PSEUDORANDOM NUMBER GENERATION BY p-ADIC ERGODIC TRANSFORMATIONS

VLADIMIR ANASHIN

Abstract. The paper study counter-dependent pseudorandom generators; the latter are generators such that their state transition function (and output function) is being modified dynamically while working: For such a generator the recurrence sequence of states satisfies a congruence $x_{i+1} \equiv f_i(x_i) \pmod{2^n}$, while its output sequence is of the form $z_i = F_i(x_i)$. The paper introduces techniques and constructions that enable one to compose generators that output uniformly distributed sequences of a maximum period length and with high linear and 2-adic spans. Some evidence is given that the corresponding stream chipher could be provably strong against a known plaintext attack (up to a plausible conjecture). Both state transition function and output function could be key-dependent, so the only information available to a cryptanalyst is that these functions belong to some (exponentially large) class. These functions are compositions of standard machine instructions (such as addition, multiplication, bitwise logical operations, etc.) The compositions should satisfy rather loose conditions; so the corresponding generators are flexible enough and could be easily implemented as computer programs.

1. Introduction

The study of ergodic, measure-preserving and equiprobable functions on the space $\mathbb{Z}_p$ of p-adic integers in [6, 16, 7, 11] was mainly motivated by possible applications to pseudorandom number generation for cryptography and simulation. In the present paper we consider generators based on these functions, *prove* that the produced sequences have some (properly defined below) 'features of randomness', and calculate *exact* values of certain (crucial for cryptographic security) parameters of these generators. Namely, we characterize all possible output sequences in the class of all sequences, calculate exact lengths of their periods, distribution of overlapping and non-overlapping k-tuples, linear complexity, and p-adic span. Also, we demonstrate that with the use of these functions it is possible to construct a stream cipher such that to recover its key is an infeasible problem (up to some plausible conjectures).

In fact, the paper introduces certain techniques and constructions that enable one to design stream ciphers with both state transition and output functions depending on key; yet *independently of key choice* the corresponding generator always provides predefined values of output sequence parameters, which are mentioned above. These functions are (key-dependent) compositions of (standard) machine instructions: arithmetic ones, such as addition and multiplication (exponentiation and raising to negative powers as well), logical ones, such as XOR, OR, AND, NEG, etc.,

---

1991 *Mathematics Subject Classification.* 11K45, 94A60, 68P25, 65C10.

Key words and phrases. Pseudorandom generator, counter-dependent generator, ergodic transformation, equiprobable function, p-adic analysis.

and others (e.g., shifts, masking). Thus, generators of this kind admit quite natural implementation as a computer program. Such generators are rather flexible: To obtain due performance a programmer could vary length of the composition and choice of machine instructions *without* affecting the above mentioned probabilistic and cryptographic characteristics.

Further, focusing on these ideas we introduce counter-dependent generators; the latter are generators such that their state transition function (and output function) is being modified dynamically while working. To be more exact, for these generators the recurrence sequence of states satisfies a congruence $x_{i+1} \equiv f_i(x_i) \pmod{2^n}$, while their output sequence is of the form $z_i = F_i(u_i)$. Note that both state transition function f_i and output function F_i depend on the number i of a step; yet newertheless the output sequence is purely periodic, its period length is a multiple of 2^n, distribution of k-tuples, $k \le n$ is uniform, its linear complexity is high, etc. Moreover, not only f_i and F_i themselves could be keyed, but also the order they are used during encryption. [1]

To give an idea of how these schemes look like, consider the following example of a counter-dependent generator modulo 2^n. Take arbitrary $m \equiv 3 \pmod 4$, then take m *arbitrary* compositions $v_0(x), \dots, v_{m-1}(x)$ of the above mentioned machine instructions (addition, multiplication, XOR, AND, etc.) and constants, then take another m *arbitrary* compositions $w_0(x), \dots, w_{m-1}(x)$ of this kind. Arrange two arrays V and W writing these $v_j(x)$ and $w_j(x)$ to memory in *arbitrary* order. Now choose arbitrary $x_0 \in \{0, 1, \dots 2^n - 1\}$ as a seed. The generator calculates the recurrence sequence of states $x_{i+1} = (i \bmod m + x_i + 2 \cdot (v_{i \bmod m}(x_i + 1) - v_{i \bmod m}(x_i))) \bmod 2^n$ and outputs the sequence $z_i = (1 + \pi(x_i) + 2 \cdot (w_{i \bmod m}(\pi(x_i) + 1) - w_{i \bmod m}(\pi(x_i)))) \bmod 2^n$, where π is a bit order reversing permutation, which reads an n-bit number $x \in \{0, 1, \dots, 2^n - 1\}$ in a reverse bit order; e.g., $\pi(0) = 0, \pi(1) = 2^{n-1}, \pi(2) = 2^{n-2}, \pi(3) = 2^{n-2} + 2^{n-1}$, etc. Then the sequence $\{x_i\}$ is a purely periodic sequence of period length $2^n m$ of n-bit numbers, and each number of $\{0, 1, \dots, 2^n - 1\}$ occurs at the period exactly m times. Moreover, if we consider $\{x_i\}$ as a binary sequence of period length $2^n mn$, then the frequency each k-tuple $(0 < k \le n)$ occurs in the sequence is exactly $\frac{1}{2^k}$. The output sequence $\{z_i\}$ is also purely periodic of period length $2^n m$, and each number of $\{0, 1, \dots, 2^n - 1\}$ occurs at the period exactly m times either. Moreover, every binary sequence obtained by reading each s^{th} bit $\delta_s(z_i)$ $(0 \le s \le n-1)$ of the output sequence is purely periodic; its period length is a multiple of 2^n, hence its linear complexity (as well as the one of the whole sequence $\{z_i\}$) exceeds 2^{n-1}.

In fact, for such stream encryption schemes the only information available to a cryptanalist is that both the output and the state transition functions belong to a

---

[1] The notion of a counter-dependent generator was originally introduced in [13]. However, in our paper we consider this notion in a broader sense: In our counter-dependent generators not only the state transition function, but also the output function depends on i. Moreover, in [13] only a particular case of counter-dependent generators is studied; namely, counter-assisted generators and their cascaded and two-step modifications. A state transition function of a counter-assisted generator is of the form $f_i(x) = i \star h(x)$, where $\star$ is a binary quasigroup operation (in particular, group operation, e.g., $+$ or XOR), and $h(x)$ does not depend on i. An output function of a counter-assisted generator does not depend on i either. The main security notion studied in [13] is diversity, which generalizes a concept of long cycles. Note that all our generators achieve maximum possible total diversity, which is equal to the order of the output set.

certain (exponentially large) class of functions, and practically nothing more. Thus, practical attacks to such stream encryption scheme seem to be ineffective.

We must immediately note here that, strictly speaking, all these results give some evidence, yet *not the proof* of cryptographic security of these ciphers. We recall, however, that today for no stream cipher based on deterministic algorithm there exists an unconditional mathematical proof of security. We ought to emphasize also that the study of stream encryption schemes below should not be considered as an exaustive cryptographic analysis. The latter one implies a study of attacks against a particular scheme, which numerical parameters have exact predefined values. Loosely speaking, further results could be considered as a 'toolkit' for a stream cipher designer, but *not* as 'make-it-yourself kit': The latter implies detailed 'assemble instructions'; following them guarantees an adequate quality of the whole thing. No such instructions are given in the present paper, only some ideas and hints.

The paper is organized as follows:

- In Section 2 we introduce some basic notions, consider standard machine instructions as continous 2-adic mappings, describe their properties and prove that under certain very loose conditions the output sequence will be uniformly distributed.
- In Section 3 we state a number of results that enable one to construct permutations with a single cycle and equiprobable functions out of standard machine instructions. Moreover, as examples of how these techniques work we reprove some of known results in this area, as well as establish new ones.
- In Section 4 we outline several ways of combining functions described in Section 3 in automaton that generates uniformly distributed sequence. There we introduce a new construction (called wreath product of automata, by analogy with a corresponding group theory construction) that enables one to build counter-dependent generators with uniformly distributed output sequences of a maximum period length.
- In Section 5 we study complexity and distribution of output sequences of automata introduced in Section 4: Linear and 2-adic spans of these sequences, their structure, distribution of k-tuples in them, etc. In particular, we prove that distribution of (overlapping) k-tuples is strictly uniform; namely, that these output sequences have a property that could be called a generalized De Bruijn: Being considered as binary sequences, they are purely periodic, their period lengths are multiples of 2^n, and each k-tuple ($k \le n$) occurs at the period the same number of times. From here we deduce that a large class of these sequences satisfy Knuth's criterion Q1 [2] of randomness.
- In Section 6 we demonstrate how to construct a stream cipher with intractable key recovery problem conjecturing that a set of k multivariate Boolean polynomials define a one-way function (it is known that to determine whether a system of k Boolean polynomials in n variables has a common zero is an NP-complete problem [3]).

