JOURNAL OF COMPLEXITY **13,** 353–383 (1997)
ARTICLE NO. CM970451

Linear Complexity Profiles: Hausdorff Dimensions for Almost Perfect Profiles and Measures for General Profiles

Harald Niederreiter* and Michael Vielhaber

Institute of Information Processing, Austrian Academy of Sciences,
Sonnenfelsgasse 19, A-1010 Vienna, Austria

Received February 28, 1997

Stream ciphers usually employ some sort of pseudorandomly generated bit strings to be added to the plaintext. The cryptographic properties of such a sequence $\underline{a}$ can be stated in terms of the so-called linear complexity profile (l.c.p.), $L_{\underline{a}}(t)$, $t \in \mathbb{N}$. If the l.c.p. is $L_{\underline{a}}(t) = t/2 + O(1)$, it is called (*almost*) *perfect*. This paper examines first those subsets $\mathcal{A}_d^{(q)}$ of $\mathbb{F}_q^\infty$ where for fixed $d \in \mathbb{N}$ the l.c.p. satisfies $|2 \cdot L_{\underline{a}}(t) - t| \leq d$ for all $t \in \mathbb{N}$. It turns out that (after suitably mapping $\mathcal{A}_d^{(q)}$ on $[0, 1] \subset \mathbb{R}$) the Hausdorff dimension is

$$\frac{1 + \log_q \varphi_d^{(q)}}{2},$$

where $\varphi_d^{(q)}$ is the largest real root of $x^d = (q-1) \cdot \sum_{i=0}^{d-1} x^i$. The second part deals with nondecreasing bounds $d\colon \mathbb{N} \to \mathbb{N}$. Since $d(t) \to \infty$ as $t \to \infty$ always leads to a Hausdorff dimension 1, here we consider the measure of the set $\mathcal{A}_d^{(q)}$. © 1997 Academic Press

1. INTRODUCTION

The theory of stream ciphers (see Rueppel, 1986, 1992) deals with generating long pseudorandom sequences from short seeds (keys). These sequences should be indistinguishable from truly random sequences when judged by any complexity measure. A well-known complexity measure in the theory of stream ciphers is the global linear complexity, which for a periodic sequence of elements of the finite field $\mathbb{F}_q$ is defined as the shortest length of a linear feedback shift register (LFSR) generating the sequence (the global linear complexity of the zero sequence is defined to be zero). A more refined notion is the *linear complexity profile* (l.c.p.) of an arbitrary sequence $\underline{a} = (a_i)_{i=1}^\infty$ from the sequence space $\mathbb{F}_q^\infty$ over $\mathbb{F}_q$. The l.c.p. of $\underline{a}$ is the sequence $(L_{\underline{a}}(t))_{t=1}^\infty$, where for each t (consider

*E-mail: niederreiter@oeaw.ac.at.

0885-064X/97 $25.00

t as describing a "time" evolution) the nonnegative integer $L_{\underline{a}}(t)$ is the shortest length of an LFSR generating the initial string $(a_1, \ldots, a_t)$, with $L_{\underline{a}}(t) = 0$ if $(a_1, \ldots, a_t)$ is the zero string. Roughly, the l.c.p. of a random sequence $\underline{a}$ will grow with the length t like $L_{\underline{a}}(t) \approx t/2$. Deviations from this "ideal" median should occur, but only of moderate size (see Niederreiter, 1988b).

Rueppel (1986) introduced the notion of a sequence $\underline{a}$ with perfect linear complexity profile, requiring $L_{\underline{a}}(t) = \lceil t/2 \rceil$ for all $t \geq 1$, and Niederreiter (1988a) generalized it to the d-almost perfect linear complexity profile for $d \in \mathbb{N}$. This characterizes sequences $\underline{a}$ with $|2 \cdot L_{\underline{a}}(t) - t| \leq d$ for every length t. In order to avoid the repeated writing of "sequences with a d-almost perfect linear complexity profile," we call them *d-perfect*. Then 1-perfect corresponds to a perfect l.c.p. in the sense of Rueppel.

For any $d \in \mathbb{N}$, the set of all d-perfect sequences over $\mathbb{F}_q$ has uncountably many elements. On the other hand, it follows from Theorem 10 in Niederreiter (1988b) that the set of d-perfect sequences from $\mathbb{F}_q^\infty$ has measure zero in the space $(\mathbb{F}_q^\infty, \mu^\infty)$ of all sequences, where μ is the equidistribution measure on $\mathbb{F}_q$ (given by $u(k) = 1/q$ for all $k \in \mathbb{F}_q$) and μ^∞ its product measure on $\mathbb{F}_q^\infty$.

As the d-perfect sequences are too many to be counted and too few to be measured, the natural thing to study is the Hausdorff dimension of that set after it has been mapped in a canonical way to the interval [0, 1]. This is done in the first part of the paper, Sections 2–7. We shall see, in particular, that in the above sense the set of 1-perfect binary sequences has Hausdorff dimension 0.5 and for higher d the d-perfect sequences (over any $\mathbb{F}_q$) form sets of higher and higher Hausdorff dimension, though never reaching 1. Thus, although all these sets have measure zero in $\mathbb{F}_q^\infty$, a sharper distinction can be made by looking at their Hausdorff dimension. As a byproduct a formula for the number of d-perfect sequences of length t, for all d and t, is given for all finite fields $\mathbb{F}_q$ (see Theorem 17). We note that partial results in this direction for the binary case $q = 2$ have been presented in our earlier paper (Niederreiter and Vielhaber, 1995).

In the second part of the paper, Sections 8–11, the condition $|2 \cdot L_{\underline{a}}(t) - t| \leq d$ is relaxed to $|2 \cdot L_{\underline{a}}(t) - t| \leq d(t)$ for all t, where d is now a nondecreasing function on the positive integers. It will turn out (as was already shown in Theorems 8 and 9 of Niederreiter, 1988b, in the setting of dynamical systems theory) that $d(t) = 1 + (1 + \varepsilon) \cdot \log_q(t)$, with $\log_q$ being the logarithm to the base q, gives the threshold between measure zero ($\varepsilon = 0$) and positive measure ($\varepsilon > 0$). If $\lim_{t \to \infty} d(t) = \infty$, the Hausdorff dimension is 1 in any case.

2. LINEAR COMPLEXITY DEVIATION

For any sequence $\underline{a} \in \mathbb{F}_q^\infty$ we have $0 \leq L_{\underline{a}}(t) \leq t$ and $L_{\underline{a}}(t) \leq L_{\underline{a}}(t + 1)$ for all t. As $L_{\underline{a}}(t)$ is typically close to $t/2$, it merits the introduction of the following concept.

DEFINITION 1. Let $\underline{a} = (a_i)_{i=1}^N \in \mathbb{F}_q^N$, $N \in \mathbb{N} \cup \{\infty\}$, be a given sequence, $(L_{\underline{a}}(i))_{i=1}^N$ its l.c.p.; then the *linear complexity deviation* of $\underline{a}$ at t is defined as

$$m_{\underline{a}}(t) := 2 \cdot L_{\underline{a}}(t) - t \ \in \ \mathbb{Z}.$$

The l.c.p. can be computed by the Berlekamp–Massey algorithm (Rueppel, 1986; Lidl and Niederreiter, 1994). The following result recalls the dynamic behavior of $L_{\underline{a}}(t)$ and derives that of $m_{\underline{a}}(t)$ from it.

PROPOSITION 2.

(i) *If $L_{\underline{a}}(t) > t/2$, then $L_{\underline{a}}(t+1) = L_{\underline{a}}(t)$.*
(ii) *If $L_{\underline{a}}(t) \leq t/2$, then there exists a unique $a \in \mathbb{F}_q$ with*

$$L_{(a_1,\ldots,a_t,a)}(t+1) = L_{\underline{a}}(t).$$

For all $b \neq a$ in $\mathbb{F}_q$ we have

$$L_{(a_1,\ldots,a_t,b)}(t+1) = t + 1 - L_{\underline{a}}(t).$$

(iii) *If $m_{\underline{a}}(t) > 0$, then $m_{\underline{a}}(t+1) = m_{\underline{a}}(t) - 1$.*
(iv) *If $m_{\underline{a}}(t) \leq 0$, then there exists a unique $a \in \mathbb{F}_q$ with*

$$m_{(a_1,\ldots,a_t,a)}(t+1) = m_{(a_1,\ldots,a_t)}(t) - 1.$$

For all $b \neq a$ in $\mathbb{F}_q$ we have

$$m_{(a_1,\ldots,a_t,b)}(t+1) = 1 - m_{(a_1,\ldots,a_t)}(t).$$

Proof. (i, ii) See Rueppel (1986, p. 34).

(iii) By (i) we have $m_{\underline{a}}(t+1) = 2 \cdot L_{\underline{a}}(t+1) - t - 1 = (2 \cdot L_{\underline{a}}(t) - t) - 1 = m_{\underline{a}}(t) - 1$.

(iv) The first part follows from the first part of (ii). For $b \neq a$ the second part of (ii) yields $m_{\underline{a}}(t+1) = 2 \cdot L_{\underline{a}}(t+1) - t - 1 = 2 \cdot (t + 1 - L_{\underline{a}}(t)) - t - 1 = 1 + t - 2 \cdot L_{\underline{a}}(t) = 1 - m_{\underline{a}}(t)$. ■

Remark 3. When working over $\mathbb{F}_2$, the case $b \neq a$ obviously boils down to $b = \overline{a} = a + 1$.

Niederreiter (1988a, 1988b), as well as Dai and Zeng (1990), has shown the intimate connection between the l.c.p. of $(a_i)_{i=1}^\infty$ and the continued fraction expansion of the generating function $\sum_{i=1}^\infty a_i x^{-i}$ in the field of a formal Laurent series over $\mathbb{F}_q$. Hence, a jump by k in the l.c.p. is equivalent to a partial quotient of degree k in the continued fraction expansion, and d-perfect sequences lead to partial quotients that are all of degree at most d.

DEFINITION 4. Let $\mathcal{A}_d^{(q)} \subset \mathbb{F}_q^\infty$ be the set of all sequences $\underline{a}$ with $|m_{\underline{a}}(t)| \leq d$ for all $t \in \mathbb{N}$. Thus, $\mathcal{A}_d^{(q)}$ contains the d-perfect infinite sequences over $\mathbb{F}_q$.

3. TRANSLATION THEOREM

As a simple consequence of Proposition 2 we obtain the following translation theorem.

THEOREM 5. *Let* $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k)$ *and* $\underline{\beta} = (\beta_1, \ldots, \beta_l)$ *be given strings with* $m_{\underline{\alpha}}(k) = m_{\underline{\beta}}(l)$. *For any length* $t \geq 0$ *and deviation* $d \in \mathbb{Z}$, *we have*

$$\begin{aligned} &\text{card}\,\{\underline{a} \in \mathbb{F}_q^{k+t} \mid a_i = \alpha_i \quad \textit{for } 1 \leq i \leq k, \quad m_{\underline{a}}(k+t) = d\} \\ =\,&\text{card}\,\{\underline{b} \in \mathbb{F}_q^{l+t} \mid b_i = \beta_i \quad \textit{for } 1 \leq i \leq l, \quad m_{\underline{b}}(l+t) = d\}. \end{aligned}$$

Proof. Induction on t starts for $t = 0$ with both cardinalities being 1 for $d = m_{\underline{\alpha}}(k)$ and 0 otherwise by assumption. The step $t \to t+1$ follows by Proposition 2(iii, iv). ■

In other words, this translation theorem says that the distribution of l.c. deviations m on all suffixes of a given finite initial string depends only on m at the end of that string, but not on the length or the elements of the initial string.

