Uniform Distribution Theory **8** (2013), no.2, 121–140

uniform distribution theory

DISTRIBUTION PROPERTIES OF CERTAIN SUBSEQUENCES OF DIGITAL SEQUENCES AND THEIR HYBRID VERSION

Roswitha Hofer—Heidrun Zellinger

ABSTRACT. This paper investigates the distribution properties of subsequences of digital sequences and their hybrid version for the special case of finite-row generating matrices and states new criterions on the index sequence which can be used to decide the uniform distribution of the corresponding subsequence. These criterions are related to earlier ones and they are applied to previously considered examples. Furthermore, a detailed study of power residues in different congruence classes is carried out, which together with the new criterions allows to give a full classification of all finite-row generating matrices that yield uniformly distributed subsequences if they are indexed by a sequence $(n^p)_{n\geq 0}$ of fixed prime exponent.

Communicated by W.G. Nowak

1. Introduction

The study of the distribution properties of subsequences is related to challenging number theoretical questions and therefore an interesting task in pure mathematics. In 1968 Gelfond [3] stated several open problems concerning the uniform distribution of the sum of digits indexed by the sequence of primes or indexed by polynomial sequences. The uniform distribution of those subsequences was recently studied by Rivat and Mauduit for primes [15] and squares [14], and for certain polynomials [2] in a joint paper with Drmota.

A further topic up to date in the theory of uniform distribution is the distribution of hybrid sequences. A hybrid sequence is built by concatenating the components of two or more different types of sequences to a higher dimensional sequence. One aim is to combine the properties of the component sequences

2010 Mathematics Subject Classification: 11K06 and 11K31.
Keywords: Uniform Distribution, digital sequences, hybrid sequences, subsequences, weighted sum of digits, power residues.
Both authors are supported by the Austrian Science Fund (FWF), Project P21943.

which is, for instance, interesting for numerical integration based on quasi-Monte Carlo methods where the elements of the sequence serve as sampling points. Another reason for building hybrid sequences is to obtain new types of sequences which may have interesting distribution properties. Recent methods for the investigation of the distribution of hybrid sequences need information on the distribution of special subsequences of the component sequences. For example, for a hybrid sequence with a Halton component sequence one needs to study arithmetic subsequences of the component sequences. Recently, a series of papers was devoted to the distribution properties of hybrid sequences (see, for example, [4] and [12] and the references therein). Hybrid sequences, where one or more component sequences are digital sequences, appear as particularly difficult to study objects and the investigation of their distribution properties is still in its infancy. One reason is, that the known methods need information about the finer distribution properties of digital sequences, and the investigation of those needs involved techniques.

In this paper we investigate the distribution properties of subsequences of digital sequences and of their hybrid version. Throughout the paper $\mathbb{F}_q$ with q prime denotes the finite field of residue classes modulo q which we identify with the set of representatives $\{0, 1, \ldots, q-1\}$. For two points $\boldsymbol{a}, \boldsymbol{b} \in [0,1)^s$ the interval $\{\boldsymbol{x} \in [0,1)^s : \boldsymbol{a} \leq \boldsymbol{x} < \boldsymbol{b}\}$, where the inequalities $\leq$ and $<$ are meant to hold coordinatewise, is abbreviated to $[\boldsymbol{a}, \boldsymbol{b})$. Furthermore, $(k_n)_{n\geq 0}$ always denotes a sequence in $\mathbb{N}_0$. Although $(k_n)_{n\geq 0}$ is not necessarily increasing we call the sequence $(\boldsymbol{x}_{k_n})_{n\geq 0}$ a *subsequence of* $(\boldsymbol{x}_n)_{n\geq 0}$.

A sequence $(\boldsymbol{x}_n)_{n\geq 0}$ in the s-dimensional unit cube $[0,1)^s$ is said to be *uniformly distributed* if for all intervals $[\boldsymbol{a}, \boldsymbol{b}) \subseteq [0,1)^s$ we have

$$\lim_{N\to\infty} \frac{\#\{n : 0 \leq n < N, \boldsymbol{x}_n \in [\boldsymbol{a}, \boldsymbol{b})\}}{N} = \lambda([\boldsymbol{a}, \boldsymbol{b})),$$

where λ denotes the s-dimensional Lebesgue measure.

A sequence $(k_n)_{n\geq 0}$ of integers is said to be uniformly distributed modulo an integer $r \geq 2$, if we have

$$\lim_{N\to\infty} \frac{\#\{n : 0 \leq n < N, k_n \equiv j \pmod r\}}{N} = \frac{1}{r}$$

for all integers $j \in \{0, \ldots, r-1\}$.

Definition 1 (Digital sequence)**.** Let $s \in \mathbb{N}$ and choose s $\mathbb{N}_0 \times \mathbb{N}_0$ matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$, q prime. For the sake of simplicity we assume that the matrices have finite columns, i.e., that each column contains only finitely many nonzero entries. To generate the ith coordinate $x_n^{(i)}$ of $\boldsymbol{x}_n$, represent the integer

n in base q

$$n = n_0 + n_1 q + \cdots + n_r q^r,$$

set

$$\boldsymbol{n} := (n_0, \ldots, n_r, 0, 0, \ldots)^T$$

and

$$C^{(i)} \cdot \boldsymbol{n} =: \left(y_0^{(i)}, y_1^{(i)}, \ldots\right)^T \pmod q.$$

Further

$$x_n^{(i)} := \frac{y_0^{(i)}}{q} + \frac{y_1^{(i)}}{q^2} + \ldots$$

We call $(\boldsymbol{x}_n)_{n\geq 0}$ a *digital sequence over $\mathbb{F}_q$ generated by $C^{(1)}, \ldots, C^{(s)}$*. (Note that for the sake of simplicity we do not distinguish the residue classes of $\mathbb{F}_q$ from their representatives $\{0, 1, \ldots, q-1\}$.)

Definition 2 (Hybrid version)**.** Let $v \in \mathbb{N}, s_1, \ldots, s_v \in \mathbb{N}$, $q_1, \ldots, q_v$ be distinct primes and for each $j \in \{1, \ldots, v\}$ let $C^{(j,1)}, \ldots, C^{(j,s_j)}$ be $\mathbb{N}_0 \times \mathbb{N}_0$ matrices over $\mathbb{F}_{q_j}$. Then we define an $(s_1 + \cdots + s_v)$-dimensional sequence $(\boldsymbol{y}_n)_{n\geq 0}$ in $[0,1)^{s_1+\cdots+s_v}$ by

$$\boldsymbol{y}_n := (\boldsymbol{x}_n^{(1)}, \ldots, \boldsymbol{x}_n^{(v)}),$$

where for each $j \in \{1, \ldots, v\}$, $\boldsymbol{x}_n^{(j)}$ denotes the nth point of the digital sequence generated by $C^{(j,1)}, \ldots, C^{(j,s_j)}$. (Again we restrict to matrices having finite columns exclusively for the sake of simplicity.)