---

[2] See [2, Section 3.5, Definition Q1]

[3] See e.g. [26, Appendix A, Section A7.2, Problem ANT-9]

2. PRELIMINARIES

Basically, a generator we consider in the paper is a finite automaton $\mathfrak{A} = \langle N, M, f, F, u_0\rangle$ with a finite state set N, state transition function $f : N \to N$, finite output alphabet M, output function $F : N \to M$ and an initial state (seed) $u_0 \in N$. Thus, this generator produces a sequence

$$\mathcal{S} = \{F(u_0), F(f(u_0)), F(f^{(2)}(u_0)), \ldots, F(f^{(j)}(u_0)), \ldots\}$$

over the set M, where

$$f^{(j)}(u_0) = \underbrace{f(\ldots f(}_{j \text{ times}} u_0)\ldots) \quad (j = 1, 2, \ldots); \quad f^{(0)}(u_0) = u_0.$$

Automata of the form $\mathfrak{A}$ will be considered either as pseudorandom generators per se, or as components of more complicated pseudorandom generators, which are introduced in Section 4; the latter produce pseudorandom sequences $\{z_0, z_1, z_2, \ldots\}$ over M according to the rule

$$z_0 = F_0(u_0), u_1 = f_0(u_0); \ldots z_i = F_i(u_i), u_{i+1} = f_i(u_i); \ldots$$

That is, at the $(i+1)^{\text{th}}$ step the automaton $\mathfrak{A}_i = \langle N, M, f_i, F_i, u_i\rangle$ is applied to the state $u_i \in N$, producing a new state $u_{i+1} = f_i(u_i) \in N$, and outputting a symbol $z_i = F_i(u_i) \in M$.

Quite often in the paper we assume that $N = \mathbb{I}_n(p) = \{0, 1, \ldots, p^n - 1\}$, $M = \mathbb{I}_m(p)$, $m \le n$, where p is (usually a prime) positive rational integer greater than 1. Moreover, mainly we are focused on the case $p = 2$ as the most convenient for computer implementations, and use a shorter notation $\mathbb{I}_n$ instead of $\mathbb{I}_n(2)$. As a rule, further we formulate results mainly for this case, making brief remarks for those of them that remain true for arbitrary p.

Now let $n = km > 1$ (may be, $k = 1$) be a positive rational integer. Let the state set N of the above mentioned automaton $\mathfrak{A}$ be $\mathbb{I}_n = \{0, 1, \ldots, 2^n - 1\}$. Further we will identify the set $\mathbb{I}_n$ either with the set of all elements of the residue class ring $\mathbb{Z}/2^n$ of integers modulo 2^n, or with a set $\mathbb{W}_n(2)$ of all n-bit words in the alphabet $\mathbb{I} = \mathbb{I}_1 = \{0, 1\}$, or with a set of all elements of a direct product

$$(\mathbb{Z}/2^m)^{(k)} = \underbrace{\mathbb{Z}/2^m \times \cdots \times \mathbb{Z}/2^m}_{k \text{ times}}$$

of k copies of the residue class ring $\mathbb{Z}/2^m$, or with a set $\mathbb{W}_k(2^m)$ of all words of length k in the alphabet $\mathbb{I}_m$. In other words, if necessary, we may treat a number $i \in \{0, 1, \ldots, 2^n - 1\}$ either as an n-bit word, or as a k-tuple of numbers of $\{0, 1, \ldots, 2^m - 1\}$, or as a k-tuple of m-bit blocks.

To be more exact, let $\delta_j^m(i) \in \mathbb{I}_m$ be the j^{th} digit of a number i in its base-2^m expansion: that is, if $i = i_0 + i_1 \cdot 2^m + i_2 \cdot (2^m)^2 + \ldots$, where $i_j \in \mathbb{I}_m$, $j = 0, 1, 2, \ldots$, then, by definition, $\delta_j^m(i) = i_j$. (For $m = 1$ we usually omit the superscript, when this does not lead to misunderstanding). With these notations, if $i \in \mathbb{I}_n$, then the word $w_k(i) \in \mathbb{W}_k(2^m)$ is a concatent $\delta_0^m(i) \ldots \delta_{k-1}^m(i)$, and a corresponding element $r_k(i) \in (\mathbb{Z}/2^m)^{(k)}$ is $r_k(i) = (\delta_0^m(i), \ldots, \delta_{k-1}^m(i))$. Thus, for each $i \in \mathbb{I}_n$ and for arbitrary mappings $F : (\mathbb{Z}/2^m)^{(k)} \to \mathbb{Z}/2^m$ and $G : \mathbb{W}_n(2) \to \mathbb{W}_k(2^m)$ the expressions $F(i)$ and $G(i)$ are correctly defined: namely, $F(i)$ stands for $F(r_k(i))$, $G(i)$ stands for $G(w_k(i))$. In view of the above mentioned bijections between $\mathbb{I}_m$ and $\mathbb{Z}/2^m$, both $F(i)$ and $G(i)$ may be considered as elements of $\mathbb{I}_m$ and $\mathbb{I}_n$, respectively.

We will need a particular mapping $\pi_s^t : \mathbb{W}_s(2^t) \to \mathbb{W}_s(2^t)$, an order reversing permutation: $\pi_s^t(u_0u_1\ldots u_{s-1}) = u_{s-1}u_{s-2}\ldots u_0$, where $u_0,\ldots,u_{s-1} \in \mathbb{I}_t$. In view of the above conventions, for each $i \in \mathbb{I}(2^n)$ the following expressions are well defined: $\pi_k^m(i), \pi_n^1(i) \in \mathbb{I}_n$ and $\pi_m^1(\delta_j^m(i)) \in \mathbb{I}_m$. In other words, $\pi_n^1(i)$ reads base-2 expansion of i in reverse order, while $\pi_k^m(i)$ reads base-2^m expansion of i in reverse order; e.g. $\pi_4^1(7) = 14$, $\pi_2^2(7) = 13$. Often, when it is clear within a context, we omit a superscript (sometimes together with a subscript) in π_k^m.

Note that functions $\pi_k^m, \pi_n^1, \delta_j^m$, being compositions of arithmetic and logical operators, are easily programmable: so $\delta_j^m(i) = \frac{i\,\mathsf{AND}(2^{mj}(2^m-1))}{2^{mj}}$ (in particular $\delta_j^1(i) = \frac{i\,\mathsf{AND}(2^j)}{2^j}$) is a composition of AND (bitwise logical multiplication, bitwise conjunction) and left and right shifts, $\pi_n^1(i) = \delta_{n-1}^1(i) + \delta_{n-2}^1(i)\cdot 2 + \cdots + \delta_0^1(i)\cdot 2^{n-1}$. Note that for certain m, n both $\delta_j^m(i)$ and $\pi_n^1(i)$ are just a machine instruction (e.g., 'read j^{th} memory cell', the latter assumed to be m-bit) or with use of writing to and reading from memory. For instance, byte order reversing permutation π_k^8 could be implemented with the use of stack writing-reading, whereas π_8^1 could be stored in memory as one-dimensional byte array (the i^{th} byte is $\pi_8^1(i)$); then π_k^8 and π_8^1 could be combined in an easy program to obtain π_n^1. Also we notice that in fact one uses the mapping π_n^1 in simulation tasks when he converts integer output $s_0, s_1, \ldots$ ($s_i \in \{0, 1, \ldots, 2^n - 1\}$) of a pseudorandom number generator into real numbers $\{\frac{s_0}{2^n}, \frac{s_1}{2^n}, \ldots\}$ of unit interval.

It worth mentioning here that, according to the above settled conventions, we can consider bitwise logical operators (such as XOR, AND, etc.) as functions defined on the set $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$: We merely represent variables in their base-2 expansions (e.g., $1\,\mathsf{XOR}\,3 = 2$, $1\,\mathsf{AND}\,3 = 1$). An m-bit right shift is just a multiplication by 2^m, whereas an m-bit left shift is integer division by 2^m, i.e., $\lfloor \frac{\cdot}{2^m} \rfloor$, with $\lfloor \alpha \rfloor$ being the greatest rational integer that does not exceed α. Note that throughout the paper we represent integers i in reverse bit order — less significant bits left, according to their occurrences in 2-adic canonical representation of $i = \delta_0(i) + \delta_1(i)\cdot 2 + \delta_2(i)\cdot 4 + \ldots$; so 0011 is 12, and not 3.

Functions π_s^t together with arithmetic operations (addition and multiplication) as well as bitwise logical operations (such as XOR, AND) and other "machine" ones (such as left and right shifts) are "building blocks" of pseudorandom generators studied below, so for reader's convenience we list the corresponding operators here, supplying them by definitions and comments, if necessary.

Bitwise logical operators are defined by the following congruences, which must hold for all $u, v \in \mathbb{N}_0$ (or, equivalently, for all $u, v \in \mathbb{Z}_2$) and for all $j = 0, 1, 2, \ldots$.

$$
\begin{aligned}
&\mathsf{XOR},\ \text{or}\ \oplus\ \text{, a bitwise 'exclusive or' operator: } \delta_j(u\,\mathsf{XOR}\,v) \equiv \\
&\delta_j(u) + \delta_j(v) \pmod 2; \\
&\mathsf{AND},\ \text{or}\ \wedge\ \text{, a bitwise 'and' operator, bitwise conjunction: } \delta_j(u\,\mathsf{AND}\,v) \equiv \\
&\delta_j(u)\cdot\delta_j(v) \pmod 2; \\
&\mathsf{OR},\ \text{or}\ \vee\ \text{, a bitwise 'or' operator, bitwise disjunction: } \delta_j(u\,\mathsf{OR}\,v) \equiv \\
&\delta_j(u) + \delta_j(v) + \delta_j(u)\cdot\delta_j(v) \pmod 2; \\
&\mathsf{NEG},\ \text{or}\ \neg\text{, a bitwise negation: } \delta_j(\mathsf{NEG}(u)) \equiv \\
&\delta_j(u) + 1 \pmod 2.
\end{aligned}
\tag{2.0.1}
$$

The other bitwise logical operators (originating from e.g. implication, etc.) could be defined by the analogy.