Remark 6. The Translation Theorem already states some self-similarity within $\mathbb{F}_q^\infty$ or $\mathcal{A}_d^{(q)}$. Every prefix of length n with $m(n) = 0$ defines a cylinder set of continuations with the same m-distribution as the whole $\mathbb{F}_q^\infty$ or $\mathcal{A}_d^{(q)}$ (which can be seen as the cylinder set of ε, the empty word).

4. SOME COUNTING FORMULAE

In the course of Theorems 8 through 17 we shall see that asymptotically there are φ^t d-perfect initial sequences of length t for some real number $\varphi \geq 1$ depending on q and the bound d. Obviously, $\varphi = q$ describes the unrestricted case, which corresponds to formally putting $d = \infty$.

DEFINITION 7. Let $d \in \mathbb{N}$ and $m \in \mathbb{Z}$. For $t \in \mathbb{N}$ define $A_{m|d}^{(q)}(t)$ as the number of sequences $\underline{a} \in \mathbb{F}_q^t$ of length t with $m_{\underline{a}}(t) = m$ and $|m_{\underline{a}}(\tau)| \leq d$ for

$1 \leq \tau \leq t$. For $t = 0$ set $A^{(q)}_{0|d}(0) = 1$ (the empty sequence ε) and $A^{(q)}_{m|d}(0) = 0$ for $m \neq 0$. For $t \in \mathbb{Z}$, $t < 0$, set $A^{(q)}_{m|d}(t) = 0$.

We shall first obtain in Theorem 8 the behavior of sequence counts while adding another symbol from $\mathbb{F}_q$ and thus increasing the length from t to $t + 1$. This behavior is an immediate consequence of Proposition 2.

THEOREM 8. *For $t \in \mathbb{Z}$ and $d \in \mathbb{N}$ we have:*

$$\begin{array}{rll}
\text{(i) } A^{(q)}_{m|d}(t+1) & = A^{(q)}_{m+1|d}(t) & \text{for } -d \leq m < 0. \\
\text{(ii) } A^{(q)}_{0|d}(t+1) & = \begin{cases} q \cdot A^{(q)}_{1|d}(t), & t \neq -1, \\ 1, & t = -1. \end{cases} & \\
\text{(iii) } A^{(q)}_{m|d}(t+1) & = q \cdot A^{(q)}_{m+1|d}(t) + (q-1) \cdot A^{(q)}_{-m+1|d}(t) & \text{for } 0 < m \leq d. \\
\text{(iv) } A^{(q)}_{m|d}(t) & = 0 & \text{for } |m| > d. \\
\text{(v) } A^{(q)}_{m|d}(t) & = 0 & \text{for } m \not\equiv t(2).
\end{array}$$

Proof. All properties are trivial for $t \leq 0$, so we can assume $t \geq 1$. By Proposition 2(iii), sequences of length t with $m(t) > 0$ produce q successors of length $t + 1$ and $m(t+1) = m(t) - 1$. This gives us part (ii) and the first term of part (iii) (which is zero for $m = d$).

A sequence with $m(t) \leq 0$ splits its successors: one (the a case) ends up with $m(t+1) = m(t) - 1$. This is part (i), where $m(t) \leq 0$. All other $q - 1$ cases (for all $b \neq a$) lead to a jump to $m(t+1) = 1 - m(t) > 0$. This yields the second term in part (iii).

Finally, parts (iv) and (v) belong to impossible cases. By Definition 7, $|m|$ must not exceed d, and the parity of m and t must be the same by Definition 1. ■

EXAMPLE 9. Let $d = 3$, then we get for $A^{(2)}_{m|3}(t)$:

m	$t = 0$	1	2	3	4	5	6	7	8	9	10	11	12	13
3				1		2		8		32		112		416
2			1		4		12		48		176		640	
1		1		4		16		56		208		768		2816
0	1		2		8		32		112		416		1536	
−1		1		2		8		32		112		416		1536
−2			1		2		8		32		112		416	
−3				1		2		8		32		112		416

The next theorem links the $A^{(q)}_{m|d}(t)$ to just the $A^{(q)}_{0|d}(t)$. The above example may serve to illustrate the theorem.

THEOREM 10. *For $t \in \mathbb{Z}$ and $d \in \mathbb{N}$, every $A^{(q)}_{m|d}(t)$ can be expressed in terms of $A^{(q)}_{0|d}(t-\tau)$ as follows:*

$$\text{(i)}\quad A^{(q)}_{m|d}(t) = A^{(q)}_{0|d}(t+m) \qquad \text{for } -d \le m \le 0.$$

$$\text{(ii)}\quad A^{(q)}_{d|d}(t) = (q-1)\cdot A^{(q)}_{0|d}(t-d).$$

$$\text{(iii)}\quad A^{(q)}_{m|d}(t) = (q-1)\cdot \sum_{k=0}^{d-m} q^k \cdot A^{(q)}_{0|d}(t-m-2k) \qquad \text{for } 1 \le m \le d-1.$$

Proof.

(i) This is trivial for $t \le 0$. For $t \ge 1$ it follows by induction from Theorem 8(i).

(ii) This is obtained from (i) and

$$A^{(q)}_{d|d}(t) = (q-1)\cdot A^{(q)}_{-d|d}(t) \qquad \text{for all } t,$$

where this identity follows from Theorem 8(i, iii).

(iii) For $1 \le m \le d-1$ we get by Theorem 8(iii) that

$$A^{(q)}_{m|d}(t) = q \cdot A^{(q)}_{m+1|d}(t-1) + (q-1)\cdot A^{(q)}_{-m+1|d}(t-1).$$

Next, by induction on $k = 1, \ldots, d-m$ and Theorem 8(iii), we obtain

$$A^{(q)}_{m|d}(t) = q^k \cdot A^{(q)}_{m+k|d}(t-k) + (q-1)\cdot \sum_{i=1}^{k} q^{i-1}\cdot A^{(q)}_{-m-i+2|d}(t-i).$$

In particular, putting $k = d - m$ this yields

$$\begin{aligned} A^{(q)}_{m|d}(t) &= q^{d-m}\cdot A^{(q)}_{d|d}(t-d+m) + (q-1)\cdot \sum_{i=1}^{d-m} q^{i-1}\cdot A^{(q)}_{-m+2-i|d}(t-i) \\ &= (q-1)\cdot q^{d-m}\cdot A^{(q)}_{0|d}(t-2d+m) \\ &\quad + (q-1)\cdot \sum_{i=0}^{d-m-1} q^i \cdot A^{(q)}_{0|d}(t-2i-m) \\ &= (q-1)\cdot \sum_{i=0}^{d-m} q^i \cdot A^{(q)}_{0|d}(t-2i-m), \end{aligned}$$

where (i) and (ii) were used in the penultimate step. ■

DEFINITION 11. For $d \in \mathbb{N}$, $t \in \mathbb{Z}$, and q the order of the underlying field we define *generalized Fibonacci numbers* by

$$\mathrm{Fib}_d^{(q)}(t) = \begin{cases} 0, & t < 0, \\ 1, & t = 0, \\ (q-1) \cdot \displaystyle\sum_{k=1}^{d} \mathrm{Fib}_d^{(q)}(t-k), & t > 0. \end{cases}$$

Remark 12. Definition 11 readily implies that $\mathrm{Fib}_d^{(q)}(t) = (q-1) \cdot q^{t-1}$ for $1 \leq t \leq d$. The usual Fibonacci numbers 1, 1, 2, 3, 5 ... are obtained with $q = 2$ and $d = 2$.

DEFINITION 13. The number of sequences leaving the bound $|m| \leq d$ at time t by leading to $m(t) = d+1$ or $m(t) = -d-1$ is defined for $t \in \mathbb{N}$ and $d \in \mathbb{N}$ as

$$O_d^{(q)}(t) := q \cdot A_{-d|d}^{(q)}(t-1) = q \cdot A_{0|d}^{(q)}(t-d-1).$$

THEOREM 14. *Let $d \in \mathbb{N}$. Then*

(i) $A_{0|d}^{(q)}(t) = (q-1) \cdot \sum_{i=1}^{d} q^i \cdot A_{0|d}^{(q)}(t-2i)$ *for all $t \in \mathbb{N}$*

(ii) $A_{0|d}^{(q)}(2t) = q^t \cdot \mathrm{Fib}_d^{(q)}(t)$ *for all $t \in \mathbb{Z}$.*

(iii) *For $t \in \mathbb{N}$ we have*

$$O_d^{(q)}(t) = \begin{cases} 0, & t \equiv d(2), \\ q^{(t-d+1)/2} \cdot \mathrm{Fib}_d^{(q)}\left(\dfrac{t-d-1}{2}\right), & t \not\equiv d(2). \end{cases}$$

Proof.

(i) We have

$$\begin{aligned} A_{0|d}^{(q)}(t) &= q \cdot A_{1|d}^{(q)}(t-1) \\ &= q \cdot (q-1) \cdot \sum_{i=0}^{d-1} q^i \cdot A_{0|d}^{(q)}(t-2-2i) \\ &= (q-1) \cdot \sum_{i=1}^{d} q^i \cdot A_{0|d}^{(q)}(t-2i), \end{aligned}$$

where we used Theorem 8(ii) in the first step and Theorem 10(ii, iii) in the second step.

(ii) The result is trivial for $t < 0$, and for $t \geq 0$ we proceed by induction. Note that $A^{(q)}_{0|d}(0) = 1$ by definition counts just the empty word ε. For $t \geq 1$ we first use (i) and then the induction hypothesis to obtain

$$\begin{aligned} A^{(q)}_{0|d}(2t) &= (q-1) \cdot \sum_{i=1}^{d} q^i \cdot A^{(q)}_{0|d}(2t-2i) \\ &= (q-1) \cdot \sum_{i=1}^{d} q^i \cdot q^{t-i} \cdot \mathrm{Fib}^{(q)}_d(t-i) \\ &= (q-1) \cdot q^t \cdot \sum_{i=1}^{d} \mathrm{Fib}^{(q)}_d(t-i) \\ &= q^t \cdot \mathrm{Fib}^{(q)}_d(t). \end{aligned}$$

(iii) Apply (ii) to the definition. ■

The combination of Theorems 10 and 14 leads to the following general formula for $A^{(q)}_{m|d}(t)$.