It is well known that a digital sequence generated by $C^{(1)}, \ldots, C^{(s)}$ is uniformly distributed if and only if the rows of the generating matrices $C^{(1)}, \ldots, C^{(s)}$ altogether are linearly independent over $\mathbb{F}_q$, i.e., that any finite set of rows of $C^{(1)}, \ldots, C^{(s)}$ is linearly independent over $\mathbb{F}_q$ (cf. e.g. [1, Section 4.4.7]). As pointed out for example in [9], for the investigation of the finer distribution properties of digital sequences and their hybrid version it makes a great difference if the generating matrices consist of finite rows exclusively or not. A row of a matrix can be denoted by $(c_r)_{r\geq 0}$ where c_r are the entries of the row, and it is said to be finite if there are only finitely many $r \in \mathbb{N}_0$ such that $c_r \neq 0$. In the following we will use the notion *finite-row matrix* to indicate that it consists of finite rows exclusively. The uniform distribution of the hybrid version was investigated for the special case of finite rows in [8] and later for the general case in [7]. Altogether it could be shown that the obvious necessary condition for uniform distribution namely that the component sequences are uniformly distributed is already a sufficient one.

In this paper we mainly restrict our investigation of the uniform distribution of subsequences of digital sequences and of their hybrid version to the special

case of finite-row generating matrices. The aims of the paper are to introduce a new criterion on the index sequence that yields uniform distribution of the subsequence of digital sequences and also one to decide the uniform distribution of the hybrid version. Furthermore, we compare the new criterions with existing ones on the index sequences by regarding some examples. Finally, we investigate the finer structure of a power index sequence. More exactly, we explore a detailed study of power residues in different congruence classes. This together with the new criterion allows to give a full classification of all finite-row generating matrices that yield uniformly distributed subsequences that are indexed by a sequence $(n^p)_{n\geq 0}$ of fixed prime exponent.

2. The New Criterions

To state our criterions we will use the notion of admissibility of a weight sequence for an index sequence defined as follows.

Definition 3. Let q be prime. We call $\gamma = (\gamma_0, \gamma_1, \dots) \in \mathbb{F}_q^{\mathbb{N}_0}$ *admissible for* $(k_n)_{n\geq 0}$ if

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{0 \leq n < N : s_{q,\gamma}(k_n) \equiv d \,(\mathrm{mod}\ q)\right\} = \frac{1}{q}$$

for all $d \in \{0, 1, \dots, q-1\}$.
Here and in the following, by $s_{q,\gamma}(m)$ we denote the q-ary weighted sum of digits of m with weight sequence γ, i.e.,

$$s_{q,\gamma}(m) := \gamma_0 m_0 + \gamma_1 m_1 + \cdots + \gamma_r m_r,$$

where $m = m_0 + m_1 q + \cdots + m_r q^r$ is the base q representation of m.

Proposition 1. *Let q be prime, $s \in \mathbb{N}$ and $C^{(1)}, \dots, C^{(s)}$ be s $\mathbb{N}_0 \times \mathbb{N}_0$ matrices over $\mathbb{F}_q$, and $(\boldsymbol{x}_n)_{n\geq 0}$ be the digital sequence over $\mathbb{F}_q$ generated by the matrices $C^{(1)}, \dots, C^{(s)}$. Then the sequence $(\boldsymbol{x}_{k_n})_{n\geq 0}$ is uniformly distributed if and only if every nontrivial linear combination of any finite set of rows of $C^{(1)}, \dots, C^{(s)}$ over $\mathbb{F}_q$ is admissible for $(k_n)_{n\geq 0}$.*

Proposition 2. *Let $v \in \mathbb{N}, s_1, \dots, s_v \in \mathbb{N}$, $q_1, \dots, q_v$ be distinct primes and for each $j \in \{1, \dots, v\}$ let $C^{(j,1)}, \dots, C^{(j,s_j)}$ be s_j finite-row $\mathbb{N}_0 \times \mathbb{N}_0$ matrices over $\mathbb{F}_{q_j}$. If the index sequence $(k_n)_{n\geq 0}$ satisfies for every $j \in \{1, \dots, v\}$ that it is periodic modulo q_j^l with period q_j^l for every $l \geq l_j$ for some $l_j \in \mathbb{N}$, then the hybrid subsequence $((\boldsymbol{x}_{k_n}^{(1)}, \dots, \boldsymbol{x}_{k_n}^{(v)}))_{n\geq 0}$ is uniformly distributed if and only if all component subsequences $(\boldsymbol{x}_{k_n}^{(j)})_{n\geq 0}$ are uniformly distributed.*

For the sake of readability the proofs of the propositions above are given in Section 3.

The distribution of subsequences of digital sequences and their hybrid version in the special case of finite-row generating matrices was already studied in [8]. Therein a sufficient but in general not necessary condition on the index sequence was given, namely: if the index sequence $(k_n)_{n\geq 0}$ is uniformly distributed modulo $(q_1 \cdots q_v)^d$ for every $d \in \mathbb{N}$, then the subsequence of every uniformly distributed hybrid version in the sense of Definition 2 generated by finite-row matrices is uniformly distributed. In [8] there can be found several examples of index sequences satisfying the sufficient condition (cf. [8, Examples 4.6, 4.8]). Let us briefly consider this sufficient condition for one component digital sequence, i.e.: if the index sequence $(k_n)_{n\geq 0}$ is uniformly distributed modulo q^d for every $d \in \mathbb{N}$, then the subsequence of every uniformly distributed digital sequence generated by finite-row matrices is uniformly distributed. Basic linear algebra yields that every nonzero finite row over $\mathbb{F}_q$ is admissible for an index sequence $(k_n)_{n\geq 0}$ which is uniformly distributed modulo q^d for every $d \in \mathbb{N}$. Hence our new criterion applies easily to such index sequences. Additionally, it is applicable for index sequences that are not uniformly distributed modulo q^d for every $d \in \mathbb{N}$.

In the following we list some (previously studied) examples of index sequences for which our new criterions may be applied.

Example 1 (Arithmetic progressions)**.** Let $(k_n)_{n\geq 0}$ be an index sequence of the form $(an + b)_{n\geq 0}$ with integers $a \geq 1$, $b \geq 0$. If a satisfies $\gcd(a, q_1 \cdots q_v) = 1$ then it is easily seen that $(an+b)_{n\geq 0}$ is uniformly distributed modulo $(q_1 \cdots q_v)^d$ for every $d \in \mathbb{N}$ and the subsequence (of the hybrid version) of a digital sequence that is generated by finite-row matrices is uniformly distributed if and only if the whole sequence is uniformly distributed (cf. [8, Example 4.6 (b)]).
In the general case where $\gcd(a, q_1 \cdots q_v) > 1$ one has to determine the admissible rows for the index sequence: Let $q \in \mathbb{P}$, $\mu := \max\{m \geq 0 : q^m | a\}$. A row $\gamma = (\gamma_0, \gamma_1, \dots) \in \mathbb{F}_q^{\mathbb{N}_0}$ is admissible for $(an + b)_{n\geq 0}$ if and only if it is linearly independent with the first μ rows of the unit matrix in $\mathbb{F}_q^{\mathbb{N}_0 \times \mathbb{N}_0}$. A periodic property of the index sequence as needed for applying Proposition 2 is obviously satisfied. Hence Proposition 1 and 2 yield a complete classification of all uniformly distributed arithmetic subsequences of digital sequences and their hybrid version with finite-row generating matrices. Note that the case of arbitrary generating matrices was investigated earlier in [6] by a sophisticated study of certain exponential sums. The study therein covers index sequences that can be interpreted as solutions of certain systems of congruences.