Note that all these operators are defined on the set $\mathbb{N}_0$ of non-negative rational integers. Moreover, they are defined on the set $\mathbb{Z}_2$ of all 2-adic integers (see [6, 16]). The latter ones within the context of this paper could be thought of as countable infinite binary sequences with members indexed by $0, 1, 2, \ldots$. Sequences with only finite number of 1's correspond to non-negative rational integers in their base-2 expansions, sequences with only finite number of 0's correspond to negative rational integers, while eventually periodic sequences correspond to rational numbers represented by irreducible fractions with odd denominators: for instance, $3 = 11000\ldots$, $-3 = 10111\ldots$, $\frac{1}{3} = 11010101\ldots$, $-\frac{1}{3} = 101010\ldots$. So $\delta_j(u)$ for $u \in \mathbb{Z}_2$ is merely the j^{th} member of the corresponding sequence.

Arithmetic operations (addition and multiplication) with these sequences could be defined via standard algorithms of addition and multiplication of natural numbers represented in base-2 expansions: Each member of a sequence, which corresponds to a sum (respectively, to product) of two given sequences, will be calculated by these algorithms within a finite number of steps.

Thus, $\mathbb{Z}_2$ is a commutative ring with respect to the so defined addition and multiplication. It is a metric space with respect to the distance $d_2(u, v)$ defined by the following rule: $d_2(u, v) = \|u - v\|_2 = \frac{1}{2^n}$, where n is the smallest non-negative rational integer such that $\delta_n(u) \neq \delta_n(v)$, and $d_2(u, v) = 0$ if no such n exists (i.e., if $u = v$). For instance $d_2(3, \frac{1}{3}) = \frac{1}{8}$. With the use of this distance it is possible to define convergent sequences, limits, continuous functions and derivatives in $\mathbb{Z}_2$.

For instance, with respect to the so defined distance, the folowing sequence tends to -1,

$$1, 3, 7, 15, 31, \ldots, 2^n - 1, \ldots \xrightarrow[d_2]{} -1,$$

bitwise logical operators (such as $\mathsf{XOR}, \mathsf{AND}$) define continuous functions in two variables, the function $f(x) = x \,\mathsf{XOR}\, a$ is differentiable everywhere on $\mathbb{Z}_2$ for every rational integer a: Its derivative is -1 for negative a, and 1 in the opposite case (see 3.22 for other examples of this kind and more detailed calculations).

Reduction modulo 2^n of a 2-adic integer v, i.e., setting all members of the corresponding sequence with indexes greater than $n - 1$ to zero (that is, taking the first n digits in the representation of v) is just an approximation of a 2-adic integer v by a rational integer with accuracy $\frac{1}{2^n}$: This approximation is an n-digit positive rational integer $v \,\mathsf{AND}(2^n - 1)$; the latter will be denoted also as $v \bmod 2^n$. For formal introduction to p-adic analysis, precise notions and results see e.g. [3] or [4].

Arithmetic and bitwise logical operations are not independent: Some of them could be expressed via the others. For instance, for all $u, v \in \mathbb{Z}_2$

$$\begin{aligned} &\mathsf{NEG}(u) = u \,\mathsf{XOR}(-1); \\ &\mathsf{NEG}(u) + u = -1; \\ &u \,\mathsf{XOR}\, v = u + v - 2(u \,\mathsf{AND}\, v); \\ &u \,\mathsf{OR}\, v = u + v - (u \,\mathsf{AND}\, v); \\ &u \,\mathsf{OR}\, v = (u \,\mathsf{XOR}\, v) + (u \,\mathsf{AND}\, v). \end{aligned} \tag{2.0.2}$$

Proofs of these identities (2.0.2) are just an exercise: For example, if $\alpha, \beta \in \{0,1\}$ then $\alpha \oplus \beta = \alpha + \beta - 2\alpha\beta$ and $\alpha \vee \beta = \alpha + \beta - \alpha\beta$. Hence:

$$u \,\mathsf{XOR}\, v = \sum_{i=0}^{\infty} 2^i(\delta_i(u) \oplus \delta_i(v)) = \sum_{i=0}^{\infty}\sum_{i=0}^{\infty} 2^i(\delta_i(u) + \delta_i(v) - 2\delta_i(u)\delta_i(v)) =$$

$$\sum_{i=0}^{\infty} 2^i(\delta_i(u)) + \sum_{i=0}^{\infty} 2^i(\delta_i(v)) - 2 \cdot \sum_{i=0}^{\infty} 2^i(\delta_i(u)\delta_i(v)) = u + v - 2(u \,\mathsf{AND}\, v).$$

Proofs of the rest identities could be made by analogy and thus are omitted. Right shift (towards more significant digits), as well as masking and reduction modulo 2^m could be derived from the above operations: An m-step shift of u is $2^m u$; masking of u is $u \,\mathsf{AND}\, M$, where M is an integer, which base-2 expansion is a mask (i.e., a string of 0's and 1's); reduction modulo 2^m, i.e., taking the least non-negative residue of u modulo 2^m is $u \bmod 2^m = u \,\mathsf{AND}(2^m - 1)$.

A common feature the above mentioned arithmetic, bitwise logical and mashine operations share is that they all, with the only exception of shifts towards less significant bits, are *compatible*, i.e. $\omega(u,v) \equiv \omega(u_1,v_1) \pmod{2^r}$ whenever both congruences $u \equiv u_1 \pmod{2^r}$ and $v \equiv v_1 \pmod{2^r}$ hold simultaneously. The notion of a compatible mapping could be naturally generalized to mappings $(\mathbb{Z}/p^l)^{(t)} \to (\mathbb{Z}/p^l)^{(s)}$ and $(\mathbb{Z}_p)^{(t)} \to (\mathbb{Z}_p)^{(s)}$; compatible mappings of the latter kind could be also considered as those satisfying Lipschitz condition with coefficient 1 (with respect to p-adic distance), see [16]. Obviously, a composition of compatible mappings is a compatible mapping. We list now some important examples of compatible operators $(\mathbb{Z}_p)^{(t)} \to (\mathbb{Z}_p)^{(s)}$, p prime (see [16]). Part of them originates from arithmetic operations:

$$\begin{aligned}
&\text{multiplication}, \cdot: \ (u,v) \mapsto uv;\\
&\text{addition}, +: \ (u,v) \mapsto u+v;\\
&\text{subtraction}, -: \ (u,v) \mapsto u-v;\\
&\text{exponentiation}, \ \uparrow_p: \ (u,v) \mapsto u \uparrow_p v = (1+pu)^v; \ \text{in particular,}\\
&\text{raising to negative powers}, \ u \uparrow_p (-r) = (1+pu)^{-r}, r \in \mathbb{N}; \ \text{and}\\
&\text{division}, \ /_p : u/_p v = u \cdot (v \uparrow_p (-1)) = \frac{u}{1+pv}.
\end{aligned} \tag{2.0.3}$$

The other part originates from digitwise logical operations of p-valued logic:

$$\begin{aligned}
&\text{digitwise multiplication } u \odot_p v : \delta_j(u \odot_p v) \equiv \delta_j(u)\delta_j(v) \pmod{p};\\
&\text{digitwise addition } u \oplus_p v : \delta_j(u \oplus_p v) \equiv \delta_j(u) + \delta_j(v) \pmod{p};\\
&\text{digitwise subtraction } u \ominus_p v : \delta_j(u \ominus_p v) \equiv \delta_j(u) - \delta_j(v) \pmod{p}.
\end{aligned} \tag{2.0.4}$$

Here $\delta_j(z)$ $(j = 0,1,2,\ldots)$ stands for the j^{th} digit of z in its base-p expansion.

More compatible mappings could be derived from the above mentioned ones. For instance, a reduction modulo p^n, $n \in \mathbb{N}$, is $u \bmod p^n = u \odot_p \frac{p^n-1}{p-1}$, an l-step shift towards more significant digits is just a multiplication by p^l, etc. Obviously, $u \odot_2 v = u \,\mathsf{AND}\, v$, $u \oplus_2 v = u \,\mathsf{XOR}\, v$.

In case $p = 2$ compatible mappings could be characterized in terms of Boolean functions. Namely, each mapping $T\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ could be considered as an ensemble of n Boolean functions $\tau_i^T(\chi_0,\ldots,\chi_{n-1})$, $i = 0,1,2,\ldots,n-1$, in n Boolean variables $\chi_0, \dots, \chi_{n-1}$ by assuming $\chi_i = \delta_i(u)$, $\tau_i^T(\chi_0, \dots, \chi_{n-1}) = \delta_i(T(u))$ for u running from 0 to $2^n - 1$. The following proposition holds.