THEOREM 15. *Let $t \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then*

$$A^{(q)}_{m|d}(t) = \begin{cases} 0, & |m| > d \text{ or } t \not\equiv m(2), \\ q^{(t+m)/2} \cdot \mathrm{Fib}^{(q)}_d\left(\dfrac{t+m}{2}\right), & -d \leq m \leq 0,\ t \equiv m(2), \\ (q-1) \cdot q^{(t-m)/2} \cdot \displaystyle\sum_{k=0}^{d-m} \mathrm{Fib}^{(q)}_d\left(\dfrac{t-m}{2} - k\right), & 1 \leq m \leq d,\ t \equiv m(2). \end{cases}$$

DEFINITION 16. For $t \in \mathbb{N}_0$ and $d \in \mathbb{N}$ let

$$A^{(q)}_{*|d}(t) := \sum_{m=-d}^{d} A^{(q)}_{m|d}(t)$$

be the overall number of d-bound sequences of length t over $\mathbb{F}_q$.

THEOREM 17. *For $t \in \mathbb{N}_0$ and $d \in \mathbb{N}$ we have*

$$A^{(q)}_{*|d}(t) = \frac{1}{q-1} \cdot q^{\lfloor (t-d)/2 \rfloor + 1} \cdot \mathrm{Fib}^{(q)}_d(\lfloor (t+d+1)/2 \rfloor).$$

Proof. We proceed by induction on t. For $t = 0$ we have $A_{*|d}^{(q)}(0) = 1$, which agrees with the right-hand side of the formula in the theorem in view of Remark 12. For the step from t to $t + 1$ we distinguish two cases.

(a) $t \equiv d(2)$: Then $O_d^{(q)}(t+1) = q^{(t-d+2)/2} \cdot \mathrm{Fib}_d^{(q)}((t-d)/2)$ by Theorem 14(iii), and thus

$$\begin{aligned} A_{*|d}^{(q)}(t+1) &= q \cdot A_{*|d}^{(q)}(t) - O_d^{(q)}(t+1) \\ &= \frac{1}{q-1} \cdot q^{(t-d)/2+2} \cdot \mathrm{Fib}_d^{(q)}\left(\frac{t+d}{2}\right) \\ &\quad - q^{(t-d)/2+1} \cdot \mathrm{Fib}_d^{(q)}\left(\frac{t-d}{2}\right) \\ &= q^{(t-d)/2+1} \cdot \left(\mathrm{Fib}_d^{(q)}\left(\frac{t+d}{2}\right) + \sum_{i=1}^{d} \mathrm{Fib}_d^{(q)}\left(\frac{t+d}{2} - i\right)\right. \\ &\quad \left. - \mathrm{Fib}_d^{(q)}\left(\frac{t-d}{2}\right)\right) \\ &= q^{(t-d)/2+1} \cdot \sum_{i=1}^{d} \mathrm{Fib}_d^{(q)}\left(\frac{t+d}{2} + 1 - i\right) \\ &= \frac{1}{q-1} \cdot q^{(t-d)/2+1} \cdot \mathrm{Fib}_d^{(q)}\left(\frac{t+d}{2} + 1\right). \end{aligned}$$

(b) $t \not\equiv d(2)$: Then $O_d^{(q)}(t+1) = 0$ by Theorem 14(iii), and thus

$$\begin{aligned} A_{*|d}^{(q)}(t+1) &= q \cdot A_{*|d}^{(q)}(t) \\ &= \frac{1}{q-1} \cdot q^{\lfloor (t-d)/2 \rfloor + 2} \cdot \mathrm{Fib}_d^{(q)}(\lfloor (t+d+1)/2 \rfloor) \\ &= \frac{1}{q-1} \cdot q^{\lfloor (t+1-d)/2 \rfloor + 1} \cdot \mathrm{Fib}_d^{(q)}(\lfloor (t+d+2)/2 \rfloor). \quad \blacksquare \end{aligned}$$

Remark 18. This finishes the combinatorics of d-perfect sequences. Theorem 17 can be stated as $A_{*|d}^{(q)}(t) = O(q^{t/2} \cdot \mathrm{Fib}_d^{(q)}(\lfloor (t+d+1)/2 \rfloor))$. This will lead to the Hausdorff dimension of $\iota(\mathcal{A}_d^{(q)})$.

We need another technical lemma, bounding the generalized Fibonacci numbers in terms of some algebraic numbers φ.

DEFINITION 19. Let $\varphi_d := \varphi_d^{(q)}$ be the largest real root of

$$x^d = (q-1) \cdot \sum_{i=0}^{d-1} x^i.$$

LEMMA 20. *For all q and $d \in \mathbb{N}$ we have*

$$\text{(i) } q - \frac{q}{q^d} \le \varphi_d^{(q)} < q - \frac{q-1}{q^d},$$
$$\text{(ii) } \frac{q-1}{q} \cdot (\varphi_d^{(q)})^t < \mathrm{Fib}_d^{(q)}(t) \le (\varphi_d^{(q)})^t \qquad \textit{for all } t \in \mathbb{N}_0.$$

Proof.

(i) For $d = 1$ we have $\varphi_1^{(q)} = q - 1$, hence the result. For $d \ge 2$ (thus $\varphi_d^{(q)} \ne 1$) we set $\varphi := \varphi_d^{(q)}$. Then

$$\begin{aligned}
\varphi^d &= (q-1) \cdot \sum_{i=0}^{d-1} \varphi^i \\
&= (q-1) \cdot \frac{\varphi^d - 1}{\varphi - 1} \\
\Leftrightarrow \varphi^{d+1} - \varphi^d &= (q-1) \cdot \varphi^d - (q-1) \\
\Leftrightarrow \varphi^{d+1} &= \varphi^d \cdot q - (q-1) \\
\Leftrightarrow \varphi &= q - \frac{q-1}{\varphi^d}.
\end{aligned}$$

Since $\varphi < q$, we have $\varphi < q - (q-1)/q^d$, and thus the upper bound is proven.

To show the lower bound for $d \ge 2$, we examine the function $f(x) = x - q + (q-1)/x^d$, which satisfies $f(\varphi) = 0$. We have

$$\begin{aligned}
f\left(q - \frac{q}{q^d}\right) &= -q^{-d+1} + (q-1)/(q^d(1 - q^{-d})^d) \\
&< -q^{-d+1} + (q-1)/(q^d - d) \\
&= (d \cdot q^{1-d} - 1)/(q^d - d) \le 0
\end{aligned}$$

for $d \ge 2$, $q \ge 2$. Thus $f(q - q/q^d) < f(\varphi)$, and from

$$f'(x) = 1 - \frac{d(q-1)}{x^{d+1}} > 0 \qquad \text{for } x \ge q - \frac{1}{2}$$

we may conclude $q – q/q^d < \varphi$.

(ii) $t = 0$ is trivial. For $1 \le t \le d$ we have in view of (i) and Remark 12,

$$\begin{aligned}
\frac{q-1}{q} \cdot (\varphi_d^{(q)})^t < \frac{q-1}{q} \cdot q^t &= (q-1) \cdot q^{t-1} = \mathrm{Fib}_d^{(q)}(t) \\
&= q^t - q^{t-1} \\
&\le q^t - t \cdot q^{t-1} \cdot q^{-d+1} \le (q - q^{-d+1})^t \le (\varphi_d^{(q)})^t.
\end{aligned}$$

The result now follows by induction on t as $(\varphi_d^{(q)})^t$ and $\mathrm{Fib}_d^{(q)}(t)$ satisfy the same recursion. ■

5. THE STEADY STATE

The formulae for $A_{m|d}^{(q)}(t)$ and $A_{*|d}^{(q)}(t)$ in the limit $t \to \infty$ give the proportion of sequences with deviation m.

DEFINITION 21. Let

$$p_d^{(q)}(m) := \lim_{\substack{t\to\infty \\ t\equiv m(2)}} \frac{A_{m|d}^{(q)}(t)}{A_{*|d}^{(q)}(t)}$$

for $d \in \mathbb{N}$ and $m \in \mathbb{Z}$ with $|m| \leq d$. There is an obvious analog for $d = \infty$.

THEOREM 22. (i) *With* $\varepsilon = (m+d) \bmod 2$ *and* $\varphi := \varphi_d^{(q)}$ *we obtain for* $d \in \mathbb{N}$ *and* $-d \leq m \leq 0$:

$$p_d^{(q)}(m) = (q-1) \cdot q^{(m+d+\varepsilon)/2-1} \cdot \varphi^{-(d-m+\varepsilon)/2},$$

and for $1 \leq m \leq d$,

$$p_d^{(q)}(m) = (q-1)^2 \cdot q^{(d-m+\varepsilon)/2-1} \cdot \sum_{k=0}^{d-m} \varphi^{-((d+m+\varepsilon)/2+k)}.$$

(ii) *For* $d = \infty$ *we obtain*

$$p_\infty^{(q)}(m) = (q-1) \cdot q^{m-1} \qquad \text{for } m \leq 0$$

and

$$p_\infty^{(q)}(m) = (q-1) \cdot q^{-m} \qquad \text{for } m > 0.$$

Proof. (i) From the form of the polynomial equation in Definition 19 it is easily seen that all roots of this equation different from $\varphi_d^{(q)}$ are less than $\varphi_d^{(q)}$ in absolute value. Since $(\varphi_d^{(q)})^t$ and $\mathrm{Fib}_d^{(q)}(t)$ satisfy the same recursion, we obtain

$$\lim_{t\to\infty} \frac{\mathrm{Fib}_d^{(q)}(t+1)}{\mathrm{Fib}_d^{(q)}(t)} = \varphi_d^{(q)}.$$

The desired formulae now follow from Theorems 15 and 17.

(ii) For $d = \infty$ we replace φ by $\lim_{d\to\infty} \varphi_d^{(q)} = q$. ■

Remark 23. Even and odd m are normalized separately to measure 1. Thus $\sum_{m=-d}^{d} p_d^{(q)}(m) = 2$.

6. BACKGROUND ON HAUSDORFF DIMENSION

We follow the introduction of the Hausdorff dimension given in Chapter 2 of Falconer (1990) for a subset $\mathcal{A}$ of the reals. Set

$$h_\varepsilon^s(\mathcal{A}) = \inf \sum_{i=1}^{\infty} |U_i|^s \qquad \text{for } s \geq 0,\ \varepsilon > 0,$$

where the infimum runs over all covers $\mathcal{U} = \{U_1, U_2, \ldots\}$ of $\mathcal{A}$ with intervals U_i of length $|U_i| \leq \varepsilon$, and letting $\varepsilon \to 0$:

$$h^s(\mathcal{A}) := \lim_{\varepsilon\to 0+} h_\varepsilon^s(\mathcal{A}).$$

Then

$$h^s(\mathcal{A}) = \begin{cases} 0, & s > D_H(\mathcal{A}) \\ \infty, & s < D_H(\mathcal{A}) \end{cases}$$

for a certain real number $D_H(\mathcal{A})$ ($h^{D_H(\mathcal{A})}(\mathcal{A})$ may assume any value in $[0, \infty]$).

DEFINITION 24. The Hausdorff dimension of a set $\mathcal{A}$ is defined as

$$\begin{aligned} D_H(\mathcal{A}) &= \inf\{s | h^s(\mathcal{A}) = 0\} \\ &= \sup\{s | h^s(\mathcal{A}) = \infty\}. \end{aligned}$$

Remark 25. The definition of $h_\varepsilon^s(\mathcal{A})$ and thus of $h^s(\mathcal{A})$ involves an infimum. Thus, an upper bound for the Hausdorff dimension is considerably easier to obtain than a lower bound, for the former one essentially defines a sequence of covers $\mathcal{U}^{(k)} = \{U_1^{(k)}, U_2^{(k)}, \ldots\}$, where $|U_i^{(k)}| \leq \varepsilon_k$ and $\varepsilon_k \to 0$. If then $\sum_{i=1}^{\infty} |U_i^{(k)}|^s$ remains bounded for every cover of the sequence, the infimum cannot be infinity. Hence the candidate s actually is an upper bound.