Example 2 (Primes)**.** Let k_n be the $(n+1)$th prime p_{n+1} and q be a prime. From Dirichlet's Prime Number Theorem (DPNT) for arithmetic progressions one knows that the sequence of primes $(p_{n+1})_{n\geq 0}$ is uniformly distributed modulo q^d amongst all residue classes that are not divisible by q. DPNT together with basic linear algebra yields that a nonzero finite weight sequence $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ with $\gamma_{l-1} \neq 0$ is admissible for the sequence of primes $(p_{n+1})_{n\geq 0}$ if and only if $l \geq 2$. This together with Proposition 1 yields a classification of all possible finite-row generating matrices such that the digital sequence indexed by the primes is uniformly distributed. As it is known, the sequence $(p_{n+1})_{n\geq 0}$ does not satisfy periodic properties and for the distribution of the hybrid version one has to study the common admissibility of finite rows over different fields of residue classes. This was done in [6, Theorem 7]).

Example 3 (Squares)**.** In the recent paper [10] subsequences, that are indexed by squares, of digital sequences generated by finite-row matrices were investigated and all uniformly distributed ones were classified. In [10] it is shown that a nonzero finite weight sequence $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ with $\gamma_{l-1} \neq 0$ is admissible for $(n^2)_{n\geq 0}$ if and only if $q = 2$, l even and $\gamma_{l-2} = \gamma_{l-1} = 1$ or if $q = 2$, $\gamma_0 = 1$ and $\gamma_i = 0$ for $i \geq 1$. This together with Proposition 1 yields [10, Theorem 1], i.e.: The subsequence $(\boldsymbol{x}_{n^2})_{n\geq 0}$ of a digital sequence generated by finite-row matrices over $\mathbb{F}_q$ is uniformly distributed if and only if $(\boldsymbol{x}_n)_{n\geq 0}$ is uniformly distributed, $q = 2$, and the sum of any finite set of rows of $C^{(1)}, \dots, C^{(s)}$ is either of the form

$$(\gamma_0, \gamma_1, \quad \gamma_2, \gamma_3, \quad \dots, \quad \gamma_{l-2}, \gamma_{l-1}, \quad 0, 0, 0, 0 \dots)$$

with $\gamma_{l-2} = \gamma_{l-1} = 1$ and l even, or of the form $(1, 0, 0, 0, \dots)$.

Note that due to Definition 3 admissibility of a weight sequence for an index sequence is related to the distribution properties of the weighted sum of digits. Hence Examples 2 and 3 are related to the weighted versions of Gelfond's problems for primes and squares.

In this paper we extend the investigation of the uniform distribution of subsequences of digital sequences and their hybrid version in [10] to subsequences that are indexed by $(n^p)_{n\geq 0}$ with fixed prime exponent. According to the criterion in Proposition 1 we study the admissibility of finite rows for such index sequences, and thereby we achieve first results for the weighted version of Gelfond's problem in the case of polynomial index sequences. To decide the admissibility we need a detailed investigation of the distribution of powers with prime exponent in the residue classes modulo prime powers. For the sake of readability this study is carried out in Section 4. Altogether we arrive at the following astonishingly concise result.

Theorem 1. *Let $p \geq 3$ and q be primes. A nonzero finite weight sequence $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ over $\mathbb{F}_q$ with $l \in \mathbb{N}$ and $\gamma_{l-1} \neq 0$ is admissible for $(n^p)_{n\geq 0}$ if and only if $p \not| (q-1)$ and $l \equiv 1 \pmod{p}$.*

Remark 1. As already mentioned in Example 3, in [10] it was shown that nonzero finite weight sequences are only admissible for $(n^2)_{n\geq 0}$ in base $q = 2$ under certain conditions on l and the last two nonzero entries in the finite weight sequence. It is interesting to note that for an index sequence $(n^p)_{n\geq 0}$ where p is an odd prime the admissibility of a finite weight sequences only depends on the length l but not on the entries of γ, and we can determine admissible weight sequences also in prime bases different from 2. Therefore it makes sense to investigate the uniform distribution of the hybrid version as well.

Using Theorem 1, Propositions 1 and 2, and the fact that for every $l \in \mathbb{N}$ $(n + kq^l)^p \equiv n^p \pmod{q^l}$ for all $n, k \in \mathbb{N}_0$, we are able to classify all uniformly distributed subsequences indexed by $(n^p)_{n\geq 0}$ with $p \geq 3$ prime of digital sequences and of the hybrid version that are generated by finite-row matrices.

Corollary 1. *Let $p \geq 3$ and q be primes, $C^{(1)}, \dots, C^{(s)}$ be finite-row matrices over $\mathbb{F}_q$. The subsequence $(\boldsymbol{x}_{n^p})_{n\geq 0}$ of the digital sequence generated by $C^{(1)}, \dots, C^{(s)}$ is uniformly distributed if and only if $p \not| (q-1)$, and every sequence γ that is built by a nontrivial linear combination of any finite set of rows of $C^{(1)}, \dots, C^{(s)}$ is nonzero and of the specific form $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ where $\gamma_{l-1} \neq 0$ with $l \in \mathbb{N}$ satisfying $l \equiv 1 \pmod{p}$.*

Furthermore, the subsequence $(\boldsymbol{y}_{n^p})_{n\geq 0}$ of a hybrid version of v digital sequences generated by finite-row matrices due to Definition 2 is uniformly distributed if and only if for every $j \in \{1, \dots, v\}$ the sequence $(\boldsymbol{x}_{n^p}^{(j)})_{n\geq 0}$ is uniformly distributed.

Example 4. A matrix of the form

$$\begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,\dots \\ 0\,0\,0\,1\,0\,0\,0\,0\,\dots \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,\dots \\ \qquad\qquad \ddots \end{pmatrix} \text{ over } \mathbb{F}_q$$

generates a uniformly distributed one-dimensional subsequence that is indexed by $(n^3)_{n\geq 0}$ whenever $3 \not| (q-1)$. From Dirichlet's Prime Number Theorem on arithmetic progressions we know that approximately half of the primes satisfy this condition. Hence by juxtaposing such uniformly distributed component subsequences based on such pairwise different primes we can build a uniformly distributed hybrid version in any dimension.

3. Proofs of Proposition 1 and 2

Proposition 1 is a generalization of [10, Proposition 1]. Its proof mainly focuses on the matrix-vector product in the construction principle of the digital sequence in order to relate the distribution of the digital sequence with the properties of nontrivial linear combinations of matrix rows. Note that the following proof does not use the finite row property and therefore Proposition 1 is valid for arbitrary generating matrices.

P r o o f o f P r o p o s i t i o n 1. Assume first, that every nontrivial linear combination of any finite set of rows of $C^{(1)}, \dots, C^{(s)}$ is admissible for $(k_n)_{n\geq 0}$. We write $C^{(i)} = \left(c_{j,r}^{(i)}\right)_{j,r=0,1,\dots}$ and by $c_j^{(i)}$ we denote the jth row of $C^{(i)}$ which is given by the sequence $(c_{j,r}^{(i)})_{r\geq 0}$. To prove the uniform distribution of $(\boldsymbol{x}_{k_n})_{n\geq 0}$ it suffices to show that $(\boldsymbol{x}_{k_n})_{n\geq 0}$ is uniformly distributed in intervals of the form

$$I := \prod_{i=1}^{s} \left[\frac{b_i}{q^{d_i}}, \frac{b_i+1}{q^{d_i}}\right)$$

with $d_i \geq 0$ and $0 \leq b_i < q^{d_i}$.