2.1. **Proposition.** ([6, Proposition 3.9]) *A mapping* $T\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ (*accordingly, a mapping* $T\colon \mathbb{Z}_2 \to \mathbb{Z}_2$) *is compatible iff each Boolean function* $\tau_i^T(\chi_0, \chi_1, \dots) = \delta_i(T(u))$, $i = 0, 1, 2, \dots$, *does not depend on variables* $\chi_j = \delta_j(u)$ *for* $j > i$.

Note. Mappings satisfying conditions of the proposition are also known as *triangle* mappings. The proposition after proper restatement (in terms of functions of p-valued logic) also holds for odd prime p. For multivariate mappings the theorem 2.1 holds either: a mapping $T = (t_1, \dots, t_s)\colon (Z_2)^{(r)} \to (Z_2)^{(s)}$ is compatible iff each Boolean function $\tau_i^{t_j}(\chi_{1,0}, \chi_{1,1}, \dots, \chi_{r,0}, \chi_{r,1}, \dots) = \delta_i(t_k(u, \dots, u_r))$ ($i = 0, 1, 2, \dots$, $k = 0, 1, \dots, s$) does not depend on variables $\chi_{\ell,j} = \delta_j(u_\ell)$ for $j > i$ ($\ell = 1, 2, \dots, r$).

Now, given a compatible mapping $T\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, one can define an induced mapping $T \bmod 2^n\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ by assuming $(T \bmod 2^n)(z) = T(z) \bmod 2^n = (T(z))\,\mathsf{AND}(2^n - 1)$ for $z = 0, 1, 2, \dots, 2^n - 1$. The induced mapping is obviuosly a compatible mapping of the ring $\mathbb{Z}/2^n$ into itself. For odd prime p, as well as for multivariate case $T\colon (\mathbb{Z}_p)^{(s)} \to (\mathbb{Z}_p)^{(t)}$ an induced mapping $T \bmod p^n$ could be defined by the analogy.

2.2. **Definition.** (See [16]). We call a compatible mapping $T\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *bijective modulo* p^n iff the induced mapping $T \bmod p^n$ is a permutation on $\mathbb{Z}/p^n$; we call T *transitive modulo* p^n, iff $T \bmod p^n$ is a permutation with a single cycle. We say that T is *measure-preserving* (respectively, *ergodic*), iff T is bijective (respectively, transitive) modulo p^n for all $n \in \mathbb{N}$. We call a compatible mapping $T\colon (\mathbb{Z}_p)^{(s)} \to (\mathbb{Z}_p)^{(t)}$ *equiprobable modulo* p^n iff the induced mapping $T \bmod p^n$ maps $(\mathbb{Z}/p^n)^{(s)}$ onto $(\mathbb{Z}/p^n)^{(t)}$, and each element of $(\mathbb{Z}/p^n)^{(t)}$ has the same number of preimages in $(\mathbb{Z}/p^n)^{(s)}$. A mapping $T\colon (\mathbb{Z}_p)^{(s)} \to (\mathbb{Z}_p)^{(t)}$ is called *equiprobable* iff it is equiprobable modulo p^n for all $n \in \mathbb{N}$.

Note. The terms measure-preserving, ergodic and equiprobable originate from the theory of dynamical systems. Namely, the compatible mapping $T\colon \mathbb{Z}_p \to \mathbb{Z}_p$ defines a dynamics on the measurable space $\mathbb{Z}_p$ with a probabilistic measure that is normalized Haar measure. The mapping T is, e.g., ergodic with respect to this measure (in the sence of the theory of dynamical systems) iff it satisfies 2.2, see [16] for details.

Both transitive modulo p^n and equiprobable modulo p^n mappings will be used as building blocks of pseudorandom generators to provide both large period length and uniform distribution of output sequences. The following obvious proposition holds.

2.3. **Proposition.** *If the state transition function* f *of the automaton* $\mathfrak{A}$ *is transitive on the state set* N, *i.e., if* f *is a permutation with a single cycle of length* $|N|$, *if, further,* $|N|$ *is a multiple of* $|M|$, *and if the output function* $F : N \to M$ *is equiprobable* (*i.e.,* $|F^{-1}(s)| = |F^{-1}(t)|$ *for all* $s, t \in M$), *then the output sequence* $\mathfrak{S}$ *of the automaton* $\mathfrak{A}$ *is purely periodic with period length* $|N|$ (i.e., maximum possible), *and each element of* M *occurs at the period the same number of times:* $\frac{|N|}{|M|}$ *exactly.* That is, the output sequence $\mathfrak{S}$ is uniformly distributed.

2.4. **Definition.** Further in the paper we call a sequence $\{s_i \in M\}$ over a finite set M *strictly uniformly distributed* iff it is purely periodic with period length t, and with every element of M occuring at the period the same number of times, i.e., exactly $\frac{t}{|M|}$. A sequence $\{s_i \in \mathbb{Z}_p\}$ of p-adic integers is called *strictly uniformly distributed modulo* p^k iff a sequence $\{s_i \bmod p^k\}$ of residues modulo p^k is strictly uniformly distributed over a residue ring $\mathbb{Z}/p^k$. Also, we say that a sequence is purely periodic of period length *exactly* t iff it has no periods of lengths smaller than t. In this case t is called the *exact period length* of the sequence.[4]

Note. A sequence $\{s_i \in \mathbb{Z}_p : i = 0, 1, 2, \ldots\}$ of p-adic integers is uniformly distributed (with respect to a normalized Haar measure μ on $\mathbb{Z}_p$) [5] iff it is uniformly distributed modulo p^k for all $k = 1, 2, \ldots$; that is, for every $a \in \mathbb{Z}/p^k$ relative numbers of occurences of a in the initial segment of length ℓ in the sequence $\{s_i \bmod p^k\}$ of residues modulo p^k are asymptotically equal, i.e., $\lim_{\ell\to\infty} \frac{A(a,\ell)}{\ell} = \frac{1}{p^k}$, where $A(a, \ell) = |\{s_i \equiv a \pmod{p^k} : i < \ell\}|$(see [1] for details). So strictly uniformly distributed sequences are uniformly distributed in the common sence of theory of distributions of sequences.

Thus, putting $N = \mathbb{Z}/2^n, M = \mathbb{Z}/2^m, n = km$, and taking as f and F respectively, $f = \overline{f} = \widetilde{f} \bmod 2^n$ and $F = \overline{F} = \widetilde{F} \bmod 2^m$, where the function $\widetilde{f} : \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatible and ergodic, and the function $\widetilde{F} : (\mathbb{Z}_2)^{(k)} \to \mathbb{Z}_2$ is compatible and equiprobable, we obtain an automaton that generates a uniformly distributed periodic sequence, and the length of a period of this sequence is 2^n. That is, each element of $\mathbb{Z}/2^m$ occurs at the period the same number of times (namely, 2^{n-m}). Obviously, the conclusion holds if one takes as F an arbitrary composition of the function $\overline{F} = \widetilde{F} \bmod 2^m$ and an equiprobable function: for instance, one may put $F(i) = \overline{F}(\pi_n(i))$ or $F(i) = \delta^m_j(i)$, etc. Also, the assertion is true for odd prime p either. Since all the automata considered further in the paper are of this kind, their output sequences (considered as sequences over $\mathbb{Z}/p^m$) are uniformly distributed purely periodic sequences, and the length of their periods is p^n, *independently of choise* both of the function $\widetilde{f}$ and of the function $\widetilde{F}$. So, the proposition 2.3 makes it possible to vary both the state transition and the output functions (for instance, to make them key-dependent) *without* affecting uniform distribution of the output sequence.

Of course, to make all this practicable, one needs to choose these functions f and F from suitably large classes of ergodic and equiprobable functions. In other words, one has to obtain certain tools to produce a number of various measure preserving, ergodic, and equprobable mappings out of elementary compatible functions like (2.0.1) and (2.0.3). We consider these tools in the next section, as well as give some estimates of how the produced classes are big.

3. Tools

In this section we introduce various techniques that enable one to construct measure preserving and/or ergodic mappings, as well as to verify whether a given mapping is measure preserving or, respectively, ergodic. We are mainly focused at the class of compatible mappings.

Using interpolation series and polynomials. The general characterization of compatible ergodic functions is given by the following

---

[4] An exact period length is also called *the smallest period* of a sequence. We do not use this term to avoid misunderstanding, since we consider a period as a repeating part of a sequence.

[5] i.e., $\mu(a + p^k\mathbb{Z}_p) = p^{-k}$ for all $a \in \mathbb{Z}_p$ and all $k = 0, 1, 2 \ldots$

3.1. **Theorem.** ([6],[7]) *A function* $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *is compatible iff it could be represented as*

$$f(x) = c_0 + \sum_{i=1}^{\infty} c_i\, 2^{\lfloor \log_2 i \rfloor} \binom{x}{i} \qquad (x \in \mathbb{Z}_2);$$

The function f *is compatible and measure-preserving iff it could be represented as*

$$f(x) = c_0 + x + \sum_{i=1}^{\infty} c_i\, 2^{\lfloor \log_2 i \rfloor + 1} \binom{x}{i} \qquad (x \in \mathbb{Z}_2);$$

The function f *is compatible and ergodic iff it could be represented as*

$$f(x) = 1 + x + \sum_{i=1}^{\infty} c_i 2^{\lfloor \log_2 (i+1) \rfloor + 1} \binom{x}{i} \qquad (x \in \mathbb{Z}_2),$$

where $c_0, c_1, c_2 \ldots \in \mathbb{Z}_2$.