On the contrary, if s is below the Hausdorff dimension, it will lead to a sum $\sum_{i=1}^{\infty} |U_i^{(k)}|^s = \infty$ for each and every cover, and so the infimum cannot be determined in this way. Here we have to apply an analog of the Mass Distribution Principle (see Theorem 4.2 in Falconer, 1990). Other special techniques to get lower bounds are given in Chapter 4 of that monograph.

LEMMA 26. *Let ν be a mass distribution on some set $A \subseteq [0, 1] \subset \mathbb{R}$. We assume that for a given s there exist two real numbers $c > 0$ and $\delta > 0$ such that*

$$\nu(U) \leq c \cdot |U|^s$$

for all intervals $U \subseteq [0, 1]$ with $|U| \leq \delta$. Then $D_H(A) \geq s$.

Proof. Let $0 < \varepsilon \leq \delta$. Let $\mathcal{U} = \{U_i\}$ be any cover of A by intervals $U_i \subseteq [0, 1]$ of length $|U_i| \leq \varepsilon \leq \delta$. Then

$$0 < \nu(A) = \nu\left(\bigcup_i U_i\right) \leq \sum_i \nu(U_i) \leq c \cdot \sum_i |U_i|^s,$$

hence

$$\sum_i |U_i|^s \geq \frac{\nu(A)}{c}.$$

It follows that the infimum over all $\mathcal{U}$ gives

$$h^s_\varepsilon(A) \geq \frac{\nu(A)}{c} \qquad \text{for all } \varepsilon \leq \delta,$$

and so $h^s(A) \geq \nu(A)/c > 0$, hence $s \leq D_H(A)$. ■

DEFINITION 27. An *N-ary interval* of degree k, $N \in \mathbb{N}$, $k \in \mathbb{N}_0$, is an interval of the form $[r \cdot N^{-k}, (r + 1) \cdot N^{-k})$, $0 \leq r \leq N^k - 2$, $r \in \mathbb{N}_0$, or $[1 - N^{-k}, 1]$.

LEMMA 28. *Consider a nonempty subset $A \subseteq [0, 1] \subset \mathbb{R}$ of the reals and N-ary intervals with $N \geq 2$. Let there be a natural number $S \leq N$ such that for each $k \in \mathbb{N}_0$ we have: If an N-ary interval I of degree k has nonempty intersection with A, then exactly S of the N-ary subintervals of I of degree $k + 1$ also have nonempty intersection with A. In this case*

$$D_H(A) \geq \frac{\log S}{\log N}.$$

Proof. Each interval $U \subset [0, 1]$ with $|U| < 1$ satisfies an inequality $N^{-k-1} \leq |U| < N^{-k}$ for a certain $k \in \mathbb{N}_0$. Thus, U can intersect at most two N-ary intervals of degree k.

Define a mass distribution ν on A such that each of the S^k N-ary intervals of degree k (of length N^{-k}) that intersect A contains a mass of S^{-k}. The mass that is covered by U can thus be bounded by $\nu(U) \leq 2 \cdot S^{-k}$.

For $s := (\log S)/(\log N)$ we thus obtain

$$\begin{aligned}\nu(U) &\leq 2\cdot S^{-k} = 2\cdot (N^{-k})^s = 2\cdot N^s\cdot (N^{-k-1})^s\\ &\leq 2\cdot N^s\cdot |U|^s\\ &\leq 2\cdot N\cdot |U|^s,\end{aligned}$$

where we used that $0 \leq s \leq 1$. Now we can apply Lemma 26. ■

EXAMPLE 29. Let $N = 3$ and $S = 2$. This describes the Cantor set, and indeed $(\log 2)/(\log 3)$ is its Hausdorff dimension.

7. THE HAUSDORFF DIMENSION OF THE d-PERFECT SEQUENCES

DEFINITION 30. The space $\mathbb{F}_q^\infty$ of all infinite sequences can be mapped onto the unit interval $[0, 1]$ by

$$\iota := \iota_q : \mathbb{F}_q^\infty \ni (a_i)_{i=1}^\infty \mapsto \sum_{i=1}^\infty \psi(a_i)q^{-i} \in [0,\ 1] \subset \mathbb{R},$$

where ψ is a fixed bijection from $\mathbb{F}_q$ to $\{0, 1, \ldots, q-1\}$.

If $\mathcal{A}_d^{(q)} \subset \mathbb{F}_q^\infty$ is the set in Definition 4, then we study the subset $\mathcal{B}_d^{(q)} := \iota(\mathcal{A}_d^{(q)})$ of $[0, 1]$.

THEOREM 31. *For all $d \in \mathbb{N}$ and q we have*

$$D_H(\mathcal{B}_d^{(q)}) = \frac{1 + \log_q \varphi_d^{(q)}}{2},$$

where $\log_q$ *denotes the logarithm to the base q and $\varphi_d^{(q)}$ is as in Definition 19.*

Proof. We work over some fixed $\mathbb{F}_q$ and set $\varphi_d := \varphi_d^{(q)}$. We first show an upper bound for the Hausdorff dimension. For fixed $t \geq 1$, consider the set of all initial strings $\underline{a}$ of length t with $|m_{\underline{a}}(\tau)| \leq d$ for $1 \leq \tau \leq t$. The cardinality of this set is $A_{*|d}^{(q)}(t)$. By Theorem 17 and Lemma 20(ii) we have

$$A_{*|d}^{(q)}(t) \leq \frac{1}{q-1}\cdot q^{(t-d)/2+1}\cdot \varphi_d^{(t+d+1)/2} \leq C\cdot (q\cdot\varphi_d)^{t/2}$$

with a constant $C > 0$ depending only on d and q. Each initial string $\underline{a}$ of length t defines a cylinder set in $\mathbb{F}_q^\infty$ consisting of all infinite continuations of this string. The image of each such cylinder set under the map ι is a closed interval of length q^{-t} in [0, 1]. Thus, $\mathcal{B}_d^{(q)}$ can be covered by $A_{*|d}^{(q)}(t)$ intervals of length q^{-t}. With $\varepsilon_t = q^{-t}$ it follows that

$$h^s_{\varepsilon_t}(\mathcal{B}_d^{(q)}) \le A_{*|d}^{(q)}(t) \cdot q^{-ts} \le C \cdot \left(\frac{\sqrt{q \cdot \varphi_d}}{q^s} \right)^t .$$

For any $s > \frac{1}{2}(1 + \log_q \varphi_d)$ we have $q^s > \sqrt{q \cdot \varphi_d}$. Thus, letting $t \to \infty$ (hence $\varepsilon_t \to 0$), we get

$$h^s(\mathcal{B}_d^{(q)}) = 0.$$

By the definition of $D_H(\mathcal{B}_d^{(q)})$ it follows that $D_H(\mathcal{B}_d^{(q)}) \le s$. Since $s > \frac{1}{2}(1 + \log_q \varphi_d)$ is arbitrary, we obtain

$$D_H(\mathcal{B}_d^{(q)}) \le \frac{1}{2}\,(1 + \log_q\, \varphi_d).$$

Thus, the upper bound is shown.

To prove the lower bound, we define for $r \in \mathbb{N}$,

$$\mathcal{A}_d^{(q)}(r) := \{\underline{a} \in \mathcal{A}_d^{(q)} \mid m_{\underline{a}}(2r \cdot n) = 0 \text{ for all } n \in \mathbb{N}\}, \qquad \mathcal{B}_d^{(q)}(r) := \iota(\mathcal{A}_d^{(q)}(r)).$$

$\mathcal{A}_d^{(q)}(r)$ contains $S := A_{0|d}^{(q)}(2r)$ initial strings (prefixes) of length $2r$ that end at $m(2r) = 0$. By Theorem 5 (or Proposition 2(iii, iv)) we can iterate this process to obtain S^n prefixes of length $2r \cdot n$ with $m(2r \cdot j) = 0$, $1 \le j \le n$. By the mapping $\iota(\mathcal{A}_d^{(q)}(r)) = \mathcal{B}_d^{(q)}(r)$ we thus obtain a subset of [0, 1] for which we can apply Lemma 28 with $N := q^{2r}$ (note that sequences in $\mathbb{F}_q^\infty$ that are ultimately constant cannot belong to $\mathcal{A}_d^{(q)}$, and so no problems with endpoints of N-ary intervals can arise). As $S \ge (q-1)/q \cdot q^r \cdot \varphi_d^r \ge (1/q) \cdot q^r \cdot \varphi_d^r$ by Theorem 14(ii) and Lemma 20(ii), we obtain

$$D_H(\mathcal{B}_d^{(q)}(r)) \ge \frac{\log_q\, S}{\log_q\,(q^{2r})} \ge \frac{\log_q(q^r \cdot \varphi_d^r \cdot q^{-1})}{2r} = \frac{1 + \log_q\, \varphi_d}{2} - \frac{1}{2r}.$$

The last inequality is valid for all $r \in \mathbb{N}$ and we have $\mathcal{A}_d^{(q)} \supseteq \mathcal{A}_d^{(q)}(r)$ and thus $\mathcal{B}_d^{(q)} \supseteq \mathcal{B}_d^{(q)}(r)$. Hence the Hausdorff dimension of $\mathcal{B}_d^{(q)}$ is bounded from below by

$$D_H(\mathcal{B}_d^{(q)}) \ge \frac{1 + \log_q\, \varphi_d}{2} - \frac{1}{2r} \qquad \text{for all } r \in \mathbb{N},$$

and together with the upper bound we finally arrive at

$$D_H(\mathcal{B}_d^{(q)}) = \frac{1 + \log_q \varphi_d}{2}. \quad \blacksquare$$

Remark 32. The values $\varphi_d^{(q)}$ and $D_H(\mathcal{B}_d^{(q)})$ may be estimated for large d by

$$\begin{aligned} \varphi_d^{(q)} &\approx q - q^{-d+1}, \\ \log_q (\varphi_d^{(q)}) &\approx 1 - 1/(q^d \cdot \log q), \\ s_d^{(q)} := D_H(\mathcal{B}_d^{(q)}) &\approx 1 - 1/(2 \cdot q^d \cdot \log q). \end{aligned}$$

Some values for $q = 2$:

$$\begin{array}{llll} \varphi_1^{(2)} = 1 & \varphi_2^{(2)} = 1.618\ldots & \varphi_3^{(2)} = 1.839\ldots & \varphi_4^{(2)} = 1.928\ldots \\ s_1^{(2)} = 0.5 & s_2^{(2)} = 0.8471\ldots & s_3^{(2)} = 0.9396\ldots & s_4^{(2)} = 0.9734\ldots \end{array}$$

($\varphi_2^{(2)}$ is the well-known “Golden ratio”).