In the following we make use of the base q representation of b_i, which we denote by

$$b_i = b_0^{(i)} q^{d_i-1} + b_1^{(i)} q^{d_i-2} + \cdots + b_{d_i-2}^{(i)} q + b_{d_i-1}^{(i)}.$$

Note that the row-vector products carried out in the construction of the nth point of the subsequence can alternatively be denoted by $s_{q,c_j^{(i)}}(k_n) \pmod q$. Using the following basic exponential sum for integers a, b

$$\frac{1}{q}\sum_{u=0}^{q-1} e\left(\frac{u(a-b)}{q}\right) = \begin{cases} 1 & \text{if } a \equiv b \pmod q \\ 0 & \text{else,} \end{cases}$$

with $e(x) := e^{2\pi i x}$ we can compute for the first N points of the subsequence the relative number of points that are contained in I as follows.

$$\begin{aligned} &\frac{1}{N}\#\left\{0 \leq n < N : \boldsymbol{x}_{k_n} \in I\right\} \\ &\quad = \quad \frac{1}{N}\sum_{n=0}^{N-1}\prod_{i=1}^{s}\prod_{l=0}^{d_i-1}\frac{1}{q}\sum_{u_l^{(i)}=0}^{q-1} e\left(\frac{u_l^{(i)}\left(s_{q,c_l^{(i)}}(k_n) - b_l^{(i)}\right)}{q}\right). \end{aligned}$$

Expanding the products, using basic properties of the exponential function, exchanging the order of the sums, separating the summand given by all $u_l^{(i)} = 0$,

and selecting terms depending on n and not depending on n yields

$$\begin{aligned}\frac{1}{N}\#\left\{0\le n<N:\boldsymbol{x}_{k_n}\in I\right\}\\ =\quad \frac{1}{q^{d_1+\cdots+d_s}}+\frac{1}{q^{d_1+\cdots+d_s}}\sum_{*}e\left(-\frac{1}{q}\sum_{i=1}^{s}\sum_{l=0}^{d_i-1}u_l^{(i)}b_l^{(i)}\right)\times\\ \times\quad \frac{1}{N}\sum_{n=0}^{N-1}e\left(\frac{1}{q}\cdot s_{q,\gamma((u_l^{(i)}))}(k_n)\right).\end{aligned}$$

Here

$$\sum_{*}\quad\text{denotes}\quad\sum_{u_0^{(1)}=0}^{q-1}\cdots\sum_{u_{d_1-1}^{(1)}=0}^{q-1}\cdots\sum_{u_0^{(s)}=0}^{q-1}\cdots\sum_{u_{d_s-1}^{(s)}=0}^{q-1}$$

but omitting the term where all $u_l^{(i)}$ are zero. Furthermore, in the last sum we used the linearity of the q-ary weighted sum of digits with respect to the weight sequence, and the notation

$$\gamma\left((u_l^{(i)})\right):=\sum_{i=1}^{s}\sum_{l=0}^{d_i-1}u_l^{(i)}c_l^{(i)}.$$

Note that because of the setting "not all $u_l^{(i)}=0$" the sequence $\gamma\left((u_l^{(i)})\right)$ is a nontrivial linear combination of finitely many rows of $C^{(1)},\ldots,C^{(s)}$, which is admissible for $(k_n)_{n\ge0}$. Using the famous Weyl-criterion for uniform distribution modulo q we obtain

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}e\left(\frac{1}{q}\cdot s_{q,\gamma((u_l^{(i)}))}(k_n)\right)=0.$$

Altogether we arrive at the desired result

$$\lim_{N\to\infty}\frac{1}{N}\#\left\{0\le n<N:\boldsymbol{x}_{k_n}\in I\right\}=\frac{1}{q^{d_1+\cdots+d_s}}=\lambda(I),$$

and the uniform distribution of $(\boldsymbol{x}_{k_n})_{n\ge0}$ follows.

To show the "only if" part of the proposition we assume that $(\boldsymbol{x}_{k_n})_{n\ge0}$ is uniformly distributed. This assumption implies that

$$\lim_{N\to\infty}\frac{1}{N}\#\left\{0\le n<N:\boldsymbol{x}_{k_n}\in I\right\}\quad=\quad\frac{1}{q^{d_1+\cdots+d_s}}$$

for every interval I of the form

$$I := \prod_{i=1}^{s} \left[\frac{b_i}{q^{d_i}}, \frac{b_i+1}{q^{d_i}} \right)$$

with $d_i \geq 0$ and $0 \leq b_i < q^{d_i}$. Note that for fixed $d_1, \ldots, d_s \in \mathbb{N}_0$ there are $q^{d_1+\cdots+d_s}$ possible settings for $(b_1, \ldots, b_s)$. We use the same notation as in the first part of the proof for the base q representation of b_i, the matrix rows, and the row-vector products, and we see; the condition $\boldsymbol{x}_{k_n} \in I$ is equivalent to the fact that k_n satisfies

$$s_{q,c_l^{(i)}}(k_n) \equiv b_l^i \pmod{q} \text{ for every } \quad 1 \leq i \leq s \text{ and } 0 \leq l \leq d_i - 1. \tag{1}$$

The uniform distribution ensures that

$$\lim_{N\to\infty} \frac{1}{N} \#\{0 \leq n < N : k_n \text{ satisfies (1)}\} \quad = \quad \frac{1}{q^{d_1+\cdots+d_s}} \tag{2}$$

for all possible $\prod_{i=1}^{s} q^{d_i}$ settings of $(b_1, \ldots, b_s)$. Computing a nontrivial linear combination of the congruences in (1) yields

$$s_{q,\gamma((u_l^{(i)}))}(k_n) \equiv b \pmod{q}.$$

where

$$b := b\left((u_l^{(i)})\right) = \left(\sum_{i=1}^{s} \sum_{l=0}^{d_i-1} u_l^{(i)} b_l^{(i)} \right) \pmod{q}$$

and

$$\gamma\left((u_l^{(i)})\right) := \sum_{i=1}^{s} \sum_{l=0}^{d_i-1} u_l^{(i)} c_l^{(i)}.$$

Note that "nontrivial" implies that not all $u_l^{(i)} = 0$ and therefore for every such setting of $u_l^{(i)}$ exactly $q^{d_1+\cdots+d_s-1}$ settings of $(b_1, \ldots, b_s)$ map to a fixed value $b \in \{0, 1, \ldots, q-1\}$. This together with (2) yields

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{0 \leq n < N : s_{q,,\gamma((u_l^{(i)}))}(k_n) \equiv b \,(\mathrm{mod}\ q)\right\} = \frac{q^{d_1+\cdots+d_s-1}}{q^{d_1+\cdots+d_s}} = \frac{1}{q}$$

for every $b \in \{0, 1, \ldots, q-1\}$ and therefore admissibility of the nontrivial linear combination of the rows for the sequence $(k_n)_{n\geq 0}$. □

The following proof of Proposition 2 exploits the special finite-row property of the generating matrices and the periodic structure of the index sequence. The main tool will be the Chinese Remainder Theorem.