Here, as usual,

$$\binom{x}{i} = \begin{cases} \dfrac{x(x-1)\cdots(x-i+1)}{i!}, & \text{for } i = 1, 2, \ldots; \\ 1, & \text{for } i = 0, \end{cases}$$

and $\lfloor \alpha \rfloor$ is the integral part of α, i.e., the largest rational integer not exceeding α. *Note.* For odd prime p an analogon of the statement of theorem 3.1 provides only sufficient conditions for ergodicity (resp., measure preservation) of f: namely, if $(c_0, p) = 1$, i.e., if c is a unit (=invertible element) of $\mathbb{Z}_p$, then the function $f(x) = c + x + \sum_{i=1}^{\infty} c_i p^{\lfloor \log_p (i+1) \rfloor + 1} \binom{x}{i}$ defines a compatible and ergodic mapping of $\mathbb{Z}_p$ onto itself, and the function $f(x) = c_0 + c \cdot x + \sum_{i=1}^{\infty} c_i p^{\lfloor \log_p i \rfloor + 1} \binom{x}{i}$ defines a compatible and measure preserving mapping of $\mathbb{Z}_p$ onto itself see [16, Theorem 2.4].

Thus, in view of theorem 3.1 one can choose a state transition function to be a polynomial with rational (not necessarily integer) key-dependent coefficients setting $c_i = 0$ for all but finite number of i. Note that to determine whether a given polynomial f with rational (and not necessarily integer) coefficients is integer valued (that is, maps $\mathbb{Z}_p$ into itself), compatible and ergodic, it is sufficient to determine whether it induces a cycle on $O(\deg f)$ integral points. To be more exact, the following proposition holds.

3.2. **Proposition.** (see [16, Proposition 4.2 (4.7 in preprint)]) *A polynomial* $f(x) \in \mathbb{Q}_p[x]$ *is integer valued, compatible, and ergodic (resp., measure preserving) iff*

$$z \mapsto f(z) \bmod p^{\lfloor \log_p (\deg f) \rfloor + 3},$$

where z *runs through* $0, 1, \ldots, p^{\lfloor \log_p (\deg f) \rfloor + 3} - 1$*, is compatible and transitive (resp., bijective) mapping of the residue ring* $\mathbb{Z}/p^{\lfloor \log_p (\deg f) \rfloor + 3}$ *onto itself.*

Despite it is not very essential for further considerations, we note, however, that the series in the statement of 3.1 and of the note thereafter are uniformly convergent with respect to p-adic distance. Thus the mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is well-defined and continuous with respect to p-adic distance, see [3, Chapter 9].

Theorem 3.1 enables one to use exponentiation in design of generators that are transitive modulo 2^n for all $n = 1, 2, 3, \ldots$ (on exponential generators see e.g. [17]).

3.3. *Example.* For any odd $a = 1 + 2m$ a function $f(x) = ax + a^x$ defines a transitive modulo 2^n generator $x_{i+1} = f(x_i) \bmod 2^n$.

Indeed, in view of 3.1 the function f defines a compatible and ergodic mapping of $\mathbb{Z}_2$ onto $\mathbb{Z}_2$ since $f(x) = (1+2m)x + (1+2m)^x = x + 2mx + \sum_{i=0}^{\infty} m^i 2^i \binom{x}{i} = 1 + x + 4m\binom{x}{1} + \sum_{i=2}^{\infty} m^i 2^i \binom{x}{i}$ and $i \geq \lfloor \log_2(i+1) \rfloor + 1$ for all $i = 2, 3, 4, \ldots$.

Such a generator could be of practical value since it uses not more than $n+1$ multiplications modulo 2^n of n-bit numbers; of course, one should use calls to the table $a^{2^j} \bmod 2^n$, $j = 1, 2, 3, \ldots, n-1$. The latter table must be precomputed, corresponding calculations involve $n-1$ multiplications modulo 2^n. Obviously, one can use m as a long-term key, with the initial state x_0 being a short-term key, i.e., one changes m from time to time, but uses new x_0 for each new message. Obviously, without a properly choosen output function such a generator is not secure. The choice of output function in more details is discussed further in the paper.

Note. A similar argument shows that for every prime p and every $a \equiv 1 \pmod{p}$ the function $f(x) = ax + a^x$ defines a compatible and ergodic mapping of $\mathbb{Z}_p$ onto itself.

For polynomials with (rational or p-adic) integer coefficients theorem 3.1 may be restated in the following form.

3.4. **Proposition.** (See [6, Corollary 4.11], [7, Corollary 4.7]) *Represent a polynomial $f(x) \in \mathbb{Z}_2[x]$ in a basis of descending factorial powers*

$$x^{\underline{0}} = 1,\ x^{\underline{1}} = x,\ x^{\underline{2}} = x(x-1), \ldots,\ x^{\underline{i}} = x(x-1)\cdots(x-i+1), \ldots,$$

i.e., let

$$f(x) = \sum_{i=0}^{d} c_i \cdot x^{\underline{i}}$$

for $c_0, c_1, \ldots, c_d \in \mathbb{Z}_2$. Then the polynomial f induces an ergodic (and, obviously, a compatible) *mapping of $\mathbb{Z}_2$ onto itself iff its coefficients c_0, c_1, c_2, c_3 satisfy the following congruences:*

$$c_0 \equiv 1 \pmod{2}, \quad c_1 \equiv 1 \pmod{4}, \quad c_2 \equiv 0 \pmod{2}, \quad c_3 \equiv 0 \pmod{4}.$$

The polynomial f induces a measure preserving mapping iff

$$c_1 \equiv 1 \pmod{2}, \quad c_2 \equiv 0 \pmod{2}, \quad c_3 \equiv 0 \pmod{2}.$$

Thus, to provide ergodicity of the polynomial mapping f it is necessary and sufficient to hold fixed 6 bits only, while the other bits of coefficients of f may vary (e.g., may be key-dependent). This guarantees transitivity of the state transition function $z \mapsto f(z) \bmod 2^n$ for each n, and hence, uniform distribution of the output sequence.

Proposition 3.4 implies that the polynomial $f(x) \in \mathbb{Z}[x]$ is ergodic (resp., measure preserving) iff it is transitive modulo 8 (resp., iff it is bijective modulo 4). A corresponding assertion holds in general case, for arbitrary prime p.

3.5. **Theorem.** (See [9], [16]) *A polynomial $f(x) \in \mathbb{Z}_p[x]$ induces an ergodic mapping of $\mathbb{Z}_p$ onto itself iff it is transitive modulo p^2 for $p \neq 2, 3$, or modulo p^3, for $p = 2, 3$. The polynomial $f(x) \in \mathbb{Z}_p[x]$ induces a measure preserving mapping of $\mathbb{Z}_p$ onto itself iff it is bijective modulo p^2.*

3.6. *Example.* The mapping $x \mapsto f(x) \equiv x + 2x^2 \pmod{2^{32}}$ (which is used in RC6, see [18]) is bijective, since it is bijective modulo 4: $f(0) \equiv 0 \pmod{4}$, $f(1) \equiv 3 \pmod{4}$, $f(2) \equiv 2 \pmod{4}$, $f(3) \equiv 1 \pmod{4}$. Thus, the mapping $x \mapsto f(x) \equiv x + 2x^2 \pmod{2^n}$ is bijective for all $n = 1, 2, \ldots$.

Hence, with the use of the theorem 3.5 it is possible to obtain transitive modulo $q>1$ mappings for arbitrary natural q: one can just take $f(z)=(1+z+\hat{q}g(z)) \bmod q$, where $g(x)\in\mathbb{Z}[x]$ is an arbitrary polynomial, and $\hat{q}$ is a product of p^{s_p} for all prime factors p of q, where $s_2=s_3=3$, and $s_p=2$ for $p\neq 2,3$. Again, the polynomial $g(x)$ may be choosen, roughly speaking, 'more or less at random', i.e., it may be key-dependent, but the output sequence will be uniformly distributed for any choice of $g(x)$. This assertion may be generalized either.