Remark 33. Now that we know $D_H(\mathcal{B}_d^{(q)})$, what is its meaning in the information-theoretic sense? Consider an information source over the alphabet $\mathbb{F}_q$. This source emits a data stream of some sort. If it is independent and identically distributed, the information rate is $\log_2 q$ bits per time unit or one q-ary digit per time unit. A lower information rate leads to a somewhat predictable symbol sequence. Not all q^t sequences of length t are then equally likely. And this is where our $D_H(\mathcal{B}_d^{(q)})$ comes into play. Assume the source emits any (a priori unknown) sequence from $\mathcal{A}_d^{(q)}$. Then the information rate is $D_H(\mathcal{B}_d^{(q)})$ q-ary digits per symbol, or stated in terms of message space versus symbol space, of all q^t sequences of length t only $q^{t \cdot D_H(\mathcal{B}_d^{(q)})}$ are possible (in the limit $t \to \infty$). Thus, $D_H(\mathcal{B}_d^{(q)})$ describes the entropy or information rate of an $\mathcal{A}_d^{(q)}$-source. By an unpublished result of Wang and Massey (see Niederreiter, 1988a, for a published proof and also the related work of Baum and Sweet, 1977), 1-perfect binary sequences consist of bits that are alternatingly fixed by internal relations ($a_1 = 1$, $a_{2k+1} = a_{2k} \oplus a_k$) or can be chosen arbitrarily (the a_{2k}). Thus, the entropy is $\frac{1}{2} = D_H(\mathcal{B}_1^{(2)})$.

Remark 34. The survey paper by Shallit (1992) treats real numbers with bounded partial quotients in their continued fraction expansion. This is the real analog of d-perfect sequences in $\mathbb{F}_q^\infty$ (compare with Section 2). In $\mathbb{R}$ the metric is not ultrametric, rendering the case much more difficult, as can already be seen from the Hausdorff dimension of the set $\overline{\mathcal{E}}_2$ of all numbers in [0, 1] with partial quotients from {1, 2}, namely

$$0.53128049\cdots < D_H(\overline{\mathcal{E}}_2) < 0.53128051\cdots.$$

The closed form for $D_H(\overline{\mathcal{E}}_2)$ is $D_H(\overline{\mathcal{E}}_2) = \lim_{n\to\infty} \sigma_n$, where σ_n is the real root of

$$\sum_{1\leq a_1, \ldots, a_n \leq 2} Q(a_1, \ldots, a_n)^{-2\sigma_n} = 1$$

and the Q polynomials (Euler's continuants) are defined recursively by $Q() = 1$, $Q(a_1) = a_1$, $Q(a_1, \ldots, a_n) = a_n \cdot Q(a_1, \ldots, a_{n-1}) + Q(a_1, \ldots, a_{n-2})$.

8. GENERALIZATION TO TIME-DEPENDENT BOUNDS

Up to now we have dealt with a fixed bound d for the allowed linear complexity deviation. Under these circumstances we will always obtain a set of measure zero. In the remaining part of the paper we will allow the bound d to be dependent on t, that is, $d\colon \mathbb{N} \to \mathbb{N}$ to be a nondecreasing function of t. We say that m is bounded by the *fence* $d(t)$.

If $d(t) \to d' < \infty$ as $t \to \infty$, then we obtain the Hausdorff dimension belonging to the constant bound d' (the initial part $d < d'$ amounts to some constant that may be put into the C in the proof of Theorem 31 and C does not affect the Hausdorff dimension). On the other hand, $d(t) \to \infty$ as $t \to \infty$ leads to a Hausdorff dimension 1, and every d other than the unrestricting case $d(t) \geq t$ leads to a measure less than 1. Thus, the important threshold here is measure zero versus positive measure.

We shall obtain upper and lower bounds for the measure, depending on $d(t)$. The lower bound here will be zero only if the upper bound and hence the measure is zero as well. We shall first obtain an even more general recursion for the $A^{(q)}_{0|d}(2t)$ (d now a function of t). Then the $A^{(q)}_{*|d}(2t)$ will be bounded by sums of $A^{(q)}_{0|d}(2t)$ and the latter ones by products of $\varphi^{(q)}_d$. Finally, we obtain from

$$\mu^\infty(\mathcal{A}^{(q)}_d) = \lim_{t\to\infty} \frac{A^{(q)}_{*|d}(2t)}{q^{2t}}$$

effectively computable bounds for the measure.

For binary sequences we shall obtain that the fence $d(t) = 1 + \lfloor \log_2(t) \rfloor$ encloses a set of measure zero, whereas $d(t) = 1 + 2 \cdot \lfloor \log_2(t) \rfloor$ leads to a positive measure.

9. EFFECTIVE AND CANONICAL FENCES

DEFINITION 35. Let $d\colon \mathbb{N} \to \mathbb{N}$ be a function with:

(i) $d(1) = 1$.

(ii) $d(t) \leq d(t+1) \leq d(t) + 1$ for all $t \in \mathbb{N}$.

(iii) If $d(t) < d(t+1)$ and $d(t+1) = d(t+2k)$ for some $t \in \mathbb{N}$ and $k \in \mathbb{N}$, then $d(t+1) = d(t+2k+1)$. For all $k \in \mathbb{N}$, if $d(2k) = 1$ then $d(2k+1) = 1$.

Then d is called an *effective fence*.

An effective fence thus starts with width 1, does not jump over a width, and stays at each width for an odd number of time steps (unless it remains constant on that level).

LEMMA 36. *If d is an effective fence and $d(t+1) = d(t) + 1$ for some $t \in \mathbb{N}$, then the sum $t + d(t)$ is even.*

Proof. For $d(1) = 1$ as the first occurrence of width 1 the sum $1 + d(1)$ is even. Until the next larger width by Definition 35(iii) there is an odd number of steps, and together with the increase by 1 of the width, $t + d(t)$ is even by induction on the widths. ■

LEMMA 37. *To every nondecreasing function d: $\mathbb{N} \to \mathbb{N}$ we can assign an effective fence Δ such that $\Delta(t) \leq d(t)$ for all $t \in \mathbb{N}$ and for all effective fences $\overline{\Delta}$ the inequality $\Delta(t) \leq \overline{\Delta}(t) \leq d(t)$ for all $t \in \mathbb{N}$ already implies $\Delta = \overline{\Delta}$.*

Proof. Construct a fence Δ by setting $\Delta(1) = 1$ and

$$\Delta(t+1) = \begin{cases} \Delta(t), & \text{if } d(t+1) = \Delta(t) \text{ or } t + \Delta(t) \text{ odd}, \\ \Delta(t) + 1, & \text{if } d(t+1) > \Delta(t) \text{ and } t + \Delta(t) \text{ even}. \end{cases}$$

By construction, no other effective fence gets nearer to d from below. ■

DEFINITION 38. The effective fence Δ in Lemma 37 is called the *canonical fence* of the function d. We emphasize this by writing $d_{\text{can}} := \Delta$.

Remark 39. As every effective fence is its own canonical fence, we have an equivalence relation on the set of all nondecreasing functions, and every equivalence class has a unique effective fence as the canonical fence of each of its members. The set of equivalence classes, or as well the set of effective fences, forms a lattice where $d(t) = 1$ is the infimum and $d(t) = t$ is the supremum, leading to $\mathcal{A}_1^{(q)}$ and $\mathbb{F}_q^\infty$, respectively.

THEOREM 40. *For every nondecreasing function d: $\mathbb{N} \to \mathbb{N}$ we have*

$$\mathcal{A}_d^{(q)} := \{\underline{a} \in \mathbb{F}_q^\infty \mid |m_{\underline{a}}(t)| \leq d(t) \text{ for all } t\}$$
$$= \mathcal{A}_{d_{\text{can}}}^{(q)} := \{\underline{a} \in \mathbb{F}_q^\infty \mid |m_{\underline{a}}(t)| \leq d_{\text{can}}(t) \text{ for all } t\}.$$

Proof. Since $\mathcal{A}_{d_{\mathrm{can}}}^{(q)} \subseteq \mathcal{A}_d^{(q)}$ is trivial, it suffices to show that for all $\underline{a} \in \mathcal{A}_d^{(q)}$ we have

$$|m_{\underline{a}}(t)| \leq d_{\mathrm{can}}(t) \qquad \text{for all } t \in \mathbb{N}.$$

This inequality is established by induction on t, with the case $t = 1$ being trivial. In the step from t to $t + 1$, the case $d_{\mathrm{can}}(t+1) = d(t+1)$ is obvious. If $d_{\mathrm{can}}(t+1) = d_{\mathrm{can}}(t) + 1$, then by Proposition 2(iii, iv),

$$|m_{\underline{a}}(t+1)| \leq |m_{\underline{a}}(t)| + 1 \leq d_{\mathrm{can}}(t) + 1 = d_{\mathrm{can}}(t+1).$$

In the remaining case, we have $d_{\mathrm{can}}(t + 1) = d_{\mathrm{can}}(t) < d(t + 1)$. By the construction of d_{can} in the proof of Lemma 37, $t + d_{\mathrm{can}}(t)$ is odd, hence $d_{\mathrm{can}}(t) + 1 \equiv t$ mod 2. On the other hand, we have $|m_{\underline{a}}(t+1)| \leq d_{\mathrm{can}}(t)+1$ as before, and from Definition 1 we have $|m_{\underline{a}}(t+1)| \equiv t+1$ mod 2, thus $|m_{\underline{a}}(t+1)| \neq d_{\mathrm{can}}(t)+1$. Now $|m_{\underline{a}}(t+1)| \leq d_{\mathrm{can}}(t) = d_{\mathrm{can}}(t+1)$ follows. ■

From now on, we assume that a given fence is already reduced to the canonical one. As an example, $\mathcal{A}_{d=\mathrm{const.}}^{(q)}$ would be defined by

$$d_{\mathrm{can}}(t) = \begin{cases} t, & \text{if } t \leq d, \\ d, & \text{if } t > d. \end{cases}$$

DEFINITION 41. Let d be an effective fence.

(i) Define δ on the even numbers as

$$\delta(t + d(t)) = d(t)$$

for $t \in \mathbb{N}$ with $t + d(t)$ even (by Definition 35 and Lemma 36, δ is defined on $2\mathbb{N}$).

(ii) With δ from part (i) let

$$r(m) = \mathrm{card}\{t \in 2\mathbb{N} \,|\, \delta(t) = m\} = \frac{1}{2} \cdot (1 + \mathrm{card}\{t \in \mathbb{N} \,|\, d(t) = m\})$$

for $m \in \mathbb{N}$.

DEFINITION 42. Let d be an effective fence and $m \in \mathbb{Z}$. For $t \in \mathbb{N}$ define $A_{m|d}^{(q)}(t)$ as the number of sequences $\underline{a} \in \mathbb{F}_q^t$ of length t with $m_{\underline{a}}(t) = m$ and $|m_{\underline{a}}(\tau)| \leq d(\tau)$ for $1 \leq \tau \leq t$. For $t = 0$ set $A_{0|d}^{(q)}(0) = 1$ and $A_{m|d}^{(q)}(0) = 0$ for $m \neq 0$. For $t \in \mathbb{Z}$, $t < 0$, set $A_{m|d}^{(q)}(t) = 0$.

