The Uniform Distribution of Sequences Generated by Iteration of Polynomials

Emil Lerner*

Faculty of Computational Mathematics and Cybernetics,
Moscow State University

March 30, 2015

Abstract

Consider a collection f of polynomials $f_i(x)$, $i = 1, \ldots, s$, with integer coefficients such that polynomials $f_i(x) - f_i(0)$, $i = 1, \ldots, s$, are linearly independent. Denote by D_m the discrepancy for the set of points $\left(\frac{f_1(x) \bmod m}{m}, \ldots, \frac{f_s(x) \bmod m}{p^n}\right)$ for all $x \in \{0, 1, \ldots, m\}$, where $m = p^n$, $n \in N$, and p is a prime number. We prove that $D_m \to 0$ as $n \to \infty$, and $D_m < c_1(\log\log m)^{-c_2}$, where c_1 and c_2 are positive constants that depend only on the collection of f_i. As a corollary, we obtain an analogous result for iterations of any polynomial (with integer coefficients) whose degree exceeds 1. Certain results on the uniform distribution were known earlier only for some classes of polynomials with $s \leqslant 3$.

1 Introduction

The construction of pseudorandom generators (PRG) is one of most important cryptographic problems; they have many various practical applications. We assume that a PRG consists of

- a transition function f defining the state of the PRG by the formula $u_{i+1} = f(u_i)$, where u_i is its state at the time moment i (therefore, the state at the time moment i is defined as an i-fold iteration of the function f of the initial state, i.e., $u_i = f^{(i)}(u_0)$);

*Electronic address: neex.emil@gmail.com

- an output function F that defines the output of the PRG at the time moment i as a function of its current state, i.e., $z_i = F(u_i)$;
- the initial state u_0 (in what follows we assume that it is chosen randomly).

In this paper we study the ability of certain functions f, namely, polynomials, to ensure the desired property of the sequence of internal states (in other words, the ability to play the role of the function f). We assume that calculations are performed modulo some number m. For the sake of uniformity or reasoning with various m, we consider the number u_i/m; evidently, it belongs to the interval from 0 to 1. In order to demonstrate that consequent values are «independent» of previous ones, we study the set formed by points, whose coordinates are equal to several successive values of u_i/m in a multidimensional unit hypercube.

With fixed m the number of points if finite and not greater than m, because the next state is uniquely defined by the previous one. Therefore, by tending m to infinity, one obtains the desired assertions for this case. Below, as a rule, m takes the form of p^n with some prime p and natural n.

It is well known that for polynomials of degree 1 the measure of the closure of the mentioned set equals 0, and with n tending to infinity all points belong to several hyperplanes [2, P. 117] inside the unit hypercube. In [4] one proves that the measure of the closure of the corresponding set equals either 0 or 1 for any compatible function f, in particular, for polynomials of any degree (see Theorem 1).

For practical applications, along with the unit measure of the closure (i.e., the fact that the s-dimensional cube is covered by the set under consideration), it is also important that the rate (with n tending to infinity), at which the cube is being covered by these points, should be the same at all regions of the cube. More formally, we say that *the projection of the function $f(x)$ is uniformly distributed in the s-dimensional cube*, if for each parallelepiped J inside the cube the ratio of the number of points in J to the total number of points with $n \to \infty$ equals the ratio of the s-dimensional volume of J to the total volume of the cube, i.e., to one. See [1],[6] for definitions of the uniformity for an arbitrary set of points.

In papers [7], [8], [9] one proves the uniformity of the corresponding sets for quadratic polynomials for the number of iterations of 2 and 3. Moreover, in the mentioned papers one obtains conditions under which the set of pairs of consecutive outputs of a quadratic generator almost satisfies the repeated logarithm law [3], namely, the principal term of the asymptotics of the discrepancy equals $m^{-1/2}$. In [5] these bounds are improved for the case of $m = 2^k$ and two iterations.

In this paper we prove the uniformity for an arbitrary polynomial of degree not less than 2 with integer coefficients and an arbitrary number of iterations with $m = p^n$, where n tends to infinity, and p is an arbitrary prime number. The proof is based on the following evident property: a sufficiently long random sequence necessarily contains any concrete subsequence; moreover, one can choose the length of the sequence so large as to make the probability of the opposite event very small. This fact is used in the induction step. Assuming the uniformity of the collection $(x, x^2, \ldots, x^{s-1})$, we fix certain subsequences in the number x so as to make the major digits of each function of the collection $(x, x^2, \ldots, x^s)$ modulo p^n easily predictable.

2 Basic notions

In this paper we apply techniques of the p-adic analysis for finding functions that can be used for constructing PRG; see, e.g., [10] for the necessary definitions. We use the definitions of the ring of integer p-adic numbers and the p-adic norm $\|\cdot\|_p$ and consider functions f from Z_p to Z_p. Recall [4] that a function from Z_p to Z_p is said to be compatible, if $\|f(x_1) - f(x_2)\|_p \leqslant \|x_1 - x_2\|_p$ for any $x_1, x_2 \in Z_p$. In other words, a function is compatible, if for each $x_1, x_2 \in Z_p$, for which the minor k digits in the p-adic notation coincide, the minor k digits in the p-adic notation of $f(x_1)$ and $f(x_2)$ also coincide.

For a compatible function $f(x)$ and a natural number $s \geqslant 2$ the set of points in the form

$$\left(\frac{x}{p^n}, \frac{f(x) \bmod p^n}{p^n}, \frac{f^{(2)}(x) \bmod p^n}{p^n}, \ldots, \frac{f^{(s-1)}(x) \bmod p^n}{p^n}\right)$$

exists for all $n \in \mathbb{N}, x \in \{0, 1, \ldots, p^n - 1\}$ (hereinafter the denotation $f^{(i)}(x)$ means the ith iteration of the function f). We call this set (note that we consider the union for all n) the s-dimensional projection of the compatible function f.

Consider a function f having a complete cycle and the corresponding sequence of states $u_i = f(u_{i-1})$. The set of points in the form

$$\left(\frac{u_i \bmod p^n}{p^n}, \frac{u_{i+1} \bmod p^n}{p^n}, \frac{u_{i+2}(x) \bmod p^n}{p^n}, \ldots, \frac{u_{i+s-1}(x) \bmod p^n}{p^n}\right)$$

coincides with the set described above, because by the definition of a complete cycle u_i runs over all values of x.

In this paper, instead of iterations of one function f, as a rule, we consider an arbitrary collection of compatible functions $f_1(x), f_2(x), \ldots, f_s(x)$. Let us generalize the definition of the projection for this case.

Let s compatible functions $f_1(x), f_2(x), \ldots, f_s(x)$ be given. We consider the set of points in the form

$$\left(\frac{f_1(x) \bmod p^n}{p^n}, \frac{f_2(x) \bmod p^n}{p^n}, \ldots, \frac{f_s(x) \bmod p^n}{p^n}\right)$$

for all $x \in \{0, 1, \ldots, p^n - 1\}$. For given $f_1, \ldots, f_s$ and fixed n we denote the multiset under consideration by $P_{f_1,\ldots,f_s}(n)$. We call the union of such sets for all n the *joint projection* of functions $f_1(x), f_2(x), \ldots, f_s(x)$.

In what follows we omit subscripts indicating collections of functions, if they are clear from the context.

In [4] one proves the following key theorem:

Theorem 1 (the 0-1 rule)**.** *For any compatible function f the measure of the closure of its two-dimensional projection equals either 0 or 1.*

One can easily generalize the mentioned theorem for the case of arbitrary s and an arbitrary collection of compatible functions $f_1, f_2, \ldots, f_s$.

Let us now give a more formal definition of the projection uniformity. Let J be some parallelepiped in the cube $[0, 1)^s$. Let $F_n(J)$ denote the ratio of the number of points that belong to $P_{f_1,\ldots f_s}(n)$ and lie in J to the total number of points p^n. Let $V(J)$ stand for the s-dimensional volume of J.

Definition 1. The joint projection of a collection of compatible functions $f_1, \ldots, f_s$ is said *to have a uniform distribution*, if

$$\lim_{n\to\infty} \sup_J |V(J) - F_n(J)| \to 0,$$

where the supremum is calculated over all possible parallelepipeds J.

In the case, when as a collection $f_1, \ldots, f_s$ one chooses the set of iterations of some compatible function f (i.e., the set $x, f(x), f^{(2)}(x), \ldots, f^{(s-1)}(x)$), we say that the *$s$-dimensional projection function f has a uniform distribution.*

Evidently, the uniformity of the projection implies that the measure of the closure equals 1. In this paper we study the uniformity of projections of polynomial functions f.

Considering the supremum for concrete n, we obtain the discrepancy D_{p^n}. Instead of estimating this value, it is more convenient to study the lower bound for the digit capacity, beginning with which the bound for the uniformity of the considered set of points is guaranteed. In this paper we use various definitions of the uniformity (measurable in terms of various errors ε); as a result, they become connected with each other and form an upper bound for the discrepancy.

Let us give several more definitions and denotations which are necessary, in particular, for studying the rate of convergence to 0 in Definition 1.

The uniformity of the projection of a collection of compatible functions means that for any positive ε there exists $N^{f_1,\dots,f_s}(\varepsilon)$ such that for any $n > N^{f_1,\dots,f_s}(\varepsilon)$ it holds $|F_n(J) - V(J)| < \varepsilon$.

In what follows, when using the denotation $N^{f_1,f_2,\dots,f_s}(k,\varepsilon) = g(k,\varepsilon)$, we take into account the fact that this function g satisfies conditions stated in the previous definition, but the minimum of the estimate is not guaranteed.

Let k be some fixed number, $a_1, a_2, \dots, a_s \in \{0, 1, \dots, p^k - 1\}$. Denote by $J_k(a_1, a_2, \dots, a_s)$ the hypercube in $[0,1)^s$ defined by inequalities

$$\begin{aligned} \frac{a_1}{p^k} &\leqslant z_1 < \frac{a_1+1}{p^k} \\ \frac{a_2}{p^k} &\leqslant z_2 < \frac{a_2+1}{p^k} \\ &\dots \\ \frac{a_s}{p^k} &\leqslant z_s < \frac{a_s+1}{p^k}, \end{aligned}$$

where $(z_1, z_2, \dots, z_s)$ are coordinates of a point from $[0,1)^s$.

Let us slightly modify Definition 1 (cf. [1]; the equivalence of definitions 1 and 2 is proved in Theorem 2). Namely,

Definition 2. The joint projection is called *uniformly distributed*, if for any number $\varepsilon > 0$ and for any natural k there exists natural $N_0^{f_1,\dots,f_s}(k,\varepsilon)$ such that for each $n > N_0^{f_1,\dots,f_s}(k,\varepsilon)$ and for all $a_1, a_2, \dots, a_s$ such that $a_1, a_2, \dots, a_s \in \{0, 1, \dots, p^k - 1\}$ it holds

$$\left| \frac{F_n(J_k(a_1, a_2, \dots, a_s))}{V(J_k(a_1, a_2, \dots, a_s))} - 1 \right| \leqslant \varepsilon,$$

where $V(J_k(a_1, a_2, \dots, a_s)) = p^{-sk}$ is the s-dimensional volume of the mentioned parallelepiped.

We omit parameters in denotations $N_0^{f_1,\dots,f_s}(k,\varepsilon)$, if they are clear from the context.

Analogously to the case of $N^{f_1,\dots,f_s}(k,\varepsilon)$, using the denotation $N_0^{f_1,\dots,f_s}(k,\varepsilon) = g(k,\varepsilon)$, we mean that the given function g satisfies conditions imposed on it in Definition 2, but the minimum of the estimate is not guaranteed.