P r o o f o f P r o p o s i t i o n 2. A uniformly distributed hybrid subsequence obviously needs uniformly distributed component subsequences.
Let us assume the uniform distribution of the component subsequences $(\boldsymbol{x}_{k_n}^{(j)})_{n\geq 0}$. In order to prove the uniform distribution of the hybrid subsequence $(\boldsymbol{y}_{k_n})_{n\geq 0}$ we regard an interval of the form

$$I = \prod_{j=1}^{v} I_j \text{ with } I_j = \prod_{i=1}^{s_j} \left[\frac{b^{(j,i)}}{q_j^{d^{(j,i)}}}, \frac{b^{(j,i)}+1}{q_j^{d^{(j,i)}}} \right)$$

with $d^{(j,i)}, b^{(j,i)} \in \mathbb{N}_0$ and $0 \leq b^{(j,i)} < q_j^{d^{(j,i)}}$ and deduce

$$\lim_{N\to\infty} \frac{1}{N} \# \left\{ 0 \leq n < N : \boldsymbol{y}_{k_n} \in I \right\} = \prod_{j=1}^{v} \frac{1}{q_j^{d^{(j,1)}+\cdots+d^{(j,s_j)}}}. \tag{3}$$

We define the length l of a finite sequence $(\gamma_r)_{r\geq 0}$ by $l =: \max\{r \in \mathbb{N} : \gamma_{r-1} \neq 0\}$. We introduce the quantity $L_j = L_j(d^{(j,1)}, \ldots, d^{(j,s_j)})$ that measures the lengths of the row in $C^{(j,1)}, \ldots, C^{(j,s_j)}$ as follows. We choose L_j minimal such that
the first $d^{(j,1)}$ rows of $C^{(j,1)}$ have lengths $\leq L_j$,
the first $d^{(j,2)}$ rows of $C^{(j,2)}$ have lengths $\leq L_j$,
...,
the first $d^{(j,s_j)}$ rows of $C^{(j,s_j)}$ have lengths $\leq L_j$.

Note that this minimum exists because of the finite-row property of the generating matrices. The construction principle together with the definition of L_j yield that the first L_j digits of k_n in base q_j, or equivalently the residue of k_n modulo $q_j^{L_j}$, determine whether $\boldsymbol{x}_{k_n}^{(j)}$ is included in the interval I_j or not.

Now we use of the assumption in the Proposition 2, namely that $(k_n)_{n\geq 0}$ satisfies for every $j \in \{1, \ldots, v\}$ that it is periodic modulo q_j^l with period q_j^l for every $l \geq l_j$ for some $l_j \in \mathbb{N}$.

We set $\mu_j := \max\{l_j, L_j\}$. Note that from the assumption in the proposition we have $k_{m+uq_j^l} \equiv k_m \pmod{q_j^l}$ for $m, u \in \mathbb{N}_0$ and $l \geq l_j$. Obviously, the residue of k_n modulo $q_j^{\mu_j}$ determines the first L_j digits in base q_j and therefore whether $\boldsymbol{x}_{k_n}^{(j)}$ is included in the Interval I_j or not.

The uniform distribution of the component sequence and the periodic property of the index sequence ensures that if we take the first $q_j^{\mu_j}$ points of the subsequence $(\boldsymbol{x}_{k_n}^{(j)})_{n\geq 0}$ we have exactly $q_j^{\mu_j-(d^{(j,1)}+\cdots+d^{(j,s_j)})} =: W_j$ points in the interval I_j. We summarize that W_j values for n in the set $\{0, \ldots, q_j^{\mu_j}-1\}$ satisfy $\boldsymbol{x}_{k_n}^{(j)} \in I_j$. We denote these values by $r_1^{(j)}, \ldots, r_{W_j}^{(j)}$.

Again using the periodic property of $(k_n)_{n\geq 0}$ we have $\boldsymbol{x}_{k_n}^{(j)} \in I_j$ if and only if $k_n \equiv k_{r_{w_j}^{(j)}} \pmod{q_j^{\mu_j}}$ for a $w_j \in \{1,\dots,W_j\}$ or equivalently $n \equiv r_{w_j}^{(j)} \pmod{q_j^{\mu_j}}$ for a $w_j \in \{1,\dots,W_j\}$.
Obviously, for the subsequence $(\boldsymbol{y}_{k_n})_{n\geq 0}$ of the hybrid version we have $\boldsymbol{y}_{k_n} \in I$ if and only if for every $j \in \{1,\dots,v\}$ $n \equiv r_{w_j}^{(j)} \pmod{q_j^{\mu_j}}$ for a $w_j \in \{1,\dots,W_j\}$.

Finally, we have $\mathcal{W} = \prod_{j=1}^{v} W_j$ different systems of congruences that are by the Chinese Remainder Theorem uniquely solvable modulo $\mathcal{M} = \prod_{j=1}^{v} q_j^{\mu_j}$. Hence regarding the hybrid version $(\boldsymbol{y}_{k_n})_{n\geq 0}$ there are exactly $\mathcal{W}$ residues modulo $\mathcal{M}$, which we denote by $r_1,\dots,r_{\mathcal{W}}$, such that: $\boldsymbol{y}_{k_n} \in I$ if and only if $n \equiv r_w \pmod{\mathcal{M}}$ for a $w \in \{1,\dots,\mathcal{W}\}$. This implies our desired result (3) since

$$\frac{\mathcal{W}}{\mathcal{M}} = \prod_{j=1}^{v} \frac{1}{q_j^{d^{(j,1)}+\dots+d^{(j,s_j)}}}.$$

□

4. Results on primepower residues

In this section we focus on the following quantity

$$T_{\gamma,d,q,p} := \lim_{N\to\infty} T_{\gamma,d,q,p}(N), \text{ where}$$
$$T_{\gamma,d,q,p}(N) := \frac{1}{N} \cdot \#\left\{0 \leq n < N : s_{q,\gamma}(n^p) \equiv d \pmod{q}\right\}$$

for primes q,p for finite weight sequences $\gamma = (\gamma_0,\gamma_1,\dots,\gamma_{l-1},0,0,\dots)$ with $d,\gamma_i \in \{0,1,\dots,q-1\}$ and $\gamma_{l-1} \neq 0$. (Here and in the following $l \in \mathbb{N}$ is the minimal index such that $\gamma_i = 0$ for all $i \geq l$.)

The following theorem lists the values of $T_{\gamma,d,q,p}$ for all settings of γ,d,q,p, which are needed to prove our result in Theorem 1 about the admissibility of rows for subsequences indexed by primepower sequences $(n^p)_{n\geq 0}$. Note that the case $p = 2$, which can be found in [10, Theorem 2], is not covered in the following.

Theorem 2. *Let $p,q \in \mathbb{P}, p \geq 3$, $l \in \mathbb{N}$.*
Case 1: *If $p = q$, then for $d = 0$ we have*

$$T_{\gamma,0,q,p} = \frac{1}{q} + \begin{cases} 0 & \text{if } l \equiv 1 \pmod{p} \\ \frac{f(l,0)}{q^{1+\lfloor (l-1)/p \rfloor}} & \text{if } l \equiv 2 \pmod{p} \\ \frac{q-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{else,} \end{cases}$$

and for $d \in \{1, \dots, q-1\}$ *we have*

$$T_{\gamma,d,q,p} = \frac{1}{q} + \begin{cases} 0 & \text{if } l \equiv 1 \pmod p \\ \frac{f(l,d)-1}{q^{1+\lfloor (l-1)/p \rfloor}} & \text{if } l \equiv 2 \pmod p \\ \frac{-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{else,} \end{cases}$$

where $f(l,d) := \#\{i \in \{1, \dots, q-1\} : c_0(i^p)\gamma_{l-2} + c_1(i^p)\gamma_{l-1} \equiv d \pmod q\}$ *with* $c_0(i^p), c_1(i^p) \in \{0, 1, \dots q-1\}$ *satisfying* $c_0(i^p) + c_1(i^p)q \equiv i^p \pmod{q^2}$ *(i.e. they are the first two digits of* i^p *in base* q*).*