3.7. **Proposition.** ([16, Lemma 4.4 and Proposition 4.5; resp., Lemma 4.11 and Proposition 4.12 in the preprint]) *Let p be a prime, and let $g(x)$ be an arbitrary composition of mappings listed in* (2.0.3). *Then the mapping $z\mapsto 1+z+p^2g(z)$ $(z\in\mathbb{Z}_p)$ is ergodic.*

In fact, both propositions 3.4, 3.7 and theorem 3.5 are particular cases of the following general

3.8. **Theorem.** ([16, Theorem 4.2, or 4.9 in the preprint]) *Let $\mathcal{B}_p$ be a class of all functions defined by series of a form $f(x)=\sum_{i=0}^{\infty}c_i\cdot x^{\underline{i}}$, where $c_0,c_1,\dots$ are p-adic integers, and $x^{\underline{i}}$ $(i=0,1,2,\dots)$ are descending factorial powers* (see 3.4). *Then the function $f\in\mathcal{B}_p$ preserves measure iff it is bijective modulo p^2; f is ergodic iff it is transitive modulo p^2 (for $p\neq 2,3$), or modulo p^3 (for $p\in\{2,3\}$).*

Note. As it was shown in [16], the class $\mathcal{B}_p$ contains all polynomial functions over $\mathbb{Z}_p$, as well as analytic (e.g., rational, entire) functions that are convergent everywhere on $\mathbb{Z}_p$. In fact, every mapping that is a composition of arithmetic operators (2.0.3) only belong to $\mathcal{B}_p$; thus, every such mapping modulo p^n could be induced by a polynomial with rational integer coefficients (see the end of Section 4 in [16]). For instance, the mapping $x\mapsto(3x+3^x) \bmod 2^n$ (which is transitive modulo 2^n, see 3.3) could be induced by a polynomial $1+x+4\binom{x}{1}+\sum_{i=2}^{n-1}2^i\binom{x}{i}=1+5x+\sum_{i=2}^{n-1}\frac{2^i}{i!}\cdot x^{\underline{i}}$ — just note that $c_i=\frac{2^i}{i!}$ are 2-adic integers since the exponent of maximal power of 2 that is a factor of $i!$ is exactly $i-\mathrm{wt}_2\,i$, where $\mathrm{wt}_2\,i$ is a number of 1's in the base-2 expansion of i (see e.g. [4, Chapter 1, Section 2, Exercise 12]); thus $\|c_i\|_2=2^{-\mathrm{wt}_2\,i}\le 1$, i.e. $c_i\in\mathbb{Z}_2$ and so $c_i \bmod 2^n\in\mathbb{Z}$.

Theorem 3.8 implies that, for instance, the state transition function $f(z)=(1+z+\zeta(q)^2(1+\zeta(q)u(z))^{v(z)}) \bmod q$ is transitive modulo q for each natural $q>1$ and arbitrary polynomials $u(x),v(x)\in\mathbb{Z}[x]$, where $\zeta(q)$ is a product of all prime factors of q. So the one can choose as a state transition function not only polynomial functions, but also rational functions, as well as analytic ones. It should be mentioned, however, that this is merely a form the function is represented (which could be suitable for some cases and unsuitable for the others), yet, for a given q, all the functions of this type may also be represented as polynomials over $\mathbb{Z}$ (see [16, Proposition 4.4; resp., Proposition 4.10 in the preprint]). For instance, certain generators of inversive kind (i.e., those using taking the inverse modulo 2^n) could be considered in such manner.

3.9. *Example.* For $f(x)=-\frac{1}{2x+1}-x$ a generator $x_{i+1}=f(x_i) \bmod 2^n$ is transitve. Indeed, the function $f(x)=(-1+2x-4x^2+8x^3-\cdots)-x=-1+x-4x^2+8(\cdots)$ is analytic and defined everywhere on $\mathbb{Z}_2$; thus $f\in\mathcal{B}_p$. Now the conclusion follows in view of 3.8 since by direct calculations it coud be easily verified that the function $f(x)\equiv -1+x-4x^2 \pmod 8$ is transitive modulo 8. Note that modulo 2^n the mapping $x\mapsto f(x) \bmod 2^n$ could be induced by a polynomial $-1+x-4x^2+8x^3+\cdots+(-1)^n2^{n-1}x^{n-1}$.

Combining operators. The class of all transitive modulo q mappings, induced by polynomials with rational integer coefficients, is rather wide: For instance, for $q=2^n$ it contains $2^{O(n^2)}$ mappings (for exact value see [9, Proposition 15], or 3.17 below). However, it could be widened significantly (up to the class of order 2^{2^n-n-1} in case $q=2^n$), by admitting also operators (2.0.4) in the composition. It turnes out that there is an easy way to construct a measure preserving or ergodic mapping out of an arbitrary compatible mapping, i.e., out of an arbitrary composition of both arithmetic (2.0.3) and logical (2.0.4) operators.

3.10**. Proposition.** [16, Lemma 2.1 and Theorem 2.5]. *Let* Δ *be a difference operator, i.e.,* $\Delta g(x) = g(x+1) - g(x)$ *by the definition. Let, further,* p *be a prime, let* c *be a coprime with* p, $\gcd(c,p)=1$, *and let* $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *be a compatible mapping. Then the mapping* $z \mapsto c + z + p\Delta g(z)$ $(z \in \mathbb{Z}_p)$ *is ergodic, and the mapping* $z \mapsto d + cx + pg(x)$, *preserves measure for arbitrary* d.

Moreover, if $p=2$, *then the converse also holds: Each compatible and ergodic (respectively each compatible and measure preserving) mapping* $z \mapsto f(z)$ $(z \in \mathbb{Z}_2)$ *could be represented as* $f(x) = 1 + x + 2\Delta g(x)$ *(respectively as* $f(x) = d + x + 2g(x)$*) for suitable* $d \in \mathbb{Z}_2$ *and compatible* $g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$.

Note. The case $p=2$ is the only case the converse of the first assertion of the proposition 3.10 holds.

3.11. *Example.* Proposition 3.10 immediately implies Theorem 2 of [19]: For any composition f of primitive functions, the mapping $x \mapsto x + 2f(x) \pmod{2^n}$ is invertible — just note that a composition of primitive functions is compatible (see [19] for the definition of primitive functions). □

Proposition 3.10 is maybe the most important tool in design of pseudorandom generators such that both their state transition functions and output functions are key-dependent. The corresponding schemes are rather flexible: In fact, one may use nearly arbitrary composition of arithmetic and logical operators to produce a strictly uniformly distributed sequence: Both for $g(x) = x \,\mathsf{XOR}(2x+1)$ and for

$$g(x) = \left(1 + 2\frac{x \,\mathsf{AND}\, x^2 + x^3 \,\mathsf{OR}\, x^4}{3 + 4(5+6x^5)^{x^6 \,\mathsf{XOR}\, x^7}}\right)^{7+\frac{8x^8}{9+10x^9}}$$

a sequence $\{x_i\}$ defined by recurrence relation $x_{i+1} = (1 + x_i + 2(g(x_i+1) - g(x_i))) \bmod 2^n$ is strictly uniformly distributed in $\mathbb{Z}/2^n$ for each $n = 1,2,3\ldots$, i.e., the sequence $\{x_i\}$ is purely periodic with *period length exactly* 2^n, and *each* element of $\{0,1,\ldots,2^n-1\}$ occurs at the period *exactly once.* We will demonstrate further that a designer could vary the function g in a very wide scope without worsening prescribed values of some important indicators of security. In fact, choosing the proper operators (2.0.1) and (2.0.3) the designer is restricted only by desirable performance, since any compatible ergodic mapping could be produced in this way:

3.12**. Corollary.** *Let* $p=2$, *and let* f *be a compatible and ergodic mapping of* $\mathbb{Z}_2$ *onto itself. Then for each* $n = 1,2,\ldots$ *the state transition function* $f \bmod 2^n$ *could be represented as a finite composition of operators* (2.0.1) *and* (2.0.3).

Proof. In view of proposition 3.10 it is sufficient to prove that for arbitrary compatible g the function $\bar g = g \bmod 2^n$ could be represented as a finite composition of operators (2.0.1) and (2.0.3). In view of 2.1, one could represent $\bar g$ as

$$\bar g(x) = \gamma_0(\chi_0) + 2\gamma_1(\chi_0,\chi_1) + \cdots + 2^{n-1}\gamma_{n-1}(\chi_0,\ldots,\chi_{n-1}),$$

where $\gamma_i=\delta_i(\bar g)$, $\chi_i=\delta_i(x)$, $i=0,1,\ldots,n-1$. Since each $\gamma_i(\chi_0,\ldots,\chi_i)$ is a Boolean function in Boolean variables $\chi_0,\ldots,\chi_i$, it could be expressed via finite number of XORs and ANDs of these variables $\chi_0,\ldots,\chi_i$. Yet each variable χ_j could be expressed as $\chi_j=\delta_j(x)=x\,\mathsf{AND}(2^j)$, and the conclusion follows. □

Using Boolean representation. So, in case $p=2$ we have two equivalent descriptions of the class of all compatible ergodic mappings, namely, theorem 3.1 and proposition 3.10. They enable one to express *any* compatible and transitive modulo 2^n state transition function either as a polynomial of special kind over a field $\mathbb{Q}$ of rational numbers, or as a special composition of arithmetic and bitwise logical operations, (2.0.3) and (2.0.1). Both these representations are suitable for programming, since they involve only standard machine instructions. However, we need one more representation, in a Boolean form (see 2.1). Despite this representation is not very convenient for programming, it will be used further for better understanding of certain important properties of the considered generators, as well for proving the ergodicity of some particular mappings, see e.g. 3.14 below. The following theorem is just a restatement of a known result from the theory of Boolean functions, the so-called bijectivity/transitivity criterion for triangle Boolean mappings. However, the latter belongs to mathematical folklore, and thus it is somewhat difficult to attribute it, yet a reader could find a proof in, e.g., [6, Lemma 4.8].