3 The d-uniformity

In essence, the error mentioned in Definition 1 is absolute for any parallelepiped, while that in Definition 2 is relative; it is calculated only for lattice hypercubes. Since the

lattice step can be chosen arbitrarily, one can approximate any parallelepiped by lattice hypercubes; this property implies the following assertion.

Theorem 2. *For a collection of compatible functions $f_1, f_2, \ldots, f_s$ Definition 1 is equivalent to Definition 2, and $N(\varepsilon) = N_0(k, \varepsilon')$, where $k = -\log_p(\varepsilon/4s), \varepsilon' = 1/2\varepsilon$.*

Proof. Let conditions of Definition 2 be fulfilled. Let us prove that

$$\forall \varepsilon > 0 : \exists N(\varepsilon) \forall n > N, \forall J : |V(J) - F_n(J)| < \varepsilon.$$

Choose $k = -\log_p(\varepsilon/4s), \varepsilon' = 1/2\varepsilon$. Let us prove that the number $N = N_0(k, \varepsilon')$ is the desired one.

Let J be some parallelepiped in $[0,1)^s$. We denote by J_k^+ the union of hypercubes in the form $J_k(a_1, \ldots, a_s)$ which have at least one common point with J and we do by J_k^- the union of hypercubes which entirely lie inside J.

Evidently, J_k^+ forms a parallelepiped and so does J_k^-.

Note that $0 \leqslant V(J_k^+) - V(J_k^-) \leqslant \varepsilon/2$. Really, in each of s measurements there exist no more than two «layers» of the lattice that lie in J_k^+, but do not lie in J_k^-. The volume of each of them does not exceed $1/p^k$. Therefore, the total difference does not exceed $2s/p^k = \varepsilon/2$.

Let us now write the condition of Definition 2 in the form

$$V(J_k(a_1, \ldots, a_s))(1 - \varepsilon') \leqslant F_n(J_k(a_1, \ldots, a_s)) \leqslant V(J_k(a_1, \ldots, a_s))(1 + \varepsilon')$$

and calculate the sum for each of sets J_k^+, J_k^-. We obtain

$$V(J_k^+)(1 - \varepsilon') \leqslant F_n(J_k^+) \leqslant V(J_k^+)(1 + \varepsilon')$$

$$V(J_k^-)(1 - \varepsilon') \leqslant F_n(J_k^-) \leqslant V(J_k^-)(1 + \varepsilon').$$

It is also evident that $V(J_k^-) \leqslant V(J) \leqslant V(J_k^+)$. In addition, $F_n(J_k^-) \leqslant F(J) \leqslant F_n(J_k^+)$, because these values are proportional to the number of points of the projection that lie inside the corresponding parallelepiped. Then we write

$$F_n(J) - V(J) \leqslant F_n(J_k^+) - V(J_k^-) \leqslant V(J_k^+)(1 + \varepsilon') - V(J_k^-) \leqslant V(J_k^+)\varepsilon' + \varepsilon/2.$$

Since J_k^+ lies inside the unit cube, we have $V(J_k^+) \leqslant 1$, and this means that the latter expression does not exceed ε (because $\varepsilon' = \varepsilon/2$). Analogously,

$$F_n(J) - V(J) \geqslant F_n(J_k^-) - V(J_k^+) \geqslant V(J_k^-)(1 - \varepsilon') - V(J_k^+) \geqslant -V(J_k^-)\varepsilon' - \varepsilon/2 \geqslant -\varepsilon.$$

Therefore, we have obtained the desired inequality

$$|F_n(J) - V(J)| \leqslant \varepsilon$$

for an arbitrary parallelepiped J.

The proof of the converse assertion is performed with the help of an analogous estimation. □

Let us strengthen Definition 2, fixing the residue x of the division by p^d for natural d. Let $d \in \mathbb{N}, \beta \in \{0, 1, \ldots, p^d - 1\}$. Denote by $P(n, d, \beta), n \geqslant d$ the multiset of points

$$\left(\frac{f_1(x) \bmod p^n}{p^n}, \frac{f_2(x) \bmod p^n}{p^n}, \ldots, \frac{f_s(x) \bmod p^n}{p^n} \right)$$

for all $x \in \{0, 1, \ldots, p^n - 1\}, x \bmod p^d = \beta$. Let $F_n^{d,\beta}(J)$ be the ratio of the number of points from $P(n, d, \beta)$ that lie in J to the cardinal number of $P(n, d, \beta)$, i.e., to p^{n-d}.

Definition 3. The joint projection of compatible functions $f_1, \ldots, f_s$ is said to be *d-uniformly distributed*, if for any number $\varepsilon > 0$ and for any natural k, d there exists natural $N = N_d^{f_1,\ldots,f_s}(k, \varepsilon)$ such that for each $n > N$, for any $\beta \in \{0, 1, \ldots, p^d - 1\}$, and for all $a_1, a_2, \ldots, a_s \in \{0, 1, \ldots, p^k - 1\}$ it holds

$$\left| \frac{F_n^{d,\beta}(J_k(a_1, a_2, \ldots, a_s))}{V(J_k(a_1, a_2, \ldots, a_s))} - 1 \right| \leqslant \varepsilon.$$

In other words, the d-uniformity is the uniformity in each p-adic ball, whose volume equals p^d.

For $N_d^{f_1,\ldots,f_s}(k, \varepsilon)$ we use assumptions analogous to above ones for N and N_0 (see the end part of Section 2).

Note that the number N_d indicated in the definition is independent of β; it depends only on its p-adic length, i.e., on d. This condition does not strengthen the definition. Really, since for fixed d the number of possible values of β is finite, one could have chosen N_d as the maximum of the corresponding numbers for each β. Nevertheless, it is more convenient to use just this statement, i.e., the uniformity with respect to β.

Evidently, the d-uniformity implies the uniformity in the sense of Definition 2, namely, it suffices to put $d = 0$. In what follows, when speaking of the uniformity, we mean the d-uniformity, if this leads to no ambiguity.

Let $n \in \mathbb{N}, n \geqslant k, x_1, x_2, \ldots, x_s \in \{0, 1, \ldots, p^n - 1\}$. Note that the point $\left(\frac{x_1}{p^n}, \frac{x_2}{p^n}, \ldots, \frac{x_s}{p^n} \right)$ belongs to $J_k(a_1, a_2, \ldots, a_s)$ if and only if the prefix of the length k in the p-adic notation of x_i coincides with a_i for all $i, 1 \leqslant i \leqslant s$ (here we assume that the

p-adic notation of x_i consists of exactly n digits, while the p-adic notation of a_i consists of exactly k digits independently of the presence of leading zeros).

One can also easily see that the condition $x \bmod p^d = \beta$ is equivalent to the fact that the latter d p-adic digits of x contain the notation of β.

4 The coin toss

In this section we prove some corollaries of the d-uniformity which we need in the induction step in the proof of the main theorem.

Let $d, r \in \mathbb{N}, d < r, \beta \in \{0, 1, \ldots, p^d - 1\}$. Denote by $\Omega(r, d, \beta)$ the set of all $x \in \{0, 1, \ldots, p^r - 1\}$ such that $x \bmod p^d = \beta$.

Speaking informally, the d-uniformity of the joint projection of the collection $f_1(x), f_2(x), \ldots, f_s(x)$ means that with fixed d, β and *fixed* sufficiently large r, under the equiprobable choice of x from $\Omega(r, d, \beta)$, the probability that the point

$$\left(\frac{f_1(x) \bmod p^r}{p^r}, \frac{f_2(x) \bmod p^r}{p^r}, \ldots, \frac{f_s(x) \bmod p^r}{p^r}\right)$$

belongs to $J_k(a_1, a_2, \ldots, a_s)$ equals approximately $V(J_k(a_1, a_2, \ldots, a_s))$. In the following lemma we prove that if for x we choose a sufficiently long string, then the probability that this event takes place *with at least one* r can be arbitrarily close to 1.

More formally, let $k \in \mathbb{N}, a_1, a_2, \ldots, a_s \in \{0, 1, \ldots, p^k - 1\}$ be given. Fix $n \in \mathbb{N}, n \geqslant d, n \geqslant k$. We say that x is *suitable*, if there exists $r \in \mathbb{N}, d + k \leqslant r \leqslant n$ such that

$$\left(\frac{f_1(x) \bmod p^r}{p^r}, \frac{f_2(x) \bmod p^r}{p^r}, \ldots, \frac{f_s(x) \bmod p^r}{p^r}\right) \in J_k(a_1, a_2, \ldots, a_s).$$

Lemma 1. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a d-uniform distribution, a value $\varepsilon > 0$ and numbers $k, d \in \mathbb{N}$ are given. Then there exists $L = L_{f_1,\ldots,f_s}(k, \varepsilon, d)$ such that for any $n > L$ and any $\beta \in \{0, 1, \ldots, p^d - 1\}$, $a_1, a_2, \ldots, a_s \in \{0, 1, \ldots, p^k - 1\}$ the ratio of the number of suitable x to $|\Omega(n, d, \beta)|$ is at least $1 - \varepsilon$.*

Proof. The proof of the lemma is based on a simple idea. Let us have a biased coin such that the probability of the head is bounded from below by some nonzero constant. Then by tossing the coin sufficiently many times one can make the probability of getting at least one head arbitrarily close to 1. One «coin toss» consists in obtaining a new value of n, namely, $N_d(k, \varepsilon)$, where d is the previous value of n. The independence of coin «tosses» is guaranteed by the presence of parameters d, β, and the boundedness from below of the

probability of the head is provided by the d-uniformity of the collection $f_1, \ldots, f_s$. Just in this lemma and in the next one we need Definition 3 that strengthens Definition 2.

Put $L^{(0)} = d$. Construct a sequence $L^{(i)}, i > 0$, as follows: let $L^{(i)}$ be equal to $N^{f_1,\ldots,f_s}_{L^{(i-1)}+k}(k, 1/2)$. Let γ_i be the ratio of the number of unsuitable x to $|\Omega(L^{(i)}, d, \beta)|$. Evidently, $\gamma_0 \leqslant 1$. Let us estimate γ_i. The definition of the uniformity and the definition of $L^{(i)}$ imply that $F^{L^{(i-1)},\beta}_{L^{(i)}}(J_k(a_1, a_2, \ldots, a_s)) \geqslant V(J_k(a_1, a_2, \ldots, a_s))/2 = \frac{1}{2p^{sk}}$ for any $\beta : 0 \leqslant \beta \leqslant p^{L^{(i-1)}} - 1$. Denote the latter number by ε' (it corresponds to the probability of getting the head in one toss). Therefore, for each $\beta \in \{0, 1, \ldots, p^{L^{(i-1)}} - 1\}$ there exists at least $\varepsilon' p^{L^{(i)} - L^{(i-1)}}$ ways to fill $L^{(i)} - L^{(i-1)}$ major positions so as to make obtained x suitable for $n = L^{(i)}$ (independently of the content of $L^{(i-1)}$ latter positions). This means that the ratio of the number of ways to fill these positions making x unsuitable does not exceed $1 - \varepsilon'$. Evidently, if x is unsuitable for $n = L^{(i)}$, then it is also unsuitable for all lesser n, in particular, for $n = L^{(i-1)}$. The number of ways to fill the latter $L^{(i-1)}$ positions making x unsuitable for $n = L^{(i-1)}$ by definition equals γ_{i-1}. Therefore, the combined share $\gamma_i \leqslant (1 - \varepsilon')\gamma_{i-1}$, because in order to make x unsuitable, one has to fill the minor $L^{(i-1)}$ positions in any of $\gamma_{i-1} p^{L^{(i-1)}}$ ways; for each of them there exists no more than $(1 - \varepsilon')p^{L^{(i)} - L^{(i-1)}}$ ways to fill the major $L^{(i)} - L^{(i-1)}$ positions. Since $\gamma_0 \leqslant 1$, we obtain $\gamma_i \leqslant (1 - \varepsilon')^i$. The latter expression is a geometric progression with the ratio $1 - \varepsilon' < 1$, which means that $\gamma_i < \varepsilon$ with $i > \log_{1-\varepsilon'} \varepsilon$. The corresponding number $L^{(i)}$ is the desired value of L, because, evidently, the ratio of suitable x does not decrease with the growth of n. □

For $L_{f_1,\ldots,f_s}(k, \varepsilon, d)$ we also use conditions analogous to those described earlier for N and N_0 (see the end part of Section 1).