Remark 43. δ gives the width of the fence that actually influences $A^{(q)}_{0|d}(t)$ for even t. There are $r(k)$ occurrences at time steps $t \equiv k(2)$ of k as the outer bound of the fence when $A^{(q)}_{k|d}(t) > 0$. Thus, in $r(k) - 1$ places (where $t \not\equiv k(2)$) the fence actually has a diminishing effect while $d(t) = k$.

EXAMPLE 44. To illustrate δ and r consider this diagram for $A^{(2)}_{m|d}(t)$:

t:		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
d(t):			1	1	1	2	3	3	3	4	4	4	4	4	5	5
$\delta(t)$:				1		1		2		3		3		4		4
m	r(m)															
5	≥ 2														48	—
4	3									4	—	**16**	—	48		288
3	2						2	—	**4**		16		**48**		288	
2	1					2		4		**24**		80		**288**		1280
1	2		1	—	2		8		24		**96**		352		**1280**	
0		1		2		4		16		48		**192**		704		**2560**
-1			1		2		4		16		48		192		704	
-2						2		4		16		48		192		704
-3							2		4		16		48		192	
-4										4		16		48		192
-5															48	

The two diagonals in boldface show the significance of δ. The value of $A^{(2)}_{0|d}(10) = 192$ depends on the three elements 4, 24, 96 in the diagonal in addition to elements below $m = 0$. Thus $\delta(10) = 3$, as the largest m-value in this diagonal is $m = 3$ at timestep $t - \delta(t) = 7$, similarly for $t = 14$ (second diagonal in boldface). The border elements are connected by hyphens within each m-value. The border contains $r(m)$ values on level m and there are $r(m) - 1$ hyphens, places where the fence has a diminishing effect.

10. $A^{(q)}_{m|d}$ FOR GENERAL $d(t)$

In this section we evaluate the quantity $A^{(q)}_{m|d}(t)$ in Definition 42 for even t. Since $A^{(q)}_{m|d}(t) = 0$ for odd m, we can assume that m is even.

THEOREM 45. *Let d be an effective fence. Then*

$$A^{(q)}_{0|d}(2t) = \begin{cases} 0, & t < 0 \\ 1, & t = 0 \\ (q-1) \cdot \sum_{\tau=1}^{\delta(2t)} q^{\tau} \cdot A^{(q)}_{0|d}(2t - 2\tau), & t > 0. \end{cases}$$

Proof. The case $t \leq 0$ follows from Definition 42. For $t \geq 1$ we show

$$A^{(q)}_{0|d}(2t) = q^k \cdot A^{(q)}_{k|d}(2t-k) + (q-1) \cdot \sum_{\tau=1}^{k-1} q^\tau \cdot A^{(q)}_{0|d}(2t-2\tau)$$

by induction on $k = 1, 2, \ldots, \delta(2t)+1$. The theorem then follows from the case $k = \delta(2t)+1$, since here $A^{(q)}_{\delta(2t)+1|d}(2t-\delta(2t)-1) = 0$ because $\delta(2t) \geq d(2t-\delta(2t)-1)$. The case $k = 1$ is obvious. For the step from k to $k + 1$ we note that

$$\begin{aligned} &q^k \cdot A^{(q)}_{k|d}(2t-k) \\ &= q^k \cdot (q \cdot A^{(q)}_{k+1|d}(2t-k-1) + (q-1) \cdot A^{(q)}_{-k+1|d}(2t-k-1)) \\ &= q^{k+1} \cdot A^{(q)}_{k+1|d}(2t-(k+1)) + (q-1) \cdot q^k \cdot A^{(q)}_{0|d}(2t-2k), \end{aligned}$$

where in the first identity we used Proposition 2(iii, iv) and the fact that

$$k \leq \delta(2t) = d(2t-\delta(2t)) \leq d(2t-k) \qquad \text{for } 1 \leq k \leq \delta(2t).$$

In the second identity we used again Proposition 2(iii, iv) as well as

$$j \leq d(u-d(u)+j) \qquad \text{for } 1 \leq j \leq d(u) \text{ and } u \in \mathbb{N}.$$

This inequality follows from $d(u-l) \geq d(u)-l$ for all $u \in \mathbb{N}$, $0 \leq l \leq d(u)-1$ (by Definition 35(ii)), and putting $l := d(u) - j$. ■

THEOREM 46. *Let d be an effective fence. Then $A^{(q)}_{0|d}(2t)$ can be computed iteratively as $A^{(q)}_{0|d}(0) = 1$, $A^{(q)}_{0|d}(2) = q \cdot (q-1)$, and*

$$A^{(q)}_{0|d}(2t) = \begin{cases} q^2 \cdot A^{(q)}_{0|d}(2t-2), \\ \quad \text{for } t > 1 \text{ and } \delta(2t) = 1 + \delta(2t-2) \\ q^2 \cdot A^{(q)}_{0|d}(2t-2) - (q-1) \cdot q^{\delta(2t)+1} \cdot A^{(q)}_{0|d}(2t-2(\delta(2t)+1)), \\ \quad \text{for } t > 1 \text{ and } \delta(2t) = \delta(2t-2) \end{cases}$$

Proof. The cases $t = 0$ and $t = 1$ follow from Theorem 45. For $t > 1$ and $\delta(2t) = 1 + \delta(2t-2)$ we obtain by Theorem 45,

$$\begin{aligned} A^{(q)}_{0|d}(2t) &= (q-1) \cdot \sum_{\tau=1}^{\delta(2t)} q^\tau \cdot A^{(q)}_{0|d}(2t-2\tau) \\ &= (q-1) \cdot q \cdot A^{(q)}_{0|d}(2t-2) + (q-1) \cdot q \cdot \sum_{\tau'=1}^{\delta(2t-2)} q^{\tau'} \\ &\quad \cdot A^{(q)}_{0|d}(2t-2-2\tau') \\ &= ((q-1) \cdot q + q) \cdot A^{(q)}_{0|d}(2t-2). \end{aligned}$$

For $t > 1$ and $\delta(2t) = \delta(2t-2)$ we have

$$\begin{aligned} A_{0|d}^{(q)}(2t) &= (q-1) \cdot \sum_{\tau=1}^{\delta(2t)} q^{\tau} \cdot A_{0|d}^{(q)}(2t-2\tau) \\ &= (q-1) \cdot q \cdot A_{0|d}^{(q)}(2t-2) + (q-1) \cdot q \cdot \sum_{\tau'=1}^{\delta(2t-2)} q^{\tau'} \\ &\quad \cdot A_{0|d}^{(q)}(2t-2-2\tau') - (q-1) \cdot q \cdot q^{\delta(2t-2)} \\ &\quad \cdot A_{0|d}^{(q)}(2t-2-2\delta(2t-2)) \\ &= q^2 \cdot A_{0|d}^{(q)}(2t-2) - (q-1) \cdot q^{\delta(2t)+1} \cdot A_{0|d}^{(q)}(2t-2(\delta(2t)+1)). \quad \blacksquare \end{aligned}$$

THEOREM 47. *Let d be an effective fence. For even m we have*

$$A_{m|d}^{(q)}(2t) = \begin{cases} A_{0|d}^{(q)}(2t+m), & -d(2t) \le m \le 0 \\ (q-1) \cdot \displaystyle\sum_{k=0}^{\delta(2t+m)-m} q^k \cdot A_{0|d}^{(q)}(2t-m-2k), & 2 \le m \le d(2t). \end{cases}$$

Proof. This follows as in Theorem 10. In the first case, we also use the bound

$$j \le d(u - d(u) + j) \qquad \text{for } 1 \le j \le d(u) \text{ and } u \in \mathbb{N}$$

shown in the proof of Theorem 45. In the second case, the upper bound for the summation index k is best verified by consulting Example 44: The falling diagonal including $A_{m|d}^{(q)}(2t)$ intersects the line $m = 0$ at $2t + m$. By Definition 41, $\delta(2t + m)$ is the largest m-value on this diagonal and replaces d in Theorem 10. $\blacksquare$

11. THE MEASURE OF $\mathcal{A}_d^{(q)}$

For a nondecreasing function d: $\mathbb{N} \to \mathbb{N}$ we put, as in Theorem 40,

$$\mathcal{A}_d^{(q)} = \{\underline{a} \in \mathbb{F}_q^{\infty} \mid |m_{\underline{a}}(t)| \le d(t) \text{ for all } t \in \mathbb{N}\}.$$

In this section we study $\mu^{\infty}(\mathcal{A}_d^{(q)})$, where μ^{∞} is the probability measure on $\mathbb{F}_q^{\infty}$ defined in Section 1. In view of Theorem 40 it suffices to consider effective fences d. Also, since the case where $\lim_{t\to\infty} d(t)$ is finite can be reduced to results in earlier sections (see Section 8), we will concentrate on the case where $\lim_{t\to\infty} d(t) = \infty$.

DEFINITION 48. For an effective fence d and $t \in \mathbb{N}$ define

$$A^{(q)}_{*|d}(t) = \sum_{m=-d(t)}^{d(t)} A^{(q)}_{m|d}(t).$$

LEMMA 49. *For every effective fence d we have*

$$\mu^{\infty}(\mathcal{A}^{(q)}_d) = \lim_{t\to\infty} \frac{A^{(q)}_{*|d}(2t)}{q^{2t}}.$$

Proof. For $t \in \mathbb{N}$ we introduce the cylinder set

$$\mathcal{A}^{(q)}_d(t) = \{\underline{a} \in \mathbb{F}_q^{\infty} \mid |m_{\underline{a}}(\tau)| \le d(\tau) \text{ for } 1 \le \tau \le t\}.$$

Then $\mathcal{A}^{(q)}_d(1) \supseteq \mathcal{A}^{(q)}_d(2) \supseteq \cdots$ and $\mathcal{A}^{(q)}_d = \cap_{t=1}^{\infty} \mathcal{A}^{(q)}_d(t)$, thus in particular

$$\mu^{\infty}(\mathcal{A}^{(q)}_d) = \lim_{t\to\infty} \mu^{\infty}(\mathcal{A}^{(q)}_d(2t)).$$

By Definitions 42 and 48 we have

$$\mu^{\infty}(\mathcal{A}^{(q)}_d(2t)) = \frac{A^{(q)}_{*|d}(2t)}{q^{2t}}. \quad \blacksquare$$

LEMMA 50. *For* $\lim_{t\to\infty} d(t) = \infty$ *we have*

$$\lim_{t\to\infty} \frac{A^{(q)}_{*|d}(2t)}{A^{(q)}_{0|d}(2t)} = \frac{q}{q-1}.$$

Proof. According to Theorem 22(ii) the unrestricted steady state has

$$p^{(q)}_{\infty}(0) = \frac{q-1}{q}.$$

Any deviation from the steady state (too high a weight on some m) will lead (after m steps for $m \ge 0$ and gradually for $m \le 0$) to a proportion too high at

$m = 0$. By the translation theorem (Theorem 5) this will diffuse into the steady state since $d(t) \to \infty$. Thus, for $t \to \infty$ we have

$$\lim_{t\to\infty} \frac{A_{*|d}^{(q)}(2t)}{A_{0|d}^{(q)}(2t)} = (p_\infty^{(q)}(0))^{-1} = \frac{q}{q-1}. \quad \blacksquare$$

Remark 51. Now we already can compute an upper bound for $\mu^\infty\ (\mathcal{A}_d^{(q)})$ by Theorem 46. Since the sequence

$$\left(\frac{A_{0|d}^{(q)}(2t)}{q^{2t}}\right)_{t=1}^{\infty}$$

decreases monotonously, we have

$$\mu^\infty(\mathcal{A}_d^{(q)}) \leq \frac{q}{q-1} \cdot \frac{A_{0|d}^{(q)}(2t)}{q^{2t}} \qquad \text{for all } t \in \mathbb{N}.$$

In Section 4 we have seen that for constant d we asymptotically have

$$A_{*|d}^{(q)}(t) \approx C \cdot q^{t/2} \cdot (\varphi_d^{(q)})^{t/2}.$$

For effective fences d: $\mathbb{N} \to \mathbb{N}$ we thus will divide the fence into regions of constant d-values (regarding d as a step function), and then each step will be bounded as stated above. We shall choose the division into steps according to the sequence $A_{0|d}^{(q)}$ which is easier to handle than $A_{*|d}^{(q)}$, thus the length of each step is determined by δ, not d.