3.13. **Theorem.** *A mapping $T\colon\mathbb{Z}_2\to\mathbb{Z}_2$ is compatible and measure preserving iff for each $i=0,1,\ldots$ the Boolean function $\tau_i^T=\delta_i(T)$ in Boolean variables $\chi_0,\ldots,\chi_i$ could be represented as Boolean polynomial of the form*

$$\tau_i^T(\chi_0,\ldots,\chi_i)=\chi_i+\varphi_i^T(\chi_0,\ldots,\chi_{i-1}),$$

where φ_i^T is a Boolean polynomial. The mapping T is compatible and ergodic iff, additionaly, the Boolean function φ_i^T is of odd weight, that is, takes value 1 exactly at the odd number of points $(\varepsilon_0,\ldots,\varepsilon_{i-1})$, where $\varepsilon_j\in\{0,1\}$ for $j=0,1,\ldots,i-1$. The latter takes place if and only if $\varphi_0^T=1$, and the degree of the Boolean polynomial φ_i^T for $i\ge1$ is exactly i, that is, φ_i^T contains a monomial $\chi_0\cdots\chi_{i-1}$.

3.14. *Example.* With the use of 3.13 it is possible to give another proof of the main result of [19], namely, of Theorem 3: *The mapping $f(x)=x+(x^2\vee C)$ over n-bit words is invertible if and only if the least significant bit of C is 1. For $n\ge3$ it is a permutation with a single cycle if and only if both the least significant bit and the third least significant bit of C are* 1.

Proof of theorem 3 of [19]. Recall that for $x\in\mathbb{Z}_2$ and $i=0,1,2,\ldots$ we denote $\chi_i=\delta_i(x)\in\{0,1\}$; also we denote $c_i=\delta_i(C)$. We will calculate $\delta_i(x+(x^2\vee C))$ as a Boolean polynomial in $\chi_0,\chi_1,\ldots$ and start with the following easy claims:

- $\delta_0(x^2)=\chi_0$, $\delta_1(x^2)=0$, $\delta_2(x^2)=\chi_0\chi_1+\chi_1$,
- $\delta_n(x^2)=\chi_{n-1}\chi_0+\psi_n(\chi_0,\ldots,\chi_{n-2})$ for all $n\ge3$, where ψ_n is a Boolean function in $n-1$ Boolean variables $\chi_0,\ldots,\chi_{n-2}$.

The first of these claims could be easily verified by direct calculations. To prove the second one represent $x=\bar x_{n-1}+2^{n-1}s_{n-1}$ for $\bar x_{n-1}=x \bmod 2^{n-1}$ and calculate $x^2=(\bar x_{n-1}+2^{n-1}s_{n-1})^2=\bar x_{n-1}^2+2^ns_{n-1}\bar x_{n-1}+2^{2n-2}s_{n-1}^2=\bar x_{n-1}^2+2^n\chi_{n-1}\chi_0 \pmod{2^{n+1}}$ for $n\ge3$ and note that $\bar x_{n-1}^2$ depends only on $\chi_0,\ldots,\chi_{n-2}$.

This gives

(1) $\delta_0(x^2\vee C)=\chi_0+c_0+\chi_0c_0$
(2) $\delta_1(x^2\vee C)=c_1$

(3) $\delta_2(x^2 \vee C) = \chi_0\chi_1 + \chi_1 + c_2 + c_2\chi_1 + c_2\chi_0\chi_1$
(4) $\delta_n(x^2 \vee C) = \chi_{n-1}\chi_0 + \psi_n + c_n + c_n\chi_{n-1}\chi_0 + c_n\psi_n$ for $n \geq 3$

From here it follows that if $n \geq 3$, then $\delta_n(x^2 \vee C) = \lambda_n(\chi_0, \dots, \chi_{n-1})$, and $\deg \lambda_n \leq n-1$, since ψ_n depends only on, may be, $\chi_0, \dots, \chi_{n-2}$.

Now successively calculate $\gamma_n = \delta_n(x + (x^2 \vee C))$ for $n = 0, 1, 2, \dots$. We have $\delta_0(x + (x^2 \vee C)) = c_0 + \chi_0 c_0$ so necessarily $c_0 = 1$ since otherwise f is not bijective modulo 2. Proceeding further with $c_0 = 1$ we obtain $\delta_1(x + (x^2 \vee C)) = c_1 + \chi_0 + \chi_1$, since χ_1 is a carry. Then $\delta_2(x + (x^2 \vee C)) = (c_1\chi_0 + c_1\chi_1 + \chi_0\chi_1) + (\chi_0\chi_1 + \chi_1 + c_2 + c_2\chi_1 + c_2\chi_0\chi_1) + \chi_2 = c_1\chi_0 + c_1\chi_1 + \chi_1 + c_2 + c_2\chi_1 + c_2\chi_0\chi_1 + \chi_2$, here $c_1\chi_0 + c_1\chi_1 + \chi_0\chi_1$ is a carry. From here in view of 3.13 we immediately have $c_2 = 1$ since otherwise f is not transitive modulo 8. Now for $n \geq 3$ one has $\gamma_n = \alpha_n + \lambda_n + \chi_n$, where α_n is a carry, and $\alpha_{n+1} = \alpha_n\lambda_n + \alpha_n\chi_n + \lambda_n\chi_n$. But if $c_2 = 1$ then $\deg \alpha_3 = \deg(\mu\nu + \chi_2\mu + \chi_2\nu) = 3$, where $\mu = c_1\chi_0 + c_1\chi_1 + \chi_0\chi_1$, $\nu = (\chi_0\chi_1 + \chi_1 + c_2 + c_2\chi_1 + c_2\chi_0\chi_1) = 0$. This implies inductively in view of (4) above that $\deg \alpha_{n+1} = n + 1$ and that $\gamma_{n+1} = \chi_{n+1} + \xi_{n+1}(\chi_0, \dots, \chi_n)$, $\deg \xi_{n+1} = n + 1$. So the conditions of 3.13 are satisfied, thus finishing the proof of theorem 3 of [19]. ☐

There are some more appications of Theorem 3.13.

3.15. **Proposition.** *Let* $F\colon \mathbb{Z}_2^{n+1} \to \mathbb{Z}_2$ *be a compatible mapping such that for all* $z_1, \dots, z_n \in \mathbb{Z}_2$ *the mapping* $F(x, z_1, \dots, z_n)\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *is measure preserving. Then* $F(f(x), 2g_1(x), \dots, 2g_n(x))$ *preserves measure for all compatible* $g_1, \dots, g_n\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *and all compatible and measure preserving* $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$*. Moreover, if* f *is ergodic then* $f(x + 4g(x))$*,* $f(x \oplus (4g(x)))$*,* $f(x) + 4g(x)$*, and* $f(x) \oplus (4g(x))$ *are ergodic for any compatible* $g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$

Proof. Since the function F is compatible, $\delta_i(F(u_0, u_1, \dots, u_n)$ does not depend on $\delta_j(u_k) = \chi_{j,k}$ for $j > i$ (see 2.1 and note thereafter). Represent

$$\delta_i(F(u_0, u_1, \dots, u_n)) = \chi_{0,i}\Psi_i(u_0, u_1, \dots, u_n) + \Phi_i(u_0, u_1, \dots, u_n),$$

where Boolean polynomials $\Psi_i(u_0, u_1, \dots, u_n)$, $\Phi_i(u_0, u_1, \dots, u_n)$ do not depend on $\chi_{0,i}$; that is, they depend only on, may be,

$$\chi_{0,0}, \dots, \chi_{0,i-1}, \chi_{1,0}, \dots, \chi_{1,i}, \dots, \chi_{n,0}, \dots, \chi_{n,i}.$$

In view of 3.13 it follows that $\Psi_i = 1$ since $F(x, z_1, \dots, z_n)$ preserves measure for all $z_1, \dots, z_n \in \mathbb{Z}_2$. Moreover, then $\Phi_i(f(x), 2g_1(x), \dots, 2g_n(x))$ does not depend on $\chi_i = \delta_i(x)$ since $\delta_j(2g(x))$ does not depend on χ_i for all $j = 1, 2, \dots, n$. Now, in view of 3.13 one has $\delta_i(f(x)) = \chi_i + \xi_i(f(x))$, where $\xi_i(f(x))$ does not depend on χ_i since f preserves measure. Finally,

$$\delta_i(F(f(x), 2g_1(x), \dots, 2g_n(x))) = \delta_i(f(x)) + \Phi_i(f(x), 2g_1(x), \dots, 2g_n(x)) = \\ \chi_i + \xi_i(f(x)) + \Phi_i(f(x), 2g_1(x), \dots, 2g_n(x)) = \chi_i + \Xi_i,$$

where the Boolean polynomial Ξ_i depends only on, may be, $\chi_0, \dots, \chi_{i-1}$. This proves the first assertion of 3.15 in view of 3.13.

We prove the second assertion along the similar lines. For $z \in \mathbb{Z}_2$ and $i = 0, 1, 2, \dots$ let $\zeta_i = \delta_i(z)$. Thus one can consider $\delta_i(z \oplus 4g(z))$ and $\delta_i(z + 4g(z))$ as Boolean polynomials in Boolean variables $\zeta_0, \zeta_1, \dots, \zeta_i$. Note that $\delta_i(z \oplus 4g(z)) = \zeta_i + \lambda_i(z)$, where $\lambda_i(z) = 0$ for $i = 0, 1$ and $\deg \lambda_i(z) \leq i - 1$ for $i > 1$, since for $i > 1$ the Boolean polynomial $\lambda_i(z)$ depends, may be, only on $\zeta_0, \dots, \zeta_{i-2}$.