Note that the proof of the lemma also allows us to calculate $L_{f_1,\ldots,f_s}(k, \varepsilon, d)$. It suffices to construct the sequence $L^{(0)} = d$, $L^{(i)} = N^{f_1,\ldots,f_s}_{L^{(i-1)}+k}(k, 1/2), i > 0$ and to put $L_{f_1,\ldots,f_s}(k, \varepsilon, d) = L^{(\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil)}$.

Let us generalize the latter lemma for the case of several collections a_i. The previous lemma guarantees that one can «truncate» a sufficiently long sequence x (i.e., calculate modulo p^r) so as to make the major k positions of $f_i(x) \bmod p^r$ coincide with some arbitrary fixed collection a_i. Now we are going to prove that even if we have m collections $a^{(j)}_i \in \{0, 1, \ldots, p^k - 1\}, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant m$, then for each collection of numbers there exists its own $r^{(j)}$, i.e., the way to «truncate» x and $f_i(x)$ so as to make the major k positions among $r^{(j)}$ positions of the number $f_i(x)$ form the number $a^{(j)}_i$. In addition, we want distinct $r^{(j)}$ to be not too close, therefore we additionally impose the condition $r^{(j)} - r^{(j-1)} > \Delta$ with some fixed natural Δ.

Let $k, d, \Delta \in \mathbb{N}$ be given. Assume also that natural m is given, as well as m collections of s numbers such that for each j, where $1 \leqslant j \leqslant m$, the collection of numbers $a_i^{(j)} \in \{0, 1, \ldots, p^k - 1\}, 1 \leqslant i \leqslant s$, is defined. We say that $x \in \{0, 1, \ldots, p^n - 1\}$ is *concurrently suitable*, if the following conditions are fulfilled:

- x is suitable for $k, d, a_i = a_i^{(j)}$ for each fixed j. We denote the corresponding numbers r by $r^{(j)}$.
- $r^{(j)} > r^{(j-1)} + k + \Delta$ for $1 < j \leqslant m$.

The parameter Δ has the following sense: it is necessary that neighboring segments of positions corresponding to degrees of p, whose values vary from $r^{(j)} - k$ to $r^{(j)} - 1$, should not be too close; namely, we require that their difference should exceed some fixed Δ.

Lemma 2. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a d-uniform distribution, and numbers $\varepsilon > 0$ and $k, d, \Delta, m \in \mathbb{N}$ are given. Then there exists $\widetilde{L} = \widetilde{L}_{f_1,\ldots,f_s}(k, \varepsilon, d, \Delta, m)$ such that for any $n > \widetilde{L}$, any $\beta \in \{0, 1, \ldots, p^d - 1\}$, and any m collections of s numbers $a_i^{(j)} \in \{0, 1, \ldots, p^k - 1\}, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant m$, the ratio of the number of x, which are concurrently suitable for $a_i^{(j)}$, to $|\Omega(n, d, \beta)|$ is at least $1 - \varepsilon$.*

Proof. Put $\varepsilon'' = 1 - \sqrt[m]{1 - \varepsilon}$. Let $\widetilde{L}^{(0)} = d$. Construct a sequence $\widetilde{L}^{(1)}, \widetilde{L}^{(2)}, \ldots, \widetilde{L}^{(s)}$ as follows: $\widetilde{L}^{(j)}$ equals $L_{f_1,\ldots,f_s}(k, \varepsilon, \widetilde{L}^{(j-1)} + \Delta)$ which was obtained in accordance with Lemma 1. Let $\gamma^{(j)}$ be the ratio of admissible x for $n = \widetilde{L}^{(j)}$ which are concurrently suitable for $m = j$ and for j first collections a_i (i.e., for which there exist $r^{(1)}, r^{(2)}, \ldots, r^{(j)}$ satisfying the above correlations). Then, taking into account the definition of $\widetilde{L}^{(i)}$, we conclude that $\gamma^{(j)} \geqslant \gamma^{(j-1)}(1 - \varepsilon'')$. Hence and from the fact that $\gamma^{(0)} = 1$ (since for $j = 1$ no conditions are imposed on x, except its belonging to $\Omega(n, d, \beta)$) it follows that $\gamma^{(m)} \geqslant (1 - \varepsilon')^m = 1 - \varepsilon$, which means that $\widetilde{L} = \widetilde{L}^{(m)}$ is the desired value. □

For $\widetilde{L}_{f_1,\ldots,f_s}(k, \varepsilon, d, \Delta, m)$ we also make assumptions analogous to those described above for N and N_0 (see the end part of Section 1).

The proof of Lemma 2 also allows us to calculate $\widetilde{L}_{f_1,\ldots,f_s}(k, \varepsilon, d, \Delta, m)$. It suffices to construct the sequence $\widetilde{L}^{(0)} = d$, $\widetilde{L}^{(j)} = L_{f_1,\ldots,f_s}(k, \varepsilon, \widetilde{L}^{(j-1)} + \Delta)$ with $j > 0$ and to put $\widetilde{L}_{f_1,\ldots,f_s}(k, \varepsilon, d, \Delta, m) = \widetilde{L}^{(m)}$.

5 Game protocols for the uniformity

For proving the uniformity of joint projections of monomials we need to simplify and to formalize the proof of the uniformity. Let us describe a certain game protocol. Players

choose in turns values of certain variables. The variables, whose values are being chosen by us, are preceded by the existential quantifier, while those, whose values are being chosen by our competitor, are preceded by the generality quantifier.

Let compatible functions $f_1(x), f_2(x), \ldots, f_s(x)$ be given. Consider the following game of two players, Good and Evil. The game has the following scheme:

1. Evil chooses numbers $k, d \in \mathbb{N}$ and $\varepsilon_1, \varepsilon_2 > 0$.

2. Good chooses the number $\widetilde{N} = \widetilde{N}_d^{f_1,\ldots,f_s}(k, \varepsilon_1, \varepsilon_2) \in \mathbb{N}$.

3. Evil chooses numbers $n > \widetilde{N}, \beta \in \{0, 1, \ldots, p^d - 1\}$ and draws on a board n successive empty cells (positions); in what follows we fill each of them with a number ranging from 0 to $p-1$. We immediately fill the latter d cells with the notation of the number β.

4. Good chooses an arbitrary set of empty positions and describes some set of admissible ways to fill these positions. The ratio of the cardinal number of the latter set to the total number of ways to fill the chosen positions should be not less than $1-\varepsilon_1$. In other words, if Good has chosen l positions, then the number of admissible variants should be at least $(1-\varepsilon_1)p^l$.

5. Evil fills positions chosen at the previous step in one of admissible ways.

6. Good colors an arbitrary set of empty positions. Let their number equal m.

7. Evil absolutely arbitrarily fills all empty uncolored positions and chooses $a_1, a_2, \ldots, a_s \in \{0, 1, \ldots, p^k - 1\}$.

8. Good describes $(1-\varepsilon_2)p^{m-sk}$ ways to fill colored positions so that for the number $x \in \{0, 1, \ldots, p^n - 1\}$, whose p-adic notation is written on the board, the point

$$\left(\frac{f_1(x) \bmod p^n}{p^n}, \frac{f_2(x) \bmod p^n}{p^n}, \frac{f_3(x) \bmod p^n}{p^n}, \ldots, \frac{f_s(x) \bmod p^n}{p^n}\right)$$

should belong to $J_k(a_1, a_2, \ldots, a_s)$. If Good succeeds in doing this, it is said to be the winner, otherwise Evil becomes the winner.

Along with the above requirements, the strategy of Good should be determinate. This means that if there are two variants of the behavior of Evil such that the latter performs the same actions on several first steps of the game, Good also must perform the same actions till Evil first behaves differently.

Note that on Step 6 Good could have always colored all positions and then could have described the necessary number of ways to fill them, while Good could have independently considered all possible variants of filling positions whose coloring would not be necessary. Nevertheless, for structuring the proof, it is convenient to «separate roles» as was described on steps 6-7.

For $\widetilde{N}_d^{f_1,\dots,f_s}(k,\varepsilon_1,\varepsilon_2) \in \mathbb{N}$ we make assumptions analogous to those described earlier for N and N_0 (see the end part of Section 1).

Lemma 3. *If Good always wins in the described game, then the joint projection of $f_1,\dots,f_s$ has a uniform distribution, while $N_d(k,\varepsilon) = \widetilde{N}_d(k,\varepsilon',\varepsilon')$, where $\varepsilon' = \varepsilon/(2p^{sk})$.*

Proof. Denote

$$\tilde{F}_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s)) = F_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s))p^{n-d}.$$

Therefore, $\tilde{F}_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s)$ is the number of points from $P_n^{d,\beta}$ that belong to $J_k(a_1,a_2,\dots,a_s)$.

Let $k,d,a_1,a_2,\dots,a_s$ be fixed. Rewrite the condition

$$\left|\frac{F_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s))}{V(J_k(a_1,a_2,\dots,a_s))} - 1\right| \leqslant \varepsilon$$

as

$$(1-\varepsilon)p^{-sk} \leqslant F_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s)) \leqslant (1+\varepsilon)p^{-sk}$$

or, alternately,

$$(1-\varepsilon)p^{n-d-sk} \leqslant \tilde{F}_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s)) \leqslant (1+\varepsilon)p^{n-d-sk}.$$

Fix some admissible way to fill l positions chosen on Step 4. Calculating the sum of all possible ways to fill $n-l-d-m$ uncolored positions on Step 7, we obtain that the quantity of values of x, for which the corresponding points belong to $J_k(a_1,a_2,\dots,a_s)$, is no less than $p^{n-l-d-m}\cdot(1-\varepsilon_2)p^{m-sk} = (1-\varepsilon_2)p^{n-l-d-sk}$. Now by summing this value over all admissible ways to fill l positions chosen on Step 4, we obtain that their amount is no less than $(1-\varepsilon_1)p^l$. This means that there exist at least $(1-\varepsilon_1)(1-\varepsilon_2)p^{n-d-sk}$ values of x, each of which satisfies conditions described on Step 8. The fulfillment of these conditions means that a point belongs to $J_k(a_1,a_2,\dots,a_s)$, which gives the inequality

$$(1-\varepsilon_1)(1-\varepsilon_2)p^{n-d-sk} \leqslant \tilde{F}_n^{d,\beta}(J_k(a_1,a_2,\dots,a_s))$$

Let us now prove the upper bound. Evidently, a point cannot concurrently belong to $J_k(a_1, a_2, \ldots, a_s)$ and to $J_k(a'_1, a'_2, \ldots, a'_s)$ with $(a_1, a_2, \ldots, a_s) \neq (a'_1, a'_2, \ldots, a'_s)$. Therefore,

$$\tilde{F}_n^{d,\beta}(J_k(a_1, a_2, \ldots, a_s)) \leqslant p^{n-d} - \sum_{(a'_1,\ldots,a'_s):(a'_i)\neq(a_i)} \tilde{F}_n^{d,\beta}(J_k(a'_1, a'_2, \ldots, a'_s)) \leqslant$$

$$\leqslant p^{n-d} - (p^{sk} - 1)(1 - \varepsilon_1)(1 - \varepsilon_2)p^{n-d-sk} =$$

$$= (1 - (1 - \varepsilon_1)(1 - \varepsilon_2))p^{n-d} + (1 - \varepsilon_1)(1 - \varepsilon_2)p^{n-d-sk} \leqslant$$

$$\leqslant (\varepsilon_1 + \varepsilon_2)p^{n-d} + p^{n-d-sk}$$

Put $\varepsilon_1 = \varepsilon_2 = \min(1 - \sqrt{1 - \varepsilon}, \varepsilon/2p^{sk})$. Then we get

$$(1 - \varepsilon_1)(1 - \varepsilon_2)p^{n-d-sk} \geqslant (1 - \varepsilon)p^{n-d-sk},$$

and

$$(\varepsilon_1 + \varepsilon_2)p^{n-d} + p^{n-d-sk} \leqslant (1 + \varepsilon)p^{n-d-sk}.$$