For every width m, there are $r(m)$ time steps where $\delta(2t) = m$. For $r(m) > m$, the $(m + 1)$st to $r(m)$th recursion (in Theorem 45) is given as that of $A_{0|m}^{(q)}(2t)$ (compare with Theorem 14(i)), thus here the increase is roughly by a factor $\sqrt{q \cdot \varphi_m^{(q)}}$. The first m values require some additional considerations, though. We start with the division into steps according to δ.

DEFINITION 52. Let d be an effective fence with $\lim_{t\to\infty} d(t) = \infty$. For $j \in \mathbb{N}$ we define

$$\Delta_j := 2 \cdot \max\{\tau \mid \delta(2\tau) = j\},$$

where δ is from Definition 41(i).

Thus we have $\delta(\Delta_j) = j$, but $\delta(\Delta_j + 2) = j + 1$. Using the function r from Definition 41(ii), furthermore

$$\Delta_j = 2 \cdot \sum_{k=1}^{j} r(k) \text{ and } r(j) = \frac{1}{2} \cdot (\Delta_j - \Delta_{j-1}).$$

The sequence $A_{0|d}^{(q)}(2 \cdot i)$, $i \in \mathbb{N}_0$, satisfies (by Theorem 45) a recursion and Δ_j is the largest integer such that $A_{0|d}^{(q)}(\Delta_j)$ is computed by a recursion of degree j. The jth step thus extends from $\Delta_{j-1} + 2$ to Δ_j.

The following lemma bounds the increase of $A_{0|d}^{(q)}(2t)$, $t \in \mathbb{N}$, in a way which is independent of previous step lengths.

LEMMA 53. *For all effective fences d with $\lim_{t\to\infty} d(t) = \infty$ and for all $k \in \mathbb{N}$ we have*

$$q^2 - q^{2-\delta(2k+2)} \leq \frac{A_{0|d}^{(q)}(2k+2)}{A_{0|d}^{(q)}(2k)} \leq q^2.$$

Proof. The upper bound follows from Theorem 46. We show the lower bound by induction on k. For $k = 1$ we have two cases, $d(2) = \delta(4) = 1$ or $d(2) = \delta(4) = 2$. Note that $A_{0|d}^{(q)}(2) = (q-1) \cdot q$ in both cases. By Theorem 46 we have $A_{0|d}^{(q)}(4) = (q-1)^2 \cdot q^2$ if $d(2) = 1$ and $A_{0|d}^{(q)}(4) = (q-1) \cdot q^3$ if $d(2) = 2$, and the lower bound follows.

We will now assume that the lower bound holds for $1 \leq i < k$ and let $j: = \delta(2k + 2)$. We can also assume that we are in the second case of Theorem 46, i.e., that $\delta(2k + 2) = \delta(2k)$. In order to apply Theorem 46, we have to bound the quotient $(A_{0|d}^{(q)}(2k))/(A_{0|d}^{(q)}(2k-2j))$ from below. From Definition 41, we have $\delta(2t + 2) \leq \delta(2t) + 1$ for all $t \in \mathbb{N}$ and thus $\delta(2k - 2j) \geq \delta(2k) - j$. Hence with $l := \delta(2k - 2j)$, out of the j (double) steps between $2k - 2j$ and $2k$ there are $j - l \geq 0$ steps where the width increases. Here, by the first case of Theorem 46, the factor is exactly q^2, whereas that factor is at least $q^2 - q^{2-l}$ in the remaining l steps by the induction hypothesis. The case $l = 0$ leads to an overall increase q^{2j} and thus will not yield the minimal value. This leads to

$$\frac{A_{0|d}^{(q)}(2k)}{A_{0|d}^{(q)}(2k-2j)} \geq \min_{1\leq l\leq j} \{q^{2\cdot(j-l)} \cdot (q^2 - q^{2-l})^l\} = q^{2j} \cdot \min_{1\leq l\leq j} \{(1 - q^{-l})^l\}.$$

Now for all $q \geq 2$ and $l \geq 1$ we have $(1 - q^{-l})^l \geq 1 - l \cdot q^{-l} \geq 1 - q^{-1}$, where the first inequality is obtained by the mean-value theorem. This gives the lower bound

$$A_{0|d}^{(q)}(2k) \geq A_{0|d}^{(q)}(2k-2j) \cdot q^{2j-1} \cdot (q-1).$$

We thus have from Theorem 46,

$$\begin{aligned} A_{0|d}^{(q)}(2k+2) &= q^2 \cdot A_{0|d}^{(q)}(2k) - (q-1) \cdot q^{j+1} \cdot A_{0|d}^{(q)}(2k-2j) \\ &\geq A_{0|d}^{(q)}(2k) \cdot \left(q^2 - (q-1) \cdot q^{j+1} \cdot \frac{1}{q^{2j-1} \cdot (q-1)} \right) \\ &= A_{0|d}^{(q)}(2k) \cdot (q^2 - q^{2-j}). \quad \blacksquare \end{aligned}$$

THEOREM 54. *For all effective fences d with $\lim_{t\to\infty} d(t) = \infty$ and for $j \geq 2$ we have*

$$\begin{aligned} & q^{r(j)+1} \cdot (q - q^{1-j})^{\min\{j-1,\, r(j)-1\}} \cdot \varphi_j^{\max\{r(j)-j,\, 0\}} \\ & \leq \frac{A_{0|d}^{(q)}(\Delta_j)}{A_{0|d}^{(q)}(\Delta_{j-1})} \\ & \leq q^{\min\{r(j)+j,\, 2\cdot r(j)\}} \cdot \varphi_j^{\max\{r(j)-j,\, 0\}}, \end{aligned}$$

where $\varphi_j = \varphi_j^{(q)}$ is given by Definition 19.

Proof. For $r(j) \leq j$ the theorem follows from Lemma 53, taking into account that due to Theorem 46 the first step after Δ_{j-1} amounts to a factor of q^2.

We may thus assume $r(j) > j$ and we show by induction on i that

$$\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i)}{A_{0|d}^{(q)}(\Delta_{j-1})} \geq q^{i+1} \cdot (q - q^{1-j})^{j-1} \cdot \varphi_j^{i-j} \qquad \text{for } j \leq i \leq r(j).$$

The case $i = j$ follows by the argument above. For $j < i \leq r(j)$ and $1 \leq \tau \leq j$ we deduce by similar arguments that

$$\begin{aligned} \frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i-2\tau)}{A_{0|d}^{(q)}(\Delta_{j-1})} &\geq q^{i-\tau+1} \cdot (q - q^{1-j})^{i-\tau-1} \\ &= q^{i-\tau+1} \cdot (q - q^{1-j})^{j-1} \cdot (q - q^{1-j})^{i-\tau-j}. \end{aligned}$$

Since $q - q^{1-j} \leq \varphi_j$ by Lemma 20(i), it follows that for $i - \tau < j$ we obtain

$$\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i-2\tau)}{A_{0|d}^{(q)}(\Delta_{j-1})} \geq q^{i-\tau+1} \cdot (q - q^{1-j})^{j-1} \cdot \varphi_j^{i-\tau-j},$$

whereas for $i - \tau \geq j$ this inequality holds by induction hypothesis. Hence by Theorem 45,

$$\begin{aligned}\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i)}{A_{0|d}^{(q)}(\Delta_{j-1})} &= (q-1)\cdot\sum_{\tau=1}^{j} q^{\tau}\cdot\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i-2\tau)}{A_{0|d}^{(q)}(\Delta_{j-1})}\\ &\geq (q-1)\cdot\sum_{\tau=1}^{j} q^{\tau}\cdot q^{i-\tau+1}\cdot(q-q^{1-j})^{j-1}\cdot\varphi_j^{i-\tau-j}\\ &= q^{i+1}\cdot(q-q^{1-j})^{j-1}\cdot(q-1)\cdot\sum_{\tau=1}^{j}\varphi_j^{i-\tau-j}\\ &= q^{i+1}\cdot(q-q^{1-j})^{j-1}\cdot\varphi_j^{i-j}.\end{aligned}$$

The last step follows from Definition 19. Putting $i = r(j)$ yields the lower bound in the theorem.

For the upper bound (and still $r(j) > j$) we first show that

$$\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i)}{A_{0|d}^{(q)}(\Delta_{j-1})} \leq q^{i+j}\cdot\varphi_j^{i-j} \qquad \text{for } 1 \leq i \leq r(j).$$

For $1 \leq i \leq j$ this holds by Lemma 53 and the fact that $\varphi_j < q$ according to Lemma 20(i). For $j < i \leq r(j)$ we proceed by induction on i and Theorem 45 to obtain

$$\begin{aligned}\frac{A_{0|d}^{(q)}(\Delta_{j-1}+2i)}{A_{0|d}^{(q)}(\Delta_{j-1})} &\leq (q-1)\cdot\sum_{\tau=1}^{j} q^{\tau}\cdot q^{i+j-\tau}\cdot\varphi_j^{i-j-\tau}\\ &= q^{i+j}\cdot\varphi_j^{-j}\cdot(q-1)\cdot\sum_{\tau=1}^{j}\varphi_j^{i-\tau}\\ &= q^{i+j}\cdot\varphi_j^{i-j},\end{aligned}$$

where we used Definition 19 in the last step. Putting $i = r(j)$ yields the upper bound in the theorem. ■

THEOREM 55. *Let d be an effective fence with* $\lim_{t\to\infty} d(t) = \infty$. *For each $k \in \mathbb{N}$ we have*

$$\begin{aligned}&\frac{q-1}{q}\cdot q^{\Delta_k/2+k}\cdot\prod_{j=1}^{k}(q-q^{1-j})^{\min\{j-1,\,r(j)-1\}}\cdot\varphi_j^{\max\{r(j)-j,\,0\}}\\ &\leq A_{0|d}^{(q)}(\Delta_k)\\ &\leq \frac{q-1}{q}\cdot q^{\Delta_k/2}\cdot\prod_{j=1}^{k} q^{\min\{j,\,r(j)\}}\cdot\varphi_j^{\max\{r(j)-j,\,0\}}.\end{aligned}$$