Case 2: *If* $p \neq q$ *and* $p \not| (q-1)$ *and therefore* $\gcd(p, \varphi(q^l)) = 1$*, then for* $d = 0$ *we have*

$$T_{\gamma,0,q,p} = \frac{1}{q} + \begin{cases} 0 & \text{if } l \equiv 1 \pmod p \\ \frac{q-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{if } l \not\equiv 1 \pmod p, \end{cases}$$

and for $d \in \{1, \dots, q-1\}$ *we have*

$$T_{\gamma,d,q,p} = \frac{1}{q} + \begin{cases} 0 & \text{if } l \equiv 1 \pmod p \\ \frac{-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{if } l \not\equiv 1 \pmod p. \end{cases}$$

Case 3: *If* $p | (q-1)$*, then for* $d = 0$ *we have*

$$T_{\gamma,0,q,p} = \frac{1}{q} + \begin{cases} 0 & \text{if } l \equiv 1 \pmod p \\ \frac{q-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{if } l \not\equiv 1 \pmod p, \end{cases}$$

and for $d \in \{1, \dots, q-1\}$ *we have*

$$T_{\gamma,d,q,p} = \frac{1}{q} + \begin{cases} \frac{-1}{q^{2+\lfloor (l-1)/p \rfloor}} & \text{if } l \not\equiv 1 \pmod p \\ \frac{p-1}{q^{1+\lfloor (l-1)/p \rfloor}} & \text{if } l \equiv 1 \pmod p \text{ and} \\ & \gamma_{l-1} c \equiv d \pmod q \text{ for one } c \in C \\ \frac{-1}{q^{1+\lfloor (l-1)/p \rfloor}} & \text{if } l \equiv 1 \pmod p \text{ and} \\ & \gamma_{l-1} c \not\equiv d \pmod q \text{ for all } c \in C, \end{cases}$$

where $C = \{1 \leq c \leq q-1 : c^{(q-1)/p} \equiv 1 \pmod q\}$.

We will present the proof of Theorem 2 after some auxiliary results. The proof will be mainly based on the following proposition that gives a detailed classification of all odd primepower p residues modulo prime powers q^l and the number of solutions for the different settings of p, q, l.

Proposition 3. *Let $p, q \in \mathbb{P}, p \geq 3$ and $l \in \mathbb{N}$. Let L be the number of incongruent solutions of $x^p \equiv a \pmod{q^l}$ with $x \in \{0, 1, \ldots, q^l - 1\}$ for a given power residue a. Then we have*

$$L = q^{l-\lfloor (l-1)/p \rfloor - 1} \qquad \text{for } a = 0.$$

Case 1: *If $q = p$ we have*

$$L = q^{(p-1)u+1} \qquad \text{for } a = q^{pu} \cdot b$$

with $b \equiv c(i^p) \pmod{q^2}$ for a $0 < c(i^p) < q^2$ satisfying $c(i^p) \equiv i^p \pmod{q^2}$ with $i \in \{1, \ldots, q-1\}$ and $u \in \{0, \ldots, \lfloor (l-2)/p \rfloor\}$.
If $l \equiv 1 \pmod{p}$ we additionally have

$$L = q^{(p-1)\cdot(l-1)/p} \qquad \text{for } a = q^{l-1} \cdot b$$

with $b \in \{1, \ldots, q-1\}$.

Case 2: *If $p \neq q$ and $p \not| (q-1)$ and therefore $\gcd(p, \varphi(q^l)) = 1$ we have*

$$L = q^{(p-1)u} \qquad \text{for } a = q^{pu} \cdot b$$

with $b \in \mathbb{N}$ such that $\gcd(b, q) = 1$ and $u \in \{0, \ldots, \lfloor (l-1)/p \rfloor\}$.

Case 3: *If $q \in \mathbb{P}$ with $p | q-1$ we have*

$$L = p \cdot q^{(p-1)u} \qquad \text{for } a = q^{pu} \cdot b$$

with $b \equiv c \pmod{q}$ for a $0 < c < q$ satisfying $c^{(q-1)/p} \equiv 1 \pmod{q}$ and $u \in \{0, \ldots, \lfloor (l-1)/p \rfloor\}$.

Other pth power residues a than those given above do not exist for $q \in \mathbb{P}$.

Proof. Note that in all three cases it suffices to prove that there are at least as many incongruent solutions as listed, since the total number of all solutions for the different values of a equals q^l. The value of L if $a = 0$ can be found in [5, Proposition 1, p.65]. Thus it remains to verify for the listed power residues $a \neq 0$ the corresponding values of L.

At first we will list some basic assertions we need for the proof:

(1) Let $q, p \in \mathbb{P}$ and $l, b \in \mathbb{N}$. The number of incongruent solutions of the congruence $x^p \equiv q^{pu} b \pmod{q^l}$ with $p \not| b$ and $q^{pu} b < q^l$ is given by

$$q^{(p-1)u} B,$$

where B is the number of incongruent solutions of $y^p \equiv b \pmod{q^{l-pu}}$ (compare, e.g., [5, Proposition 2, p.65]).

(2) If $m \in \mathbb{Z}^+$ possesses primitive roots and $\gcd(a,m) = 1$, then a is an nth power residue mod m iff $a^{\phi(m)/d} \equiv 1 \pmod{m}$, where $d = \gcd(n, \phi(m))$. If $x^n \equiv a \pmod{m}$ is solvable, there are exactly d solutions (compare, e.g., [11, Proposition 4.2.1] or [5, Satz 2, p.67]).

(3) Let $m \in \mathbb{N}$, $q \in \mathbb{P}$ and $\mu := \max\{k \in \mathbb{N}^0 : q^k | m\}$. Then we have for all $i \in \mathbb{N}$ with $\lfloor \log_q(i) \rfloor \leq \mu$

$$q^{\mu - \lfloor \log_q(i) \rfloor} \left| \binom{m}{i} \right. .$$

(This can be checked by regarding the prime factor q in the prime factorization of $i!$ and of $m(m-1)\cdots(m-i+1)$.)

(4) Let q be an odd prime, and $0 < c < q^2$ with $\gcd(c,q) = 1$. If c is a qth power residue modulo q^2, then c is also the qth power residue modulo q^l with $l > 2$. In particular, we have for such power residues c

$$c^{(q-1)q^{l-2}} \equiv 1 \pmod{q^l}$$

with $l > 2$. (The proof of this assertion uses the Binomial Theorem and Assertions (2) and (3).)

(5) Suppose that a is odd, $l \geq 3$, and consider the congruence $x^n \equiv a(2^l)$. If n is odd, a solution always exists and it is unique (compare, e.g., [11, Proposition 4.2.2] or [5, Satz 3 and Satz 4 (3), p.67-68]).

(6) If q is an odd prime $q \not| a$, and $q \not| n$, then if $x^n \equiv a \pmod{q}$ is solvable, so is $x^n \equiv a \pmod{q^l}$ for $l \geq 1$. All these congruence have the same number of solutions (compare, e.g., [11, Proposition 4.2.3]).

We will give the main ideas of the proof for the most involved case $q = p$, the other cases can be treated analogously. Note that although we prove the case $q = p$ we will use both variables in the following to be consistent with the remaining cases.

Assume first that $l \equiv 1 \pmod{q}$ and consider $a = q^{l-1} \cdot b$ with $b \in \{1, \ldots, q-1\}$. From Euler's Theorem and Assertion (2) we know that for each b the congruence $y^p \equiv b \pmod{q}$ has a unique solution y in $\{1, \ldots, q-1\}$ (and for different b's the solutions are different). This together with Assertion (1) implies that there are $L = q^{(p-1)(l-1)/p}$ different solutions x for given b.