This means that inequalities

$$(1 - \varepsilon_1)(1 - \varepsilon_2)p^{n-d-sk} \leqslant \tilde{F}_n^{d,\beta}(J_k(a_1, a_2, \ldots, a_s)),$$

which were obtained above, and

$$\tilde{F}_n^{d,\beta}(J_k(a_1, a_2, \ldots, a_s)) \leqslant (\varepsilon_1 + \varepsilon_2)p^{n-d} + p^{n-d-sk}$$

lead to the desired correlations

$$(1 - \varepsilon)p^{n-d-sk} \leqslant \tilde{F}_n^{d,\beta}(J_k(a_1, a_2, \ldots, a_s)) \leqslant (1 + \varepsilon)p^{n-d-sk}.$$

Note that $1 - \sqrt{1 - \varepsilon} > \varepsilon/2$ with $\varepsilon > 0$. Therefore, with $s, k \in \mathbb{N}, p \geqslant 2$ it holds $\min(1 - \sqrt{1 - \varepsilon}, \varepsilon/(2p^{sk})) = \varepsilon/(2p^{sk})$, which means that in accordance with the said above, $N_d(k, \varepsilon) = \widetilde{N}_d(k, \varepsilon/(2p^{sk}), \varepsilon/(2p^{sk}))$. □

Consider the following modification of the game described above:

0. Good fixes some natural constant $c_0 = c_0^{f_1,\ldots,f_s}$.

1. Evil fixes $k, d \in \mathbb{N}$ and $\varepsilon_1 > 0$.

2. Good chooses the number $\widehat{N} = \widehat{N}_d^{f_1,\ldots,f_s}(k, \varepsilon_1)$.

3. Evil chooses numbers $n > \widehat{N}, \beta \in \{0, 1, \ldots, p^d - 1\}$ and draws on a board n sequential empty cells-positions, each of which in what follows will be filled with a number from 0 to $p-1$. The latter d cells are immediately filled with the notation of the number β.

4. Good chooses an arbitrary set of empty positions and defines some set of admissible ways to fill these positions. The ratio of the cardinal number of the latter set to the total number of ways to fill the chosen positions should be at least $1 - \varepsilon_1$.

5. Evil fills positions chosen on the previous step in one of admissible ways.

6. Good colors an arbitrary set of positions which are not filled yet. Denote their number by m.

7. Evil absolutely arbitrarily fills all empty positions except colored ones and chooses $a_1, a_2, \ldots, a_s \in \{0, 1, \ldots, p^k - 1\}$.

8. Good defines p^{m-sk} ways to fill colored positions so as to satisfy the following condition. Denote by $x \in \{0, 1, \ldots, p^n - 1\}$ the number, whose p-adic notation will be written on the board; $x_1 = f_1(x) \bmod p^n, x_2 = f_2(x) \bmod p^n, \ldots, x_n = f_n(x) \bmod p^n$. Denote by b_i numbers, whose p-adic notation is the prefix of the length k of the row consisting of n symbols of the p-adic notation of x_i (i.e., $b_i = \lfloor x_i / p^{n-k} \rfloor$). Require that b_i should differ from a_i no more than by c_0 (hereinafter in the condition «differ no more than by c_0» imposed on p-adic numbers of the length k, the difference is understood as the minimum of two differences calculated modulo p^k; in other words, 0 and $p^k - 1$ are treated as different by 1). In the case, when Good can define p^{m-sk} ways to fill the colored positions, each of which satisfies the above requirement, Good is said to be the winner, otherwise Evil is said to win.

   Let us impose one additional requirement to the techniques proposed by Good; namely, for two distinct collections $a_1, a_2, \ldots, a_s$, assuming that the rest actions of Evil are the same, sets of techniques proposed by Good should be non-intersecting.

As above, the strategy of Good is assumed to be determinate.

For $\widehat{N}_d^{f_1,\ldots,f_s}(k, \varepsilon_1)$ we make assumptions analogous to those made above for N and N_0 (see the end part of Section 1).

Lemma 4. *In the case, when Good always wins in the modified game, it can also be the winner in the initial game, and* $\widetilde{N}_d(k, \varepsilon_1, \varepsilon_2) = \widehat{N}_d(k_2, \varepsilon_1)$, *where* $k_2 = k + \log_p \frac{2sc_0^{f_1,\ldots,f_s}}{\varepsilon_2}$.

Proof. Let us apply Lemma 3. Assume that there exists an oracle that implements a winning strategy for Good in the modified game. Let us describe the strategy for a mediator that uses this oracle, which is winning for the non-modified game.

Assume that on the first step the oracle gives a number c_0. After obtaining k the mediator calculates $k_2 = k + \log_p \frac{2sc_0}{\varepsilon_2}$. Note that

$$\frac{(p^{k_2-k} - 2c_0)^s}{p^{(k_2-k)s}} \geqslant (1 - \varepsilon_2).$$

Really, for $0 < \varepsilon_2 < 1$ we have

$$(1 - \varepsilon_2)^{1/s} \leqslant 1 - \frac{\varepsilon_2}{s},$$

therefore with $k_2 = k - \log_p \frac{\varepsilon_2}{2sc_0}$ it holds

$$\left(\frac{p^{k_2-k} - 2c_0}{p^{k_2-k}}\right)^s = \left(1 - \frac{2c_0}{p^{k_2-k}}\right)^s = \left(1 - \frac{\varepsilon_2}{s}\right)^s \geqslant 1 - \varepsilon_2.$$

Furthermore, the mediator will concurrently use $(p^{k_2-k} - 2c_0)^s$ oracles which implement the winning strategy for the modified game. On steps 1-6 he sends the data obtained from oracles to Evil and does the data given by Evil to oracles unchanged, except the fact that on Step 1 he sends to the oracles k_2 instead of k. Since the oracles are determinate, the data produced by them coincide. Having obtained on Step 7 numbers $a_1, a_2, \ldots, a_s$, the mediator use them to form collections $a_1 p^{k_2-k} + b_1, a_2 p^{k_2-k} + b_2, \ldots, a_s p^{k_2-k} + b_s$ for all possible combinations of $b_i \in \{c_0, c_0 + 1, \ldots, p^{k_2-k} - c_0 - 1\}$. Therefore he gets $(p^{k_2-k} - 2c_0)^s$ collections of numbers, each of which belongs to $\{0, 1, \ldots, p^{k_2} - 1\}$. Then he sends these collections to the oracles as $a_1, a_2, \ldots, a_s$. One can easily see that if any of the sent numbers varies no more than by c_0, then their first k digits remain equal initial $a_1, a_2, \ldots, a_s$. Therefore, the techniques for filling m colored positions defined by oracles satisfy requirements imposed on Step 8 of the non-modified game. Each oracle defines $p^{m-k_2 s}$ techniques, therefore, their total number is $p^{m-k_2 s}(p^{k_2-k} - 2c_0)^s$. The additional requirement described on Step 8 guarantees that no technique is counted twice. The inequality

$$\frac{p^{m-k_2 s}(p^{k_2-k} - 2c_0)^s}{p^{m-ks}} \geqslant \frac{p^{m-k_2 s}(1 - \varepsilon_2)(p^{k_2-k})^s}{p^{m-ks}} = 1 - \varepsilon_2$$

completes the proof of the lemma. □

6 The uniformity of the joint projection of monomials

Let us first prove one simple assertion which will allow us to restrict the variation of major positions under the linear combination of several numbers. Here the deviation is

understood as the minimum of two differences modulo p^k, i.e., 0 and p^k-1 are considered to differ by 1.

Lemma 5. *Fix a natural number m and a collection of integer numbers $a_i, 1 \leqslant i \leqslant m$. Put $c_0 = |a_1| + |a_2| + \ldots + |a_m|$. Then for any natural $n, k : n \geqslant k$ and for any $x_1, x_2, \ldots, x_m \in \{0, 1, \ldots, p^n - 1\}$ the number, whose p-adic notation is formed by the first k digits in the n-digit notation of the number $(a_1x_1 + a_2x_2 + \ldots + a_mx_m) \bmod p^n$, differs from the number $(a_1y_1 + a_2y_2 + \ldots + a_my_m) \bmod p^k$ (here y_i is the number, whose p-adic notation is formed by the first k digits in the n-digit p-adic notation of x_i) no more than by c_0.*

Proof. Let us first note that for any $k, n, k \leqslant n$ and any $x, y \in \{0, 1, \ldots, p^n-1\}$ the number formed by the first k digits of $x+y$ differs from the sum modulo p^k of numbers formed by the k first digits of x, y no more than by 1. This property follows from the procedure of addition of numbers in a column; namely, the value that is moved to the major k positions in the summation process, does not exceed 1. An analogous correlation is valid for the difference $x - y$ and the difference of their k major positions, because the borrow in the subtraction procedure does not exceed 1. After establishing these two facts, one can easily obtain the desired assertion by induction with respect to $|a_1| + |a_2| + \ldots + |a_m|$. □

In other words, Lemma 5 asserts that if we calculate a linear combination of several numbers and then choose the k major positions among n ones, we will deviate at most by c_0 from the result obtain by performing these operations in the converse order, i.e., if we first truncate the minor $n - k$ positions and then calculate the linear combination.

Let us now prove the key theorem of this paper.

Theorem 3. *Let $s \in \mathbb{N}$. The joint projection of the collection $f_1(x) = x$, $f_2(x) = x^2, \ldots, f_s(x) = x^s$ has a d-uniform distribution, and*

$$\begin{aligned} \widehat{N}_d^x(k, \varepsilon_1) &= k + d \\ \widehat{N}_d^{x,x^2,\ldots,x^s}(k, \varepsilon_1) &= \widehat{L}_{x,x^2,\ldots,x^{s-1}}(2k + \lceil \log_p s \rceil, \varepsilon_1, d, \lceil \log_p s \rceil, s-1) \text{ with } s > 1 \\ c_0^{x,\ldots,x^s} &= s^2. \end{aligned}$$

Proof. Let us prove the theorem by induction. The induction base for $s = 1$ is evident, namely, the condition that $\frac{x}{p^n}$ should belong to the semiinterval $J_k(a_1)$ is equivalent to the corresponding choice of k major digits of x; therefore, the desired correlation is valid for any $\varepsilon \geqslant 0$ (and $n \geqslant d + k = \widehat{N}_d$).

Denote by $\mathrm{ord}_p i$ the maximal degree of p, which is a divisor of i, $\theta(i) = i/p^{\mathrm{ord}_p i}$.

Now let the joint projection $x, x^2, \ldots, x^{s-1}$ have a uniform distribution. Let us prove a uniform distribution of the joint projection $x, x^2, \ldots, x^s$. According to Lemma 4, to this end it suffices to define the corresponding move of Good on each even step of the modified game.

The proof is based on the following idea: we obtain the necessary major digits of monomials $x, \ldots, x^s$, changing the certain collection of positions in the major half of x (to this end, we color them on Step 6 of the modified game). The minor half will be composed so as to make the dependence of the major k positions of monomials on the content of controllable positions easily predictable. Lemma 2 guarantees that the ratio of such x can be arbitrarily large.

