difficulty. (Actually these ideas were already used in [10]).

Summing up this means that for all unitary irreducible representations D that are different from D_k , $0 \le k < m$, we obtain

$$\sum_{0 \le n < N} \Lambda(n) D(S(n)) = O(N^{1-\eta})$$

for some $\eta > 0$.

We recall that the group G is generated by the transition matrices M(j), $0 \le j < q$. Next let U be the subgroup of G that is generated by S(mn), $n \ge 0$, where m = m(G). It was shown in [10] that U is a subgroup of G of index m and that M(j)U, $0 \le j < m$, are the cosets of U. Furthermore set

$$C = \bigcup_{0 \le j < m, (j,m)=1} M(j)U$$

and let ν denote the normalized counting measure on C, that is,

$$\nu(S) = \frac{\#(C \cap U)}{\#C}.$$

It is an easy exercise to show that (5.5) is satisfied for this measure ν . As mentioned above this completes the proof of Theorem 5.5.

Bibliography

- [1] J.-P. Allouche and J. Shallit, *Automatic sequences. Theory, applications, generalizations,* Cambridge University Press, Cambridge, 2003.
- [2] Y. Bugeaud, Automatic continued fractions are transcendental or quadratic. *Ann. Sci. École Norm. Sup.*, to appear.
- [3] J. Bésineau, Indépendance statistique d'ensembles liés à la fonction "somme des chiffres", Acta Arith. 20 (1972), 401–416.

- [4] C. Dartyge and G. Tenenbaum, Sommes des chiffres de multiples d'entiers, Ann. Inst. Fourier 55 (2005), no. 7, 2423–2474.
- [5] C. Dartyge and G. Tenenbaum, Congruences de sommes de chiffres de valeurs polynomiales, *Bull. London Math. Soc.* 38 (2006), no. 1, 61–69.
- [6] J.-M. Deshoulliers, M. Drmota, and J. Morgenbesser, Subsequences of automatic sequences indexed by $|n^c|$ and correlations, *J. Number Theory* **132** (2012), 1837–1866.
- [7] M. Drmota and P.J. Grabner, Analysis of digital functions and applications. Combinatorics, automata and number theory, 452–504, Encyclopedia Math. Appl., 135, Cambridge Univ. Press, Cambridge, 2010.
- [8] M. Drmota, C. Mauduit, and J. Rivat, The sum-of-digits function of polynomial sequences, J. Lond. Math. Soc. (2) 84 (2011), no. 1, 81–102.
- [9] M. Drmota, C. Mauduit, and J. Rivat, The Thue-Morse sequence along squares is normal, *manuscript*.
- [10] M. Drmota and J. Morgenbesser, Israel J. Math. 190 (2012), 157-193.
- [11] E. Fouvry and C. Mauduit, Méthodes de crible et fonctions sommes des chiffres, Acta Arith. 77 (1996), no. 4, 339–351.
- [12] E. Fouvry and C. Mauduit, Sommes des chiffres et nombres presque premiers, *Math. Ann.* 305 (1996), no. 3, 571–599.
- [13] A.O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données. Acta Arith. 13 1967/1968 259–265.
- [14] G. Harman and J. Rivat, Primes of the form $[p^c]$ and related questions, *Glasgow Math. J.* **37** (1995), 131–141.
- [15] D.-H. Kim, On the joint distribution of q-additive functions in residue classes, J. Number Theory 74 (1999), no. 2, 307–336.
- [16] B. Martin, C. Mauduit, and J. Rivat, Théorème des nombres premiers pour les fonctions digitales, *manuscript*.
- [17] C. Mauduit, Automates finis et équirépartition modulo 1, C. R. Acad. Sci. Paris Sér. I Math. 299 (1984), no. 5, 121–123.
- [18] C. Mauduit, Automates finis et ensembles normaux, Ann. Inst. Fourier (Grenoble) 36 (1986), no. 2, 1Ű-25.
- [19] C. Mauduit, Substitutions et équirépartition modulo 1, Colloque de Théorie Analytique des Nombres "Jean Coquet" (Marseille, 1985), 85-Ű89, Publ. Math. Orsay, 88-02, Univ. Paris XI, Orsay, 1988.
- [20] C. Mauduit, Caractérisation des ensembles normaux substitutifs, *Invent. Math.* 95 (1989), no. 1, 133–147.
- [21] C. Mauduit, Multiplicative properties of the Thue-Morse sequence, *Period. Math. Hun-gar.* 43 (2001), 137–153.
- [22] C. Mauduit and J. Rivat, Répartition des fonctions q-multiplicatives dans la suite $(|n^c|)_{n\in\mathbb{N}}, c > 1$, Acta Arith. **71** (1995), 171–179.

- [23] C. Mauduit and J. Rivat, Propriétés q-multiplicatives de la suite $\lfloor n^c \rfloor$, Acta Arith. 118 (2005), 187–203.
- [24] C. Mauduit and J. Rivat, La somme des chiffres des carrés, Acta Math. 203 (2009), no. 1, 107–148.
- [25] C. Mauduit and J. Rivat, Sur un problème de Gelfond: la somme des chiffres des nombres premiers, Ann. of Math. (2) 171 (2010), no. 3, 1591–1646.
- [26] C. Mauduit and J. Rivat, Prime numbers along Rudin-Shapiro sequences, manuscript.
- [27] J. Morgenbesser, The sum of digits of $|n^c|$, Acta Arith. 148 (2011), no. 4, 367–393.
- [28] M. Peter, The asymptotic distribution of elements in automatic sequences, *Theoret. Comput. Sci.*, (1-3) **301** (2003) 285–312.
- [29] L. Spiegelhofer, Piatetski-Shapiro sequences via Beatty sequences, manuscript.

Author information

Michael Drmota, Institut of Discrete Mathematics and Geometry, TU Wien, Wiedner Hauptstr. 8–10, 1040 Wien, Austria. E-mail: michael.drmota@tuwien.ac.at