Consider now $a = q^{pu} \cdot b$ with $b \equiv c(i^p) \pmod{q^2}$ with $c(i^p)$ from Proposition 3. Assume at first $u = 0$. For fixed i we abbreviate $c(i^p)$ as c in the following. We have to prove that here exist $L = q$ solutions for $a = c + q^2 k$ with $k \in \mathbb{N}_0$. Because of Assertion (2) it is sufficient to prove that the congruence

$(c+q^2k)^{\phi(m)/d} = (c+q^2k)^{(q-1)q^{l-1}/q} \equiv 1 \pmod{q^l}$ holds. The congruence holds as

$$(c+q^2k)^{(q-1)q^{l-2}} = c^{(q-1)q^{l-2}} + \sum_{i=1}^{(q-1)q^{l-2}} \binom{(q-1)q^{l-2}}{i} c^{(q-1)q^{l-2}-i} k^i q^{2i}$$

and by Assertion (4) $c^{(q-1)q^{l-2}} \equiv 1 \pmod{q^l}$ and by Assertion (3) the sum is congruent zero modulo q^l.
For the case $u \in \{1, \ldots, \lfloor (l-2)/p \rfloor\}$ we apply Assertion (1). From the case $u = 0$ we know that the congruence $y^p \equiv b \pmod{q^{l-pu}}$ with $b = c + q^2k$, $k \in \mathbb{N}_0$ has q different solutions $y_1, \ldots, y_q \in \{0, \ldots, q^{l-pu}-1\}$ for fixed b. Therefore, the number of different solutions for fixed b are $L = q \cdot q^{(p-1)u}$.

With an analogous case distinction between $u = 0$ and $u > 0$ one can verify the values for a and L in Case 2 and Case 3 of Proposition 3. The case $u = 0$ follows for $q = 2$ by Assertion (5) (the cases $l \in \{1, 2\}$ can easily be handled separately), and for $q \neq 2$ with $\gcd(p, \phi(q^l)) = 1$ by Euler's Theorem and Assertion (2) and (6). For $p|q-1$ the result follows by the Assertions (2) and (3). Proofs for $u > 0$ work in all cases analogously to the case $q = p$ by applying Assertion (1). □

Having verified Proposition 3 we are able to prove Theorem 2.

P r o o f o f T h e o r e m 2: Since for $n \equiv m \pmod{q^l}$ we have $n^p \equiv m^p \pmod{q^l}$ and therefore $s_{q,\gamma}(n^p) = s_{q,\gamma}(m^p)$, we obtain

$$\left\lfloor \frac{N}{q^l} \right\rfloor \cdot q^l \cdot T_{\gamma,d,q,p}(q^l) \leq N \cdot T_{\gamma,d,q,p}(N) \leq \left(\left\lfloor \frac{N}{q^l} \right\rfloor + 1 \right) \cdot q^l \cdot T_{\gamma,d,q,p}(q^l),$$

hence $T_{\gamma,d,q,p} = T_{\gamma,d,q,p}(q^l)$.

We restrict to the proof of Case 1, the other cases follow analogously. Assume that $p \in \mathbb{P}, p \geq 3$ and $q = p$. We determine the pth power residues a from Proposition 3 which are elements of the sets

$$A_d := \{0 \leq a < q^l : s_{q,\gamma}(a) \equiv d \pmod{q}\}$$

with $d \in \{0, 1, \ldots, q-1\}$. Trivially $0 \in A_0$ and therefore $0 \notin A_d$ for $d \neq 0$.
Let us now determine the number of $a \in A_d$ of the form

$$a = q^{pu} \cdot b \text{ with } b \equiv c(i^p) \pmod{q^2} \text{ and } u \in \{0, \ldots, \lfloor (l-2)/p \rfloor\}$$

(compare Proposition 3 Case 1).
Consider at first the special case that $l \equiv 2 \pmod{q}$. Then for the maximal value of u (i.e., $u = (l-2)/p$) the base q representation of a is given by

$$a = (0 \ldots 0 a_{l-2} a_{l-1})_q$$

where $a_{l-2} = c_0(i^p)$ and $a_{l-1} = c_1(i^p)$. Here $c_0(i^p)$ and $c_1(i^p)$ denote the digits of $c(i^p)$ in base q for $i \in \{1, \dots, q-1\}$. Note that for this special case we have $a \in A_d$ if and only if $c_0(i^p)\gamma_{l-2} + c_1(i^p)\gamma_{l-1} \equiv d \pmod q$.
For the other values of u the base q representation of $a = q^{pu} \cdot b$ is given by

$$a = (0 \dots 0\, c_0(i^p)c_1(i^p)a_{pu+2} \dots a_{l-2}a_{l-1})_q\,.$$

For $a_{pu+2}, \dots, a_{l-2}$ arbitrary the digit of a_{l-1} is uniquely determined by the condition $a \in A_d$. As there exist $q-1$ different $c(i^p)$'s the number of $a \in A_d$ of this form for given u is $(q-1)q^{l-pu-3}$.

In the case $l \equiv 1 \pmod q$ we additionally have power residues of the form

$$a = q^{l-1} \cdot b \text{ with } b \in \{1, \dots, q-1\},$$

i.e., $a = (0 \dots 0a_{l-1})_q$ with $a_{l-1} = b$. Therefore we have $q-1$ a's of this form and one such $a \in A_d$ for each $d \neq 0$.

Let $e(l) := l - \lfloor (l-1)/p \rfloor - 1$. Altogether we obtain by Proposition 3 for $d = 0$ (note that $\lfloor (l-2)/p \rfloor = (\lfloor (l-1)/p \rfloor - 1)$ for $l \equiv 1 \pmod p$, $(\lfloor (l-2)/p \rfloor - 1) = (\lfloor (l-1)/p \rfloor - 1)$ for $l \equiv 2 \pmod p$ and $\lfloor (l-2)/p \rfloor = \lfloor (l-1)/p \rfloor$ for $l \not\equiv 1 \pmod p \wedge l \not\equiv 2 \pmod p$)

$$q^l \cdot T_{\gamma,0,q,p}(q^l) = q^{e(l)} + \begin{cases} \sum_{u=0}^{\lfloor (l-1)/p \rfloor - 1} q^{(p-1)u+1}(q-1)q^{l-pu-3} \\ \qquad \text{if } l \equiv 1 \pmod p, \\ \sum_{u=0}^{\lfloor (l-1)/p \rfloor - 1} (q-1)q^{l-u-2} + q^{(p-1)(l-2)/p+1} f(l,0) \\ \qquad \text{if } l \equiv 2 \pmod p, \\ \sum_{u=0}^{\lfloor (l-1)/p \rfloor} (q-1)q^{l-u-2} \\ \qquad \text{else.} \end{cases}$$

As $\sum_{u=0}^{\lfloor (l-1)/p \rfloor} (q-1)q^{l-u-1} = q^l - q^{e(l)}$ we obtain

$$q^l \cdot T_{\gamma,0,q,p}(q^l) = \begin{cases} q^{l-1} & \text{if } l \equiv 1 \pmod p, \\ q^{l-1} + q^{e(l)} \cdot f(l,0) & \text{if } l \equiv 2 \pmod p, \\ q^{l-1} + (q-1)q^{e(l)-1} & \text{else.} \end{cases}$$

The given values of $T_{\gamma,0,q,p}$ in Case 1 follow immediately. For $d \neq 0$ we have analogously

$$q^l \cdot T_{\gamma,d,q,p}(q^l) = \begin{cases} \sum_{u=0}^{\lfloor (l-1)/p \rfloor - 1} (q-1)q^{l-u-2} + q^{(p-1)(l-1)/p} \\ \qquad \text{if } l \equiv 1 \pmod{p}, \\ \sum_{u=0}^{\lfloor (l-1)/p \rfloor - 1} (q-1)q^{l-u-2} + q^{e(l)} f(l,d) \\ \qquad \text{if } l \equiv 2 \pmod{p}, \\ \sum_{u=0}^{\lfloor (l-1)/p \rfloor} (q-1)q^{l-u-2} \\ \qquad \text{else,} \end{cases}$$

$$= \begin{cases} q^{l-1} & \text{if } l \equiv 1 \pmod{p}, \\ q^{l-1} + q^{e(l)}\,(f(l,d)-1) & \text{if } l \equiv 2 \pmod{p}, \\ q^{l-1} - q^{e(l)-1} \text{else.} \end{cases}$$

The values of $T_{\gamma,d,q,p}$ in Case 1 follow.