0. Put $c_0^{x,\ldots,x^s} = s^2$.

2. Put $\Delta = \lceil \log_p s \rceil$. Let us now calculate N' as

$$\widehat{L}_{x,x^2,\ldots,x^{s-1}}(2k + \Delta, \varepsilon_1, d, \Delta, s - 1).$$

As $\widehat{N}_d^{x,x^2,\ldots,x^s}(k, \varepsilon_1)$ we choose $2N'$. Here we have used the induction hypothesis, i.e., the uniformity of the collection $x, \ldots, x^{s-1}$, and applied Lemma 2 to it.

In what follows we understand $\widehat{N}_d$ as $\widehat{N}_d^{x,x^2,\ldots,x^s}(k, \varepsilon_1)$.

4. Good chooses the minor N' positions (i.e., the half of positions that corresponds to the less significant positions), except the latter d ones, which are filled already. As admissible techniques, Good chooses ones which are concurrently suitable for the collection $a_i^{(j)}$:

$$a_i^{(j)} = \begin{cases} 0, & i \neq j \\ p^k, & i = j \end{cases}$$

Lemma 2 guarantees that their ratio to the total number of ways to fill the minor N' positions (the number of the latter equals $p^{N'-d}$) is at least $1 - \varepsilon_1$.

6. Since on Step 5 Evil has chosen one of defined techniques, there exist numbers $r^{(j)}$ satisfying conditions of Lemma 2. We color exactly sk positions; namely, the major k positions (they correspond to degrees of p from p^{n-k} to p^{n-1}), and for each $r^{(j)}$ we color positions which correspond to degrees from $p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}$ to $p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)+k-1}$, i.e., exactly k positions for each j from 1 to $s-1$. Conditions 2 in the definition of a concurrently suitable collection $r^{(j)}$ and the fact that $\Delta \geqslant \mathrm{ord}_p(j+1)$ with all j under consideration guarantee that all sets of positions do not intersect.

8. In order to avoid any ambiguity in understanding $a_i^{(j)}$ defined on Step 4 and a_i provided by Evil on Step 7, we denote the latter by $\tilde{a}_i$. On Step 6 exactly sk positions are chosen, therefore now we have to fill them in exactly one way so as to make the initial rows of the length k differ from $\tilde{a}_i$ provided by Evil on Step 7 no more than by c_0. Firstly, we fill the major k positions of x with the value $\tilde{a}_1$. Now we denote by b_j the k-digit number which occupies positions from $p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}$ to $p^{n-r^{(j)}-\Delta-\mathrm{ord}_p(j+1)+k-1}$ (these positions were colored on Step 6). Denote by B the number, whose p-adic notation would have been written on the board, if each of b_j had equaled 0. Therefore,

$$x = B + \sum_{j=1}^{s-1} b_j p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}. \tag{1}$$

Fix

$$b'_j = (\tilde{a}_{j+1} - \left\lfloor \frac{B^{j+1} \bmod p^n}{p^{n-k}} \right\rfloor) \bmod p^k. \tag{2}$$

In other words, let b'_j equal the difference between $\tilde{a}_{j+1}$ and the first k digits of B^{j+1} calculated modulo p^k. Now let b_j equal $b'_j(\theta(j+1))^{-1} \bmod p^k$ (since, by definition, $\theta(j+1)$ is not multiple of p, desired $(\theta(j+1))^{-1}$ exists modulo p^k). Let us write obtained b_j in the corresponding positions on the board and prove that obtained x satisfies the requirements stated in the description of Step 8 of the modified game.

Firstly, since the first k digits of x represent the notation of $\tilde{a}_1$ (as was fixed earlier), the desired assertion is valid for $f_1(x) = x$.

Let us now prove the desired assertion for $f_t(x) = x^t, 2 \leqslant t \leqslant s$. Consider the expression for x^t. Let us immediately remove the brackets in the above expression 1) for x in terms of $B, b_1, b_2, \ldots, b_{s-1}$. Since $n \geqslant \widehat{N}_d = 2N', r^{(j)} \leqslant N', \Delta \geqslant \mathrm{ord}_p(j+1)$, we have $n - r^{(j)} + \Delta - \mathrm{ord}_p(j+1) \geqslant n - N' \geqslant n/2$, which means that products containing at least two terms with b_j (for the same or distinct values of j) vanish after the calculation of x^t modulo p^n. Therefore,

$$f_t(x) \bmod p^n = x^t \bmod p^n = (B^t + \sum_{j=1}^{s-1} tB^{t-1} b_j p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}) \bmod p^n. \tag{3}$$

Consider the expression $tB^{t-1}b_j p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)} \bmod p^n$. Note that the multiplication by $p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}$ shifts the p-adic notation of the number by $n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)$ positions to the left. Therefore, digits of $tB^{t-1}b_j$ that occupy the positions which correspond to degrees of p not lesser than $n-(n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)) =$

$r^{(j)}-\Delta+\mathrm{ord}_p(j+1)$ do not affect the result, because they vanish after the calculation modulo p^n.

Let us first prove that the major digits of $x^t \bmod p^n$ are nearly independent of the choice of b_j with $j \neq t-1$.

Consider the expression $B^{t-1}b_j p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)} \bmod p^n$ for $j \neq t-1$. Taking into account the above reasoning, we can write $((B^{t-1}b_j) \bmod p^{r^{(j)}-\Delta+\mathrm{ord}_p(j+1)})p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}$. In accordance with the definition of $r^{(j)}$, the choice of $a_i^{(j)}$, and the choice of an admissible set for the minor N' positions on Step 4, the first $2k+\Delta$ p-adic digits in the $r^{(j)}$-digit notation of the number $B^{t-1} \bmod p^{r^{(j)}}$ are zeros. Since $\Delta \geqslant \mathrm{ord}_p(j+1)$, this means that at least $2k+\mathrm{ord}_p(j+1)$ first digits in the $(r^{(j)}-\Delta+\mathrm{ord}_p(j+1))$-digit notation of $B^{t-1} \bmod p^{r^{(j)}-\Delta+\mathrm{ord}_p(j+1)}$ are zeros. Taking into account the inequality $b_j < p^k$, this means that at least $k+\mathrm{ord}_p(j+1)$ major digits in the notation of $(b_j B^{t-1}) \bmod p^{r^{(j)}-\Delta+\mathrm{ord}_p(j+1)}$ are zeros. Hence it follows that the number of zeros in the n-digit notation of the number $(b_j B^{t-1}p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)}) \bmod p^n$ is the same. Thus, we have proved that at least k major digits in the notation of the latter number are zeros.

Let us now prove that the choice of b_{t-1} guarantees the presence of almost desired digits at the beginning of the notation of $x^t \bmod p^n$. Consider the expression $tB^{t-1}b_j p^{n-r^{(j)}+\Delta-\mathrm{ord}_p(j+1)} \bmod p^n$ for $j = t-1$. Let us represent t as $\theta(t)p^{\mathrm{ord}_p t}$. Then the expression takes the form $(\theta(t)b_{t-1}B^{t-1}p^{n-r^{(t-1)}+\Delta-\mathrm{ord}_p(t)+\mathrm{ord}_p(t)}) \bmod p^n = (\theta(t)b_{t-1}B^{t-1}p^{n-r^{(t-1)}+\Delta}) \bmod p^n$. Consider separately $(b_{t-1}B^{t-1}p^{n-r^{(t-1)}+\Delta}) \bmod p^n$. Reasoning similarly to the case when $j \neq t-1$, we can write

$$((b_{t-1}B^{t-1}) \bmod p^{n-(n-r^{(t-1)}+\Delta)})p^{n-r^{(t-1)}+\Delta} =$$

$$= ((b_{t-1}B^{t-1}) \bmod p^{r^{(t-1)}-\Delta})p^{n-r^{(t-1)}+\Delta}.$$

By the definition of $r^{(j)}$, the choice of $a_i^{(j)}$, and the choice of an admissible set for the minor N' positions on Step 4, the first $2k+\Delta$ p-adic digits in the $r^{(t-1)}$-digit notation of the number $B^{t-1} \bmod p^{r^{(t-1)}}$ form the notation of the number p^k. This means that the first $2k$ digits in the $(r^{(t-1)}-\Delta)$-digit notation of $B^{t-1} \bmod p^{r^{(t-1)}-\Delta}$ also form the notation of p^k.

The latter property is equivalent to the fact that the first k digits of the number $(b_{t-1}B^{t-1}) \bmod p^{r^{(t-1)}-\Delta}$ form the notation of b_{t-1}, because k zeros that follow the unit in the $2k$-digit notation of the number p^k cancel the possible carry-out. Therefore, the first k digits in the n-digit notation of $(b_{t-1}B^{t-1}p^{n-r^{(t-1)}+\Delta}) \bmod p^n$ also form the notation of b_{t-1}.

Let us now consider the addends that enter in the sum for x^t in formula (3). We have $s-2$ expressions in the form $(B^{t-1}b_j p^{n-r^{(j)}+\Delta)-\mathrm{ord}_p(j+1)}) \bmod p^n$ for $j \neq t-1$ which enter in the sum for x^t with the coefficient t, one expression $(B^{t-1}b_{t-1}p^{n-r^{(t-1)}+\Delta}) \bmod p^n$ which enters in it with the coefficient $\theta(t)$, and one expression B^t which enters in this sum with the coefficient 1. Taking into account the proved assertion, as well as the fact that $b_t\theta(t) = b'_t$, in view of the definition of b'_t, we conclude that considering (with the same coefficients) the numbers whose notations are formed by the k major digits in each term, we will get $\tilde{a}_t$ calculated modulo p^k.

It remains to prove that the influence of the minor digits is smoothed over. Consider the linear combination with coefficients $c_1 = c_2 = \ldots = c_{s-2} = t, c_{s-1} = \theta(t), c_s = 1$. By Lemma 5, the k major digits of this linear combination calculated modulo p^n differ from the linear combination of numbers formed by the k major digits of the initial numbers calculated modulo p^k at most by

$$\sum_{i=1}^{s} c_s = t(s-2) + \theta(t) + 1 \leqslant s^2,$$

which coincides with the constant c_0 chosen on Step 0. Therefore, obtained x satisfies requirements of item 8 of the modified game.

Let us now discuss the question of why with various collections a_i we obtain distinct x. Let us have a collection $\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_s$ and $\tilde{a}'_1, \tilde{a}'_2, \ldots, \tilde{a}'_s$. If $\tilde{a}_1 \neq \tilde{a}'_1$, then obtained x differ in the first k positions. In other words, let $\tilde{a}_i \neq \tilde{a}'_i$ with some $i > 1$. Then corresponding b'_{i-1} are also distinct (see (2)), because in both cases B coincide being independent of $\tilde{a}_j$ with $j > 1$. This means that b_{i-1} are also distinct, which implies the diversity of x.

The obtained strategy proves the theorem. □

7 Estimation of the uniformity limits

Recall that the equality sign following any of symbols $N, \widetilde{N}, \widehat{N}, L, \widetilde{L}$ means that the function in the right-hand side can serve as the corresponding bound n, not necessarily the minimal one.

Theorem 4. *It holds* $\widehat{N}_d^{x,x^2,\ldots,x^s}(k,\varepsilon) = \exp\{p^{c_1(s)k - c_2(s)\log\varepsilon + c_3(s)}\} + d\exp\{p^{c_4(s)k - c_5(s)\log\varepsilon + c_6(s)}\}$, *where* c_i *are some functions that depend only on* s *and* p.