Proof. We have $\Delta_1 = 2 \cdot r(1) = 1 + \operatorname{card}\{t \in \mathbb{N} \mid d(t) = 1\}$, and from Theorem 14(ii) we get for $k = 1$,

$$\begin{aligned} A_{0|d}^{(q)}(\Delta_1) &= A_{0|1}^{(q)}(\Delta_1) = q^{\Delta_1/2} \cdot \mathrm{Fib}_1^{(q)}(\Delta_1/2) = q^{\Delta_1/2} \cdot (q-1)^{\Delta_1/2} \\ &= \frac{q-1}{q} \cdot q^{\Delta_1/2+1} \cdot \varphi_1^{r(1)-1}. \end{aligned}$$

For arbitrary k we proceed by induction and Theorem 54. ■

THEOREM 56. *For every effective fence d with* $\lim_{t\to\infty} d(t) = \infty$ *we have the following bounds for* $\mu^\infty(\mathcal{A}_d^{(q)})$*:*

$$\begin{aligned} \prod_{j=1}^{\infty}(1-q^{-j})^{r(j)-1} &\le \prod_{j=1}^{\infty}(1-q^{-j})^{\min\{j-1,\, r(j)-1\}} \cdot \left(\frac{\varphi_j}{q}\right)^{\max\{r(j)-j,\, 0\}} \\ &\le \mu^\infty(\mathcal{A}_d^{(q)}) \\ &\le \prod_{j=1}^{\infty}\left(\frac{\varphi_j}{q}\right)^{\max\{r(j)-j,\, 0\}} \le \prod_{j=1}^{\infty}\left(1-\frac{q-1}{q^{j+1}}\right)^{\max\{r(j)-j,\, 0\}}. \end{aligned}$$

Proof. From Lemmas 49 and 50 we get

$$\mu^\infty(\mathcal{A}_d^{(q)}) = \frac{q}{q-1} \cdot \lim_{k\to\infty} \frac{A_{0|d}^{(q)}(\Delta_k)}{q^{\Delta_k}}.$$

The inner bounds now follow from Theorem 55 by letting $k \to \infty$. The outer bounds are obtained from Lemma 20(i). ■

LEMMA 57. *If*

$$U := \prod_{j=1}^{\infty}\left(1-\frac{q-1}{q^{j+1}}\right)^{\max\{r(j)-j,\, 0\}} > 0,$$

then

$$L := \prod_{j=1}^{\infty}(1-q^{-j})^{r(j)-1} > 0.$$

Proof. First, $\max\{r(j)-j,\, 0\}$ may be replaced by $r(j)-1$, since

$$\begin{aligned} 1 > \prod_{j=1}^{\infty}\left(1-\frac{q-1}{q^{j+1}}\right)^{j-1} &\ge \prod_{j=1}^{\infty}\left(1-\frac{1}{q^{j}}\right)^{j-1} > e^{-2\cdot\sum_{j=1}^{\infty}(j-1)/q^j} \\ &= e^{-2/(q-1)^2} \ge e^{-2}. \end{aligned}$$

Furthermore, for $q \geq 2$ and $j \in \mathbb{N}$ we have

$$\begin{aligned}
&(1-q^{-j}) - \left(1 - \frac{q-1}{q} \cdot q^{-j}\right)^3 \\
&\quad = 1 - q^{-j} - 1 + 3\,\frac{q-1}{q} \cdot q^{-j} - 3\left(\frac{q-1}{q}\right)^2 \cdot q^{-2j} + \left(\frac{q-1}{q}\right)^3 \cdot q^{-3j} \\
&\quad \geq q^{-j} \cdot \left(-1 + 3\,\frac{q-1}{q} - 3\left(\frac{q-1}{q}\right)^2 \cdot q^{-j}\right) \\
&\quad \geq q^{-j} \cdot \left(\frac{1}{2} - 3(q-1)^2 \cdot q^{-3}\right) \\
&\quad \geq q^{-j} \cdot \left(\frac{1}{2} - \frac{3 \cdot 4}{27}\right) > 0.
\end{aligned}$$

Hence $L \geq (U \cdot e^{-2})^3 > 0$. ■

The following is the main result of this section. Compare this result with Theorems 8 and 9 of Niederreiter (1988b), which were shown by the theory of dynamical systems.

THEOREM 58. *Let d be an effective fence. Then:*

$$\begin{array}{llcl}
\text{(i)} & \displaystyle\sum_{t=1}^{\infty} q^{-d(t)} < \infty & \Leftrightarrow & \mu^{\infty}(\mathcal{A}_d^{(q)}) > 0. \\
\text{(ii)} & \displaystyle\sum_{t=1}^{\infty} q^{-d(t)} = \infty & \Leftrightarrow & \mu^{\infty}(\mathcal{A}_d^{(q)}) = 0. \\
\text{(iii)} & \begin{array}{l}\underline{\lim}_{t\to\infty}(d(t) - \alpha \cdot \log_q(t)) \\ \quad > -\infty \textit{ for some } \alpha > 1\end{array} & \Rightarrow & \mu^{\infty}(\mathcal{A}_d^{(q)}) > 0. \\
\text{(iv)} & \overline{\lim}_{t\to\infty}(d(t) - \log_q(t)) < \infty & \Rightarrow & \mu^{\infty}(\mathcal{A}_d^{(q)}) = 0.
\end{array}$$

Proof. (i) In view of Lemma 57, any bound from Theorem 56 may be used to separate the cases $\mu^{\infty}(\mathcal{A}_d^{(q)}) = 0$ and $\mu^{\infty}(\mathcal{A}_d^{(q)}) > 0$. We use the lower bound

$$\begin{aligned}
\mu^{\infty}(\mathcal{A}_d^{(q)}) > 0 &\Leftrightarrow \log \mu^{\infty}(\mathcal{A}_d^{(q)}) > -\infty \\
&\Leftrightarrow \log \prod_{k=1}^{\infty} \left(1 - \frac{1}{q^k}\right)^{r(k)-1} > -\infty \\
&\Leftrightarrow \sum_{k=1}^{\infty} (r(k)-1) \cdot \left(-\frac{1}{q^k}\right) > -\infty \\
&\Leftrightarrow \sum_{k=1}^{\infty} (2 \cdot r(k) - 1) \cdot q^{-k} < \infty.
\end{aligned}$$

Since $r(k)$ leads to $2 \cdot r(k) - 1$ time steps where $d(t) = k$, we obtain

$$\mu^{\infty}(\mathcal{A}_d^{(q)}) > 0 \Leftrightarrow \sum_{k=1}^{\infty} \sum_{\substack{t=1 \\ d(t)=k}}^{\infty} q^{-d(t)} < \infty \Leftrightarrow \sum_{t=1}^{\infty} q^{-d(t)} < \infty.$$

(ii) is equivalent to (i).

(iii) $\sum_{t=1}^{\infty} q^{-d(t)} \leq C \cdot \sum_{t=1}^{\infty} q^{-\alpha \cdot \log_q (t)} = C \cdot \sum_{t=1}^{\infty} (1/t^{\alpha}) < \infty$ for some $C > 0$. The result follows from (i).

(iv) $\sum_{t=1}^{\infty} q^{-d(t)} \geq C \cdot \sum_{t=1}^{\infty} q^{-\log_q (t)} = C \cdot \sum_{t=1}^{\infty} (1/t) = \infty$ for some $C > 0$. The result follows from (ii). ■

EXAMPLE 59. We shall now obtain measure bounds for the fences defined by the functions $d(t) = 1 + \lfloor \log_2 (t) \rfloor$ and $d(t) = 1 + 2 \cdot \lfloor \log_2 (t) \rfloor \leq 1 + \lfloor 2 \cdot \log_2 (t) \rfloor$ in the case $q = 2$ (cases (iv) and (iii) in Theorem 58, respectively).

(i) Let $d(t) = 1 + \lfloor \log_2 (t) \rfloor$ with $q = 2$. Then by Theorem 58(iv)

$$\mu^{\infty}(\mathcal{A}_d^{(2)}) = 0.$$

(ii) We let $d(t) = 1 + 2 \cdot \lfloor \log_2 (t) \rfloor$ with $q = 2$. The canonical fence now contains a width k for every even k, and $k = 1$ exactly once, and the odd $k = 2j + 1$, $k \geq 3$, occur $2^j - 1$ times. Thus

$$\mu^{\infty}(\mathcal{A}_d^{(2)}) =: \mu \geq \prod_{j=1}^{\infty} \left(1 - \frac{1}{2^{2j+1}}\right)^{2^{j-1}-1}.$$

Since $\log (1 - \varepsilon) \geq -\varepsilon/(1 - \varepsilon)$ and here $\varepsilon \leq \frac{1}{8}$, we may bound by $\log (1 - \varepsilon) \geq -\frac{8}{7} \cdot \varepsilon$. Therefore

$$\log \mu \geq -\frac{8}{7} \cdot \sum_{j=1}^{\infty} \frac{2^{j-1} - 1}{2^{2j+1}} = -\frac{2}{21}.$$

The measure thus is at least $e^{-2/21} \approx 0.909 \ldots > 0$.

REFERENCES

Baum, L. E., and Sweet, M. M. (1977), Badly approximable power series in characteristic 2, *Ann. Math.* **105,** 573–580.

Dai, Z. D., and Zeng, K. C. (1990), Continued fractions and the Berlekamp–Massey algorithm, *in* "Advances in Cryptology—AUSCRYPT '90" (J. Seberry and J. Pieprzyk, Eds.), Lecture Notes in Computer Science, Vol. 453, pp. 24–31, Springer-Verlag, Berlin.

Falconer, K. (1990), “Fractal Geometry—Mathematical Foundations and Applications,” Wiley, Chichester.

Lidl, R., and Niederreiter, H. (1994), “Introduction to Finite Fields and Their Applications,” rev. ed., Cambridge Univ. Press, Cambridge.

Niederreiter, H. (1988a), Sequences with almost perfect linear complexity profile, *in* “Advances in Cryptology—EUROCRYPT ’87” (D. Chaum and W. L. Price, Eds.), Lecture Notes in Computer Science, Vol. 304, pp. 37–51, Springer-Verlag, Berlin.

Niederreiter, H. (1988b), The probabilistic theory of linear complexity, *in* “Advances in Cryptology—EUROCRYPT ’88” (C. G. Günther, Ed.), Lecture Notes in Computer Science, Vol. 330, pp. 191–209, Springer-Verlag, Berlin.

Niederreiter, H. (1990), A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences, *J. Cryptology* **2,** 105–112.

Niederreiter, H., and Vielhaber, M. (1995), On the fractal nature of the set of all binary sequences with almost perfect linear complexity profile, *in* “Communications and Multimedia Security” (R. Posch, Ed.), pp. 214–221, Chapman & Hall, London.

Rueppel, R. A. (1986), “Analysis and Design of Stream Ciphers,” Springer-Verlag, Berlin.

Rueppel, R. A. (1992), Stream ciphers, *in* “Contemporary Cryptology—The Science of Information Integrity” (G. J. Simmons, Ed.), pp. 65–134, IEEE Press, New York.

Shallit, J. (1992), Real numbers with bounded partial quotients: A survey, *Enseign. Math. Sér. II,* **38,** 151–187.