We leave out the proofs for the values of $T_{\gamma,d,q,p}$ in Case 2 and 3 which can be carried out analogously and are even easier due to structure of the power residues a given in Case 2 and Case 3 of Proposition 3. □

We close this section with Lemma 1 from which (together with Theorem 2) we derive Theorem 1.

Lemma 1. *Let $q \geq 3$ be a prime and $p = q$.*

(1) *Let $c_0(i^p), c_1(i^p) \in \{1, \ldots, q-1\}$ be the digits in the base q representation of the $c(i^p)$'s from Proposition 3 (i.e., $c(i^p) = c_0(i^p) + c_1(i^p)q$), then we have*

$$c_0(i^p) + c_0\big((q-i)^p\big) = q \qquad \text{for every } i \in \{1, \ldots q-1\},$$
$$c_1(i^p) + c_1\big((q-i)^p\big) = q-1 \qquad \text{for every } i \in \{1, \ldots q-1\}.$$

(2) *Let $f(l,d) := \#\{i \in \{1, \ldots, q-1\} : c_0(i^p)\gamma_{l-2} + c_1(i^p)\gamma_{l-1} \equiv d \pmod{q}\}$. Then $f(l,d) = 1$ for every $d \in \{1, \ldots, q-1\}$ and $f(l,0) = 0$ if and only if $\gamma_{l-2} \neq 0$ and $\gamma_{l-1} = 0$.*

Proof. It is easy to prove that $c(i^p) + c((q-i)^p) \equiv 0 \pmod{q^2}$ for all $i \in \{1, \ldots, q-1\}$. From that Part (1) follows immediately.
For Part (1) we assume that there exist $\gamma_{l-2}, \gamma_{l-1} \in \{0, 1, \ldots, q-1\}$ such that $f(l,d) = 1$ for every $d \in \{1, \ldots q-1\}$ and $f(l,0) = 0$. Then for $i \in \{1, \ldots, q-1\}$ the following congruences must hold

$$c_0(i^p)\gamma_{l-2} + c_1(i^p)\gamma_{l-1} \equiv d_i \pmod{q}$$

with $d_i \in \{1, \dots, q-1\}$ and $d_i \neq d_j$ for $i \neq j$. Obviously these congruences cannot hold if $\gamma_{l-2} = \gamma_{l-1} = 0$. By summing up these $q-1$ congruences and using the relations between the digits given in Part (1), we end up with the congruence $(q-1)^2/2 \cdot \gamma_{l-1} \equiv 0 \pmod{q}$ and therefore $\gamma_{l-1} = 0$ and $\gamma_{l-2} \neq 0$. Conversely, $\gamma_{l-2} \neq 0$ and $\gamma_{l-1} = 0$ yields the desired result since for $q = p$ we have $\{c_0(i^p) : 1 \leq i \leq q-1\} = \{1, \dots, q-1\}$.

□

P r o o f o f T h e o r e m 1: To decide the admissibility of a finite nonzero weight sequence $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ with $\gamma_{l-1} \neq 0$ for $(n^p)_{n \geq 0}$ we need

$$T_{\gamma,d,q,p} = \frac{1}{q} \text{ for every } d \in \{0, 1, \dots, q-1\}. \tag{4}$$

Using the detailed results for that magnitude in Theorem 2 and the results in Lemma 1 we see if $p|(q-1)$ (4) cannot hold and in the other cases (4) holds if and only if $l \equiv 1 \pmod{p}$. □

REFERENCES

[1] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010.

[2] DRMOTA, M.—MAUDUIT, C.—RIVAT, J.: *The sum-of-digits function of polynomial sequences,* J. Lond. Math. Soc. (2) **84** (2011), no. 1, 81-102.

[3] GELFOND, A.O.: *Sur les nombres qui ont des propriétés additives et multiplicatives données.* Acta Arith. **13** (1968), 259–265.

[4] GOMEZ-PEREZ, D.—HOFER, R.—NIEDERREITER, H.: *A general discrepancy bound for hybrid sequences involving Halton sequences,* Unif. Distr. Theory. **8** (2013), no. 1, 31–45.

[5] HLAWKA, E.—SCHOISSENGEIER, J.: *Zahlentheorie. Eine Einführung*, Second edition, Manz-Verlag, Wien, 1990.

[6] HOFER, R.: *On subsequences of Niederreiter-Halton sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008 (Pierre L' Ecuyer and Art B. Owen, eds.), pp. 423–438, Springer, Berlin, Heidelberg, 2009.

[7] HOFER, R.: On the distribution properties of Niederreiter-Halton sequences, J. Number Theory **129** (2009), 451–463.

[8] HOFER, R.—KRITZER, P.—LARCHER, G.—PILLICHSHAMMER, F.: *Distribution properties of generalized van der Corput-Halton sequences and their subsequences*, Int. J. Number Theory **5** (2009), 719–746.

[9] HOFER, R.—LARCHER, G.: *On existence and discrepancy of certain digital Niederreiter-Halton sequences*, Acta Arith. **141** (2010), 369–394.

[10] HOFER, R.— LARCHER, G.—ZELLINGER, H.: *On the digits of squares and the distribution of quadratic subsequences of digital sequences,* Proc. Amer. Math. Soc **141** (2013), 1551–1565.

[11] IRELAND, K.—ROSEN, M.: *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1990.

[12] KRITZER, P.—PILLICHSHAMMER, F.: *On the existence of low-diaphony sequences made of digital sequences and lattice points,* Math. Nachrichten (**286)** (2013), no. 2-3, 224–235.

[13] LARCHER, G.—NIEDERREITER, H.: *Generalized (t, s)-sequences, Kronecker-type sequences, and Diophantine approximations of formal Laurent series, Trans. Amer. Math. Soc.* **347** (1995), no.6, 2051–2073.

[14] MAUDUIT, C.—RIVAT, J.: *La somme des chiffres des carrés,* Acta Math. **203** (2009), no. 1, 107–148.

[15] MAUDUIT, C.—RIVAT, J.: *Sur un problme de Gelfond : la somme des chiffres des nombres premiers,* Ann. of Math. (2) **171** (2010), no. 3, 1591-1646.

Received December 29, 2012
Accepted March 7, 2013

Roswitha Hofer
Heidrun Zellinger
Institute of Financial Mathematics
University of Linz
Altenbergerstraße 69
A-4040 Linz, Austria
E-mail: roswitha.hofer@jku.at
heidrun.zellinger@jku.at