Proof. Correlations established in lemmas 1,2,3,4 and Theorem 3 give the following system of equalities:

- $N_d^x(k,\varepsilon) = k + d$;
- $N_d^{x,\dots,x^s}(k,\varepsilon) = \widetilde{N}_d^{x,\dots,x^s}(k, \varepsilon/(2p^{sk}), \varepsilon/(2p^{sk}))$;
- $\widetilde{N}_d^{x,\dots,x^s}(k,\varepsilon_1,\varepsilon_2) = \widehat{N}_d^{x,\dots,x^s}(k + \log_p \frac{2s^3}{\varepsilon_2}, \varepsilon_1)$;
- $\widehat{N}_d^{x,\dots,x^s}(k,\varepsilon_1) = 2\widetilde{L}_{x,x^2,\dots,x^{s-1}}(2k + \lceil \log_p s \rceil, \varepsilon_1, d, \lceil \log_p s \rceil, s-1)$;
- the following way to calculate $\widetilde{L}_{f_1,\dots,f_s}$: $\widetilde{L}^{(0)} = d$, $\widetilde{L}^{(j)} = L_{f_1,\dots,f_s}(k,\varepsilon,\widetilde{L}^{(j-1)} + \Delta)$ with $j > 0$ and put $\widetilde{L}_{f_1,\dots,f_s}(k,\varepsilon,d,\Delta,m) = \widetilde{L}^{(m)}$;
- the following way to calculate $L_{f_1,\dots,f_s}(k,\varepsilon,d)$: $L^{(0)} = d$, $L^{(i)} = N^{f_1,\dots,f_s}_{L^{(i-1)}+k}(k,1/2)$ with $i > 0$ and put $L_{f_1,\dots,f_s}(k,\varepsilon,d) = L^{(\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil)}$.

Introduce the following denotations:
$N_d^{x,\dots,x^s}(k,1/2) = A(s,k) + dB(s,k)$;
$\widetilde{N}_d^{x,\dots,x^s}(k,1/(4p^{sk}),1/(4p^{sk})) = \widetilde{A}(s,k) + d\widetilde{B}(s,k)$;
$\widehat{N}_d^{x,\dots,x^s}(k,1/(4p^{sk})) = \widehat{A}(s,k) + d\widehat{B}(s,k)$;
$L_{x^1,\dots,x^s}(k,1/(4p^{sk}),d) = A_L(s,k) + dB_L(s,k)$;
$\widetilde{L}_{x^1,\dots,x^s}(k,1/(4p^{sk}),d,\lceil \log_p s \rceil, s) = A_{\widetilde{L}}(s,k) + dB_{\widetilde{L}}(s,k)$.
Then
$N_d^{x,\dots,x^s}(k,\varepsilon) = \widetilde{N}_d^{x,\dots,x^s}(k,\varepsilon/(2p^{sk}),\varepsilon/(2p^{sk}))$ gives
$A(s,k) = \widetilde{A}(s,k), \quad B(s,k) = \widetilde{B}(s,k)$.

$\widetilde{N}_d^{x,\dots,x^s}(k,\varepsilon_1,\varepsilon_2) = \widehat{N}_d^{x,\dots,x^s}(k + \log_p \frac{2s^3}{\varepsilon_2}, \varepsilon_1)$ gives
$\widetilde{A}(s,k) = \widehat{A}(s, k + \log_p \frac{2s^3}{1/(4p^{sk})}), \quad \widetilde{B}(s,k) = \widehat{B}(s, k + \log_p \frac{2s^3}{1/(4p^{sk})})$.

$\widehat{N}_d^{x,\dots,x^s}(k,\varepsilon_1) = 2\widetilde{L}_{x,x^2,\dots,x^{s-1}}(2k + \lceil \log_p s \rceil, \varepsilon_1, d, \lceil \log_p s \rceil, s-1)$ gives
$\widehat{A}(s,k) = 2A_{\widetilde{L}}(s-1,k), \quad \widehat{B}(s,k) = 2B_{\widetilde{L}}(s-1,k)$.

Let some function $f(d) = a + bd$ be given. Then for each constant Δ we can construct the following sequence of functions $f_i(d)$: $f_0(d) = d, f_i(d) = f(f_{i-1}(d) + \Delta)$. We can represent obtained $f_i(d)$ as $f_i(d) = a_i + db_i$. Denote such numbers a_i and b_i by $A_{rec}(a,b,i,\Delta)$ and $B_{rec}(a,b,i,\Delta)$, respectively.
Let us estimate A_{rec} and B_{rec} with $b \geqslant 2, a > 0$:

$$A_{rec} = a + b(a + \Delta + b(a + \Delta + \ldots + (a + \Delta + b(a + \Delta))\ldots)) \leqslant (a + \Delta)b^i, \quad B_{rec} = b^i.$$

Then the following way to calculate $\widetilde{L}_{f_1,\ldots,f_s}$: $\widetilde{L}^{(0)} = d$, $\widetilde{L}^{(j)} = L_{f_1,\ldots,f_s}(k, \varepsilon, \widetilde{L}^{(j-1)} + \Delta)$ with $j > 0$ and $\widetilde{L}_{f_1,\ldots,f_s}(k, \varepsilon, d, \Delta, m) = \widetilde{L}^{(m)}$ gives

$A_{\widetilde{L}}(s,k) = A_{rec}(A_L(s,k), B_L(s,k), s, \lceil \log_p(s+1) \rceil)$,

$B_{\widetilde{L}}(s,k) = B_{rec}(A_L(s,k), B_L(s,k), s, \lceil \log_p(s+1) \rceil)$.

The following way to calculate $L_{f_1,\ldots,f_s}(k, \varepsilon, d)$: $L^{(0)} = d$, $L^{(i)} = N^{f_1,\ldots,f_s}_{L^{(i-1)}+k}(k, 1/2), i > 0$ and $L_{f_1,\ldots,f_s}(k, \varepsilon, d) = L^{(\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil)}$ gives:

$A_L(s,k) = A_{rec}(A(s,k), B(s,k), \lceil \log_{1-1/(2p^{sk})}(1/(4p^{sk})) \rceil, k)$,

$B_L(s,k) = B_{rec}(A(s,k), B(s,k), \lceil \log_{1-1/(2p^{sk})}(1/(4p^{sk})) \rceil, k)$.

Since $-\log(1 - 1/(2p^{sk})) > 1/(2p^{sk})$, we have:

$A_L(s,k) \leqslant A_{rec}(A(s,k), B(s,k), \lceil 2p^{sk} \log(4p^{sk}) \rceil, k)$,

$B_L(s,k) \leqslant B_{rec}(A(s,k), B(s,k), \lceil 2p^{sk} \log(4p^{sk}) \rceil, k)$.

Therefore,

$A(1,k) = k$,

$B(1,k) = 1$,

$A(s,k) = \widetilde{A}(s,k)$,

$B(s,k) = \widetilde{B}(s,k)$,

$\widehat{A}(s,k) = 2A_{\widetilde{L}}(s-1,k)$,

$\widehat{B}(s,k) = 2B_{\widetilde{L}}(s-1,k)$,

$\widetilde{A}(s,k) = \widehat{A}(s, \lceil k + \log_p(2s^3 4p^{sk}) \rceil)$,

$\widetilde{B}(s,k) = \widehat{B}(s, \lceil k + \log_p(2s^3 4p^{sk}) \rceil)$,

$A_{rec}(a,b,\Delta,i) \leqslant (a+\Delta)b^i$,

$B_{rec}(a,b,\Delta,i) = b^i$,

$A_{\widetilde{L}}(s,k) = (A_L(s,k) + \lceil \log_p(s+1) \rceil) B_L(s,k)^s$,

$B_{\widetilde{L}}(s,k) = B_L(s,k)^s$,

$A_L(s,k) = (k + A(s,k)) B(s,k)^{\lceil 2p^{sk} \log(4p^{sk}) \rceil}$,

$B_L(s,k) = B(s,k)^{\lceil 2p^{sk} \log(4p^{sk}) \rceil}$.

Taking the logarithm, we obtain

$\log A(1,k) = \log k$,

$\log B(1,k) = 0$,

$\log A(s,k) = \log \widetilde{A}(s,k)$,

$\log B(s,k) = \log \widetilde{B}(s,k)$,

$\log \widehat{A}(s,k) = \log 2 + \log A_{\widetilde{L}}(s-1,k)$,

$\log \widehat{B}(s,k) = \log 2 + \log B_{\widetilde{L}}(s-1,k)$,

$\log \widetilde{A}(s,k) = \log \widehat{A}(s, \lceil k + \log_p(2s^3 4p^{sk}) \rceil)$,

$\log \widetilde{B}(s,k) = \log \widehat{B}(s, \lceil k + \log_p(2s^3 4p^{sk})\rceil)$,
$\log A_{\widetilde{L}}(s,k) = \log(A_L(s,k) + \lceil \log_p(s+1)\rceil) + s \log B_L(s,k)$,
$\log B_{\widetilde{L}}(s,k) = s \log B_L(s,k)$,
$\log A_L(s,k) = \log(k + A(s,k)) + \lceil 2p^{sk} \log(4p^{sk})\rceil \log B(s,k)$,
$\log B_L(s,k) = \lceil 2p^{sk} \log(4p^{sk})\rceil \log B(s,k)$.

Let us obtain bounds for the repeated logarithm. To this end we will apply the correlation written above the statement of the theorem, using the equality sign. With $x \geqslant 2$ and $y \geqslant 2$ we have $xy \geqslant x+y$; this allows us to approximately calculate the logarithm of the sum as the sum of logarithms, provided that addends satisfy the mentioned conditions.

In above correlations we are interested in the upper bound for the case when $s > 1$. Let us replace the initial conditions with $B(1,k) = 2, A(1,k) = k+2$. Since we have replaced certain values with greater ones, in sums in the right-hand sides of the correlations all addends (except $\log 2$ or, possibly, $\lceil \log_p(s+1)\rceil$) exceed 2. In above correlations we are interested in the upper bound for the case when $s > 1$. Let us replace initial conditions with $B(1,k) = 2, A(1,k) = k+2$. Note that the substituted values exceed initial ones. By replacing the rest constants with greater values we also make the resulting bound more rough. Now we assume that all summands exceed 2 (we replace $\log 2$ with 2, and do $\lceil \log_p(s+1)\rceil$) with $s+1$). Now, using the inequality from the previous paragraph, we replace the sum with the product. Then we calculate the logarithm (of the base p) and again replace constants with upper bounds (thus, for example, $\log_p 2 < 1$, and logarithms of the rest constants are less than the latter themselves). As a result, we obtain the following simple recurrent correlations for (overestimated) double logarithms:

$\log_p \log A(1,k) = k+2$,
$\log_p \log B(1,k) = 2$,
$\log_p \log \widetilde{A}(1,k) = k$,
$\log_p \log \widetilde{B}(1,k) = 2$,
$\log_p \log A(s,k) = \log_p \log \widetilde{A}(s,k)$,
$\log_p \log B(s,k) = \log_p \log \widetilde{B}(s,k)$,
$\log_p \log \widetilde{A}(s,k) = \log_p \log \widehat{A}(s, k+sk+3s+3)$,
$\log_p \log \widetilde{B}(s,k) = \log_p \log \widehat{B}(s, k+sk+3s+3)$,
$\log_p \log \widehat{A}(s,k) = 1 + \log_p \log A_{\widetilde{L}}(s-1,k)$,
$\log_p \log \widehat{B}(s,k) = 1 + \log_p \log B_{\widetilde{L}}(s-1,k)$,
$\log_p \log A_{\widetilde{L}}(s,k) = \log_p \log A_L(s,k) + 2s + s + \log_p \log B_L(s,k)$,
$\log_p \log B_{\widetilde{L}}(s,k) = s + \log_p \log B_L(s,k)$,
$\log_p \log A_L(s,k) = k + \log_p \log A(s,k) + sk + \log_p \log B(s,k)$,

$\log_p \log B_L(s,k) = sk + \log_p \log B(s,k)$.

But even these (amplified) double logarithms A and B, evidently, linearly depend on k (with fixed s). This means that the linear upper bound with respect to k is also fulfilled for non-modified double logarithms A and B.

Thus, we have obtained a bound for $N_d^{x,\dots,x^s}(k,1/2)$. Let us now perform the initial induction step of Theorem 3, where ε is arbitrary.

We have

$L^{(0)} = d$, $L^{(i)} = N_{L^{(i-1)}+k}(k,1/2)$ with $i > 0$ and $L_{x,\dots,x^s}(k,\varepsilon,d) = L^{(\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil)}$, whence with the help of bounds for A_{rec} and B_{rec} we obtain

$$L_{x,\dots,x^s}(k,\varepsilon,d) \leqslant (A(s,k)+k)B(s,k)^{\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil} + dB(s,k)^{\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil}.$$

Using the formula for $\widetilde{L}(s,k)$ and the same bounds for A_{rec} and B_{rec}, we get

$$\widetilde{L}_{x,\dots,x^s}(k,\varepsilon,d,\Delta,s) \leqslant ((A(s,k)+k)B(s,k)^{\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil} + \Delta)B(s,k)^{s\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil} +$$

$$dB(s,k)^{s\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil}.$$

With $0 < x < 1, 0 < \varepsilon < 1$, it holds $\lceil \log_{1-x} \varepsilon \rceil \geqslant -(\log \varepsilon)/x + 1$, therefore $\lceil \log_{1-1/(2p^{sk})} \varepsilon \rceil < -2p^{sk} \log \varepsilon + 1$.

Let us represent $2p^{(s-1)(2k+\lceil \log_p s \rceil)}$ as $c(s)p^{2(s-1)k}$, where $c(s)$ is some function of s. Therefore,

$$\widehat{N}_d^{x,\dots,x^s}(k,\varepsilon_1) = 2\widetilde{L}_{x,\dots,x^{s-1}}(2k+\lceil \log_p s \rceil, \varepsilon_1, d, \lceil \log_p s \rceil, s-1) \leqslant$$

$$2((A(s-1,2k+\lceil \log_p s \rceil)+2k+\lceil \log_p s \rceil)B(s-1,2k+\lceil \log_p s \rceil)^{-c(s)p^{2(s-1)k}\log \varepsilon_1 + 1} + \lceil \log_p s \rceil) \times$$

$$B(s-1,2k+\lceil \log_p s \rceil)^{(s-1)(-c(s)p^{2(s-1)k}\log \varepsilon_1 + 1)} +$$

$$2dB(s-1,2k+\lceil \log_p s \rceil)^{(s-1)(-c(s)p^{2(s-1)k}\log \varepsilon_1 + 1)}.$$

Consider double logarithms of the coefficient at d and the free term in last but one expression. Taking into account the obtained above linear (with respect to k) bounds for double logarithms of A and B, we obtain linear with respect to k and $\log \varepsilon$ bounds for these functions.

□

8 The uniformity for linear combinations

In lemmas 6-10, as well as in theorems 5, 6, we understand the sentence «the joint projection of the collection $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution» as a requirement stronger than Definition 3, namely, the existence of a winning strategy for the modified game.

We intend to prove that the uniformity of the collection $(f_1(x), \ldots, f_s(x))$ implies that of the collection $(g_1(x), \ldots, g_s(x))$, provided that the second collection is obtained from the first one by adding to one of functions an integer linear combination of the rest ones or by adding an integer constant, or by multiplying by such a constant. Hence and from Theorem 3 we deduce the uniformity of the s-dimensional projection of polynomials.

Lemma 6. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and u is a natural number. Then the joint projection of the collection $p^u f_1(x), f_2(x), \ldots, f_s(x)$ also has a uniform distribution, and*

$$\begin{aligned} \widehat{N}_d^{p^u f_1, f_2, \ldots, f_s}(k, \varepsilon) &= \widehat{N}_d^{f_1, \ldots, f_s}(k+u, \varepsilon) \\ c_0^{p^u f_1, f_2, \ldots, f_s} &= c_0^{f_1, \ldots, f_s}. \end{aligned}$$

Proof. Assume that there exists an oracle which implements a winning strategy for the collection $f_1(x), f_2(x), \ldots, f_s(x)$. Let us represent the strategy for the mediator that uses this oracle.

The mediator uses p^{su} identical oracles. On steps 0-6 he sends unchanged data from oracles to Evil and from Evil to oracles, except the fact that instead of k he informs oracles of the number $k+u$. Since the oracles are determinate, the data obtained from them coincide. The mediator transforms the collection $a_1, a_2, \ldots, a_s$ of numbers of the length k obtained on Step 7 into p^{su} collections of numbers of the length $k+u$ in the following way: to a_1 he appends (in all possible ways) the major u digits, and does to $a_2, \ldots, a_s$ (in all possible ways) the minor u ones (thus, the total number of used variants is $(p^s)^u = p^{su}$). Then he sends to each oracle one of collections and obtains from them $p^{su} p^{m-(k+u)s} = p^{m-sk}$ ways to fill m positions which were not filled on Step 6. Evidently, the obtained variants satisfy conditions imposed on $f_2(x), \ldots, f_s(x)$, because the first k digits of the corresponding numbers in collections sent to the oracles coincide with $a_2, \ldots, a_s$. One can also easily see that the stated condition is also fulfilled for $f_1(x)$, because the minor k positions among $k+u$ ones in notations of numbers sent to the oracles as a_1 coincide with a_1, and the multiplication by p^u make the p-adic notation of

a number shift by u positions to the left. This means that each of p^{m-sk} ways to fill the colored positions proposed by oracles satisfy the conditions imposed on it on Step 8 of the game. All these variants are distinct due to the additional requirement imposed on them on Step 8; consequently, the mediator can present them to Evil as a response implied by Step 8 of the protocol.

For various collections $a_1, a_2, \ldots, a_s$, the collections presented to the oracles are also distinct, therefore the validity of the additional requirement for the mediator follows from its validity for the oracles. □

Lemma 7. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and u is an integer number mutually prime with p. Then the joint projection of the collection $uf_1(x), f_2(x), \ldots, f_s(x)$ also has a uniform distribution, and*

$$\begin{aligned} \widehat{N}_d^{uf_1,f_2,\ldots,f_s}(k,\varepsilon) &= \widehat{N}_d^{f_1,\ldots,f_s}(k,\varepsilon) \\ c_0^{uf_1,f_2,\ldots,f_s} &= uc_0^{f_1,\ldots,f_s}. \end{aligned}$$

Proof. Assume that there exist an oracle which implements a winning strategy for the collection $f_1(x), f_2(x), \ldots, f_s(x)$. Let us describe the strategy for the mediator, who uses this oracle.

On steps 0-6 the mediator sends unchanged data from oracles to Evil and from Evil to oracles, except the fact that on Step 0 he multiplies c_0 (obtained from an oracle) by u. Denote the value of c_0 initially obtained from an oracle by c_0'. Having obtained on Step 7 numbers $a_1, a_2, \ldots, a_s$, the mediator calculates $a_1' = a_1 u^{-1} \bmod p^k$ (the desired inverse value exists, because u is mutually prime with p) and sends the collection $a_1', a_2, a_3, \ldots, a_s$ to an oracle. Let us prove that the variants of filling the colored positions proposed by the oracle satisfy the stated conditions. This, evidently, is true for $f_2(x), f_3(x), \ldots, f_s(x)$. It is also true that the first k digits of $f_1(x)$ differ from a_1' at most by c_0'. By Lemma 5 this implies that the first k digits of $f_1(x)u$ differ from a_1 at most by c_0; therefore, the condition stated on Step 8 is also fulfilled for $f_1(x)$.

For different collections $a_1, a_2, \ldots, a_s$, the collections sent to an oracle are also different; therefore the fulfillment of the additional condition for an oracle implies its validity for the mediator. □

Lemma 8. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and u is an integer nonzero number. Then the joint projection of the collection $uf_1(x), f_2(x), \ldots, f_s(x)$ also has a uniform*

distribution, and

$$\begin{aligned} \widehat{N}_d^{uf_1,f_2,\ldots,f_s}(k,\varepsilon) &= \widehat{N}_d^{f_1,\ldots,f_s}(k+ord_p u,\varepsilon) \\ c_0^{uf_1,f_2,\ldots,f_s} &= \theta(u)c_0^{f_1,\ldots,f_s}. \end{aligned}$$

Proof. The desired assertion follows from two previous lemmas and the representation $u=\theta(u)p^{\mathrm{ord}_p u}$. □

Lemma 9. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and u is an integer number. Then the joint projection of the collection $f_1(x)+u, f_2(x), \ldots, f_s(x)$ also has a uniform distribution, and*

$$\begin{aligned} \widehat{N}_d^{f_1+u,f_2,\ldots,f_s}(k,\varepsilon) &= \widehat{N}_d^{f_1,\ldots,f_s}(k,\varepsilon) \\ c_0^{f_1+u,f_2,\ldots,f_s} &= c_0^{f_1,\ldots,f_s}+u+1. \end{aligned}$$

Proof. Assume that there is an oracle, which implements a winning strategy for the collection $f_1(x), f_2(x), \ldots, f_s(x)$. Let us describe the strategy for the mediator which uses this oracle.

On steps 0-7 the mediator sends unchanged data from the oracles to Evil, and from Evil to the oracles, except the fact that on Step 0 he increases c_0 (obtained from an oracle) by $u+1$. Denote the value of c_0 initially obtained from an oracle by c_0'. Let us prove that the variants of filling the colored positions proposed by an oracle on Step 8 satisfy the stated conditions. Evidently, this is true for $f_2(x), f_3(x), \ldots, f_s(x)$. Moreover, the first k digits of $f_1(x)$ differ from a_1 at most by c_0'. Let us represent $f_1(x)+u$ as $1\cdot f_1(x)+u\cdot 1$. Since $n_0>k$, the first k digits in the n-digit notation of 1 are zeros. By Lemma 5 this means that the first k digits of $f_1(x)+u$ differ from a_1 at most by c_0; therefore, the condition stated on Step 8 is also fulfilled for $f_1(x)$.

If collections $a_1, a_2, \ldots, a_s$ are distinct, then so are collections given to an oracle, therefore the validity of the additional condition for the mediator follows from its validity for an oracle. □

Lemma 10. *Assume that the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and $u_2, u_3, \ldots, u_s$ are arbitrary integer numbers. Then the joint projection of the collection $f_1(x)+\sum\limits_{i=2}^{s} u_i f_i(x), f_2(x), \ldots, f_s(x)$ also has a uniform distribution, and*

$$\begin{aligned} \widehat{N}_d^{f_1+\sum\limits_{i=2}^{s} u_i f_i,f_2,\ldots,f_s}(k,\varepsilon) &= \widehat{N}_d^{f_1,\ldots,f_s}(k,\varepsilon) \\ c_0^{f_1+\sum\limits_{i=2}^{s} u_i f_i,f_2,\ldots,f_s} &= c_0^{f_1,\ldots,f_s}+\sum_{i=2}^{s} u_i. \end{aligned}$$

Proof. Assume that some oracle implements a winning strategy for the collection $f_1(x), f_2(x), \ldots, f_s(x)$. Let us describe the strategy for the mediator which uses this oracle.

On steps 0-6 the mediator sends unchanged data from the oracles to Evil and from Evil to the oracles, except the fact that on Step 0 he increases the value of c_0 (obtained from an oracle) by $1 + \sum_{i=2}^{s} u_i$. Denote the value of c_0 initially obtained from an oracle by c_0'. After obtaining on Step 7 numbers $a_1, a_2, \ldots, a_s$, he calculates $a_1' = a_1 - \sum_{i=2}^{s} u_i a_i \bmod p^k$ and sends the collection $a_1', a_2, a_3, \ldots, a_s$ to an oracle. Let us prove that the variants of filling the colored positions proposed by an oracle satisfy the stated conditions. Evidently, this is true for $f_2(x), f_3(x), \ldots, f_s(x)$. It is also true that the first k digits of $f_1(x)$ differ from a_1' at most by c_0'. By Lemma 5 hence we deduce that the first k digits of $f_1(x) + \sum_{i=2}^{s} u_i f_i(x)$ differ from a_1 at most by c_0; therefore, the condition stated on Step 8 is also fulfilled for $f_1(x)$.

If collections $a_1, a_2, \ldots, a_s$ are distinct, then so are the collections sent to an oracle, because $a_2, \ldots, a_s$ are sent unchanged, and if they coincide, then the number subtracted from a_1 also equals the same value. Therefore, if the additional condition is valid for an oracle, then it is also valid for the mediator. □

9 The uniformity for polynomials

Theorem 5. *Let A be an arbitrary nondegenerate integer $s \times s$-matrix. Assume that the column of polynomials $f_1, \ldots, f_s$ is given by the correlation $(f_1, \ldots, f_s)^T = A(x, \ldots, x^s)^T + z$, where z is an arbitrary constant integer $s \times 1$-column. The joint projection of the collection $f_1(x), f_2(x), \ldots, f_s(x)$ has a uniform distribution, and*

$$N^{f_1,\ldots,f_s}(\varepsilon) = \exp\{c_1 \varepsilon^{-c_2}\},$$

where c_1, c_2 are positive constants depending only on the collection of f_i and independent of ε.

Proof. By Theorem 3 the joint projection of the collection $x, x^2, \ldots, x^s$ has a uniform distribution. In view of lemmas 8, 9, and 10 we can perform three operations with the collection, namely,

- add an integer constant to any function;
- multiply any function by an integer nonzero constant;

- add to any function an integer linear combination of the rest functions;

as above, the joint projection has a uniform distribution. To complete the proof, it remains to show that these operations allow us to transform the collection $x, x^2, \dots, x^s$ into that $f_1(x), f_2(x), \dots, f_s(x)$.

Really, lemmas 6-10 change the value of k only in the following way: they add to k some constant independent of k and ε. Therefore, taking into account Theorem 4, we obtain the correlation

$$\widehat{N}_0^{f_1,\dots,f_s}(k,\varepsilon_1) = \exp\{p^{c_1 k - c_2 \log\varepsilon + c_3}\},$$

where c_1, c_2, c_3 are some constants depending on the collection of f_i (we replace d with 0, which makes the second term in the bound in Theorem 4 vanish). Lemmas 6-10 define some value $c_0^{f_1,\dots,f_s}$. Sequentially applying lemmas 3 and 4, we get

$$N_0^{f_1,\dots,f_s}(k,\varepsilon) = \widetilde{N}_0^{f_1,\dots,f_s}(k,\varepsilon/(2p^{sk}),\varepsilon/(2p^{sk})) = \widehat{N}_0^{f_1,\dots,f_s}(k+\log_p \frac{2sc_0^{f_1,\dots,f_s}}{\varepsilon/(2p^{sk})},\varepsilon/(2p^{sk})).$$

Note that both $\log_p(\varepsilon/(2p^{sk})$ and $\log_p \frac{2sc_0^{f_1,\dots,f_s}}{\varepsilon/(2p^{sk})}$ are representable as a linear combination of $1, k, \log\varepsilon$, whose coefficients depend only on $f_1, \dots, f_s$ and are independent of k, ε. In accordance with Theorem 2 we set $k = -\log_p\varepsilon + \log_p 4s$ and thus obtain desired

$$N^{f_1,\dots,f_s}(\varepsilon) = \exp\{c_1\varepsilon^{-c_2}\}.$$

for some positive numbers c_1, c_2 (their positiveness follows from the nonnegativity of N and the fact that the bound increases as ε diminishes).

Let us now prove that by described operations we can get the collection $(f_1, \dots, f_s)$. To this end, let us begin with the collection $(f_1, \dots, f_s)$ and obtain that $x, \dots, x^s$ by the following operations:

- add to any function an integer constant;
- divide any function by an integer nonzero constant;
- add to any function an integer linear combination of the rest functions,

and then perform the corresponding inverse operations in the converse order.

Let us obtain functions in three steps.

1. Firstly, get rid of free terms, just subtracting them. This allows us to represent the collection $f_1, \dots, f_s$ in the form $A(x, \dots, x^s)^T$ with some matrix A. Below in the proof of the theorem we identify the collection of functions $f_1, \dots, f_s$ with this matrix A.

2. Obtain an upper-triangular matrix.

3. Sequentially, starting with the last column, reduce the matrix to the desired form.

Step 1 is evident.

Let us describe Step 2 in detail. Assume that for some number t, $0 \leqslant t \leqslant s$, for each column $i, 1 \leqslant i \leqslant t$, all elements below the diagonal equal zero. Let us describe the way to proceed from $t = t'$ to $t = t' + 1$. At the very beginning we assume that $t = 0$, and with $t = s$ we obtain the desired value.

Let us sequentially apply the Euclid algorithm to elements of the column $t'+1$ for some pairs of rows. We obtain the GCD in the column $t'+1$, subtracting the corresponding rows from each other (this is a particular case of the linear combination). Let us first calculate the GCD for rows $t' + 1$ and $t' + 2$. After determining the GCD in one row (modified by the algorithm), in column $t' + 1$ we get 0. We find the GSD for the remaining row and for row $t' + 3$. Proceeding this process for all j up to s we find the GSD for pairs of rows, one of which is the only row (among rows with numbers from $t' + 1$ to $j - 1$) whose $(t' + 1)$-st element differs from zero, and the other one is the jth row. Each time after calculating the GSD in one row modified by the algorithm, we get zero in it in the $(t' + 1)$-st place.

Thus, we have proved that among rows with numbers from $t' + 1$ to s there is only one row with a nonzero element at the $(t' + 1)$-st position. Now we can add it to row $t' + 1$ and then subtract from it the just obtained row $t' + 1$; thus we get a unique nonzero element in row $t' + 1$, which means that in column $t' + 1$ all elements located below the diagonal also equal zero.

Let us now describe the way in which we implement Step 3. We sequentially, for t varying from s to 1, perform the following operation: first we divide row t by its only nonzero element located on the diagonal and thus turn this element to 1. Then from each row from 1 to $t - 1$ we subtract row t multiplied by the tth element of the current row. Thus we make the tth row the only row whose tth element differs from zero. After performing this operation for $t = 1$ we obtain the unit matrix. □

Lemma 11. *Let the joint projection of a collection of functions $f_1(x), f_2(x), \ldots, f_s(x)$ have a uniform distribution. Then the joint projection of any subcollection $f_{i_1}, f_{i_2}, \ldots, f_{i_k}, 1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant s$, also has a uniform distribution.*

Proof. One can easily deduce the desired assertion from the definition, summing numbers of points in the corresponding volumes over all possible values of $a_j, 1 \leqslant j \leqslant n, j \notin \{i_1, i_2, \ldots, i_k\}$. □

Theorem 6. *Let $f(x)$ be an arbitrary polynomial with integer coefficients of a degree greater than 1, and let s be an arbitrary natural number. Then the s-dimensional projection of the polynomial $f(x)$ has a uniform distribution, and*

$$N^{x,f,\ldots,f^{(s-1)}}(\varepsilon) = \exp\{c_1\varepsilon^{-c_2}\}$$

for some positive c_1, c_2 depending only on the polynomial f.

Proof. Let the degree of $f^{(s-1)}(x)$ equal d. Evidently, no two polynomials in the set $x, f(x), f^{(2)}(x), \ldots, f^{(s-1)}(x)$ have one and the same degree. Let us add to this set arbitrary polynomials so as to make the resulting set contain exactly one polynomial of degree i for each $i, 1 \geqslant i \geqslant d$. In view of Theorem 5 (since the triangular matrix is nondegenerate), the joint projection of this set of functions has a uniform distribution. Since $x, f(x), f^{(2)}(x), \ldots, f^{(s-1)}(x)$ is its subset, in accordance with the previous lemma, the joint projection of this set also has a uniform distribution, which was to be proved.

Evidently, by excluding several f_i we will not increase N, therefore it holds

$$N^{x,f,\ldots,f^{(s-1)}}(\varepsilon) = \exp\{c_1\varepsilon^{-c_2}\}$$

for some positive c_1, c_2 depending only on the polynomial f. □

Corollary 1. *Resolving the mentioned bound with respect to ε and taking into account that $m = p^n$, one can easily obtain $D_m \leqslant c_1 \log\log m^{-c_2}$ for some positive c_1, c_2.*

10 Conclusion

In this paper we prove that the projection of any linearly independent (after eliminating free terms) collection of polynomials has a uniform distribution modulo p^n with $n \to \infty$ for any prime p. In particular, this is true for the projection of iterations of any polynomial, whose degree exceeds 2. In the case, when such a polynomial contains a complete cycle, the set of points, whose coordinates are s sequential terms of the recurrent sequence generated by this polynomial, also has a uniform distribution modulo p^n with $n \to \infty$ for any prime p.

The estimate of the convergence rate obtained in this paper is much weaker than that established for concrete classes of polynomials in [7],[8],[9]. In Definition 1 we use the discrepancy $\varepsilon = \sup|V(J) - F_n(J)|$ considered in the mentioned papers. The bounds proved in these papers allow us to obtain the main term of the asymptotics of ε in the form m^c, where $c = -1/2$ with some logarithmic corrections concordant with the repeated

logarithm law (note that there exist polynomials, for which this bound is violated, see [9]). The estimate for the convergence rate established in this paper allows us only to ascertain that the lower boundary for ε decreases being the double logarithm of the absolute value raised to some negative degree, which is essentially weaker.

In the following papers we intend to generalize the obtained result for the case of polynomials of many variables. Moreover, it seems possible to establish a criterion for preserving the uniformity of a collection of functions for a finite automaton and, therefore, to replace linear combinations (see Section 8) with a more general construction.

References

1. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences.* (Wiley, New York, 1974; Nauka, Moscow, 1985).

2. D.E. Knuth, *The Art of Computer Programming. Vol 2.* Vil'yams, Moscow – St. Petersburg. – Kiev, 2003 (Russ. transl.).

3. W. Feller, *An Introduction to Probability Theory and Its Applications.* Vol. 1. (John Wiley and Sons, Inc., New York, 1966; Mir, Moscow, 1984).

4. Anashin V., Khrennikov A. *Applied Algebraic Dynamics.* Vol. 49 of de Gruyter Expositions in Mathematics. Berlin—N.Y.: Walter de Gruyter GmbH & Co. 2009.

5. Blaželková O., Strauch O. Pseudo-randomness of quadratic generators *Uniform Distribution Theory* 2, **2** , pp. 105–120. 2007.

6. Drmota M., Tichy R.F. *Sequences, Discrepancies and Applications.*, Lecture Notes in Mathematics, **1651**, Berlin, Heidelberg: Springer-Verlag. 1997.

7. Eichenauer-Herrmann J. Quadratic congruential pseudorandom numbers: Distribution of lagged pairs. *J. Comput. Appl. Math.*, **79**, pp. 75–85. 1997.

8. Eichenauer-Herrmann J. Quadratic congruential pseudorandom numbers: distribution of triples. *J. Comput. Appl. Math.*, **62**, pp. 239–253. 1995.

9. Eichenauer-Herrmann J., Herrmann E., Wegenkittl S. *A survey of quadratic and inversive congruential pseudorandom numbers.* In H. Niederreiter, P. Hellekalek, G. Larcher, and P. Zinterhof, editors, Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics, **127**, pp. 66–97. Springer, New York, 1997.

10. Mahler K. *P-adic numbers and their functions.* Cambridge: Cambridge University Press, 1981.