Next, we claim that $\delta_i(z+4g(z))=\delta_i(z)+\mu_i(z)$, where $\mu_i(z)=\mu_i^g(z)$ is 0 for $i=0,1$ and $\deg\mu_i(z)\le i-1$ for $i>1$. Indeed, $\mu_i(z)=\lambda_i(z)+\alpha_i(z)$, where the Boolean polynomial $\alpha_i(z)$ is a carry. Yet $\alpha_i(z)=0$ for $i=0,1,2$, and $\alpha_i(z)=\zeta_{i-1}\lambda_{i-1}(z)+\zeta_{i-1}\alpha_{i-1}(z)+\lambda_{i-1}(z)\alpha_{i-1}(z)$ for $i\ge 3$, and $\alpha_i(z)$ depends only on, may be, $\zeta_0,\dots,\zeta_{i-1}$ since $\alpha_i(z)$ is a carry. However, $\deg\alpha_3(z)=2$ and if $\deg\alpha_{i-1}(z)\le i-2$ then $\deg\delta_{i-1}(z)\alpha_{i-1}(z)\le i-1$, $\deg\lambda_{i-1}(z)\alpha_{i-1}(z)\le i-1$, and $\deg\zeta_{i-1}\lambda_{i-1}(z)\le i-1$ since $\alpha_{i-1}(z)$ depends only on, may be, $\zeta_0,\dots,\zeta_{i-2}$ and $\lambda_{i-1}(z)$ depends, may be, only on $\zeta_0,\dots,\zeta_{i-3}$. Thus $\deg\alpha_i(z)\le i-1$ and hence $\deg\mu_i(z)\le i-1$.

Now, since $f(x)$ is egodic, $\delta_i(f(x))=\chi_i+\xi_i(x)$, where the Boolean polynomial ξ_i depends only on, may be, $\chi_0,\dots,\chi_{i-1}$ and, additionally, $\xi_0=1$, and $\deg\xi_i=i$ for $i>0$ (see 3.13); i.e. $\xi_i(x)=\chi_0\chi_1\cdots\chi_{i-1}+\vartheta_i(x)$, where $\deg\vartheta_i(x)\le i-1$ for $i>0$. Hence, for $*\in\{+,\oplus\}$ one has $\delta_i(f(x*4g(x)))=\delta_i(x*4g(x))+\delta_0(x*4g(x))\delta_1(x*4g(x))\cdots\delta_{i-1}(x*4g(x))+\vartheta_i(x*4g(x))$; thus $\delta_i(f(x*4g(x)))=\chi_i+\chi_0\cdots\chi_{i-1}+\beta_i^*(x)$, where $\deg\beta_i^*(x)\le i-1$ for $i>0$, and $\delta_0(f(x*4g(x)))=\delta_0(x*4g(x))+1=\chi_0+1$. Finally, $f(x*4g(x))$ for $*\in\{+,\oplus\}$ is ergodic in view of 3.13.

In a similar manner it could be demonstrated that $f(x)*4g(x)$ is ergodic for $*\in\{+,\oplus\}$: $\delta_i(f(x)*4g(x))=\delta_i(f(x))$ for $i=0,1$ and thus satisfy the conditions of 3.13. For $i>1$ on has $\delta_i(f(x)\oplus 4g(x))=\chi_i+\xi_i(x)+\delta_{i-2}(g(x))$; but $\delta_{i-2}(g(x))$ does not depend on χ_{i-1},χ_i. Thus the Boolean polynomial $\xi_i(x)+\delta_{i-2}(g(x))$ in variables $\chi_0,\dots,\chi_{i-1}$ is of odd weight, since $\xi_i(x)$ is of odd weight, thus proving that $f(x)\oplus 4g(x)$ is ergodic.

Now represent $g(x)=g(f^{-1}(f(x)))=h(f(x))$, where $f^{-1}(x)$ is the inverse mapping for f. Clearly, $f^{-1}(x)$ is well defined since the mapping $f\colon\mathbb{Z}_2\to\mathbb{Z}_2$ is bijective; moreover $f^{-1}(x)$ is compatible and ergodic. Finally $\delta_i(f(x)+4g(x))=\delta_i(f(x))+\mu_i'(f(x))$, where the Boolean polynomial $\mu_i'(x)=\mu_i^h(x)$ in Boolean variables $\chi_0,\dots,\chi_{i-1}$ does not contain a monomial $\chi_0\cdots\chi_{i-1}$ (see the claim above). This implies that the Boolean polynomial $\mu_i'(f(x))$ in Boolean variables $\chi_0,\dots,\chi_{i-1}$ does not contain a monomial $\chi_0\cdots\chi_{i-1}$ either, since $\delta_j(f(x))=\chi_j+\xi_j(x)$ and $\xi_j(x)$ depend only, may be, on $\chi_0,\dots,\chi_{j-1}$ for $j=2,3,\dots$. Hence, $\delta_i(f(x)+4g(x))=\chi_i+\xi_i(x)+\mu_i'(f(x))$ and the Boolean polynomial $\xi_i(x)+\mu_i'(f(x))$ in Boolean variables $\chi_0,\dots,\chi_{i-1}$ is of odd weight. This finishes the proof in view of 3.13. □

3.16. *Example.* With the use of 3.15 it is possible to construct very fast generators $x_{i+1}=f(x_i)\bmod 2^n$ that are transitive modulo 2^n. For instance, take

$$f(x)=(\dots((((x+c_0)\oplus d_0)+c_1)\oplus d_1)+\dots+c_m)\oplus d_m,$$

where $c_0\equiv 1\pmod 2$, and the rest of c_i,d_i are 0 modulo 4. By the way, this generator, looking somewhat 'linear', is as a rule rather 'nonlinear': the corresponding polynomial over $\mathbb{Q}$ is of high degree. The general case of these functions f (for arbitrary c_i,d_i) was studied by the author's student Ludmila Kotomina: She proved that such a function is ergodic iff it is transitive modulo 4.

Counting the number of transitive mappings. The preceeding results enable us to calculate the number of all compatible transitive modulo 2^n mappings of $\mathbb{Z}/2^n$ onto itself and the number of them that are induced by *polynomial mappings over* $\mathbb{Z}$, i.e., that could be expressed as polynomials with rational integer coefficients.

3.17. **Proposition.** *There are exactly* 2^{2^n-n-1} *compatible and transitive modulo* 2^n *mappings* $T\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$*. For* $n \le 3$ *all of them could be represented as polynomials over* $\mathbb{Z}$*; if* $n > 3$*, then exactly* $2^{\sum_{i=0}^{\rho(n)}(n-i+\mathrm{wt}_2\, i)-6}$ *of them could be represented as polynomials over* $\mathbb{Z}$ (see 3.4). *Moreover,* $\sum_{i=0}^{\rho(n)}(n-i+\mathrm{wt}_2\, i)-6 \sim \frac{1}{2}n^2$ *as* $n \to \infty$*.* Here $\mathrm{wt}_2\, i$ is the binary weight of non-negative rational integer i (i.e., the number of 1's in base-2 expansion of i), and $\rho(n)$ is the biggest natural number k such that $k - \mathrm{wt}_2\, k < n$.

Proof. The first assertion is an easy consequence of 3.13: obviously, the number of Boolean functions of odd weight in i variables is exactly 2^{2^i-1}, and the result follows.

To prove the second assertion we first note that each integer-valued polynomial $f(x) \in \mathbb{Q}_p[x]$ over a field $\mathbb{Q}_p$ of p-adic numbers (that is, a polynomial, which takes values in $\mathbb{Z}_p$ at each point of $\mathbb{Z}_p$) admits a unique representation

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} \tag{3.17.1}$$

for suitable $a_0, a_1, a_2, \dots \in \mathbb{Z}_p$, with only finite number of non-zero $a_0, a_1, a_2, \dots$ (see e.g. [3]). Further, the polynomial (3.17.1) is identically zero modulo 2^n iff $a_i \equiv 0 \pmod{2^n}$ for all $i = 0, 1, 2, \dots$ (see proposition 4.2 of [6]). Lastly, the polynomial (3.17.1) is a polynomial over $\mathbb{Z}_2$ iff it could be represented in the form of 3.4, i.e., iff $a_i \equiv 0 \pmod{2^{\mathrm{ord}_2\, i!}}$ for all $i = 0, 1, 2, \dots$. Here and after $\mathrm{ord}_p\, q$ stands for the greatest power of a prime p, which is a factor of $q \in \mathbb{N}$: $p^{\mathrm{ord}_p\, q} \mid q$, but $p^{1+\mathrm{ord}_p} \nmid q$; it is well known that $\mathrm{ord}_p\, i! = \frac{1}{p-1}(i - \mathrm{wt}_p\, i)$, see e.g. [4], Chapter 1, Section 2, Exercise 13.

Thus, each mapping of $\mathbb{Z}/2^n$ onto $\mathbb{Z}/2^n$ that is induced by polynomial over $\mathbb{Z}$ admits a unique representation by polynomial (3.17.1) of degree not greater than $\rho(n)$, and with $a_0, a_1, a_2, \dots \in \mathbb{Z}/2^n$ such that $a_i \equiv 0 \pmod{2^{i-\mathrm{wt}_2\, i}}$ for $i = 2, 3, \dots$. In view of 3.1, the latter polynomial is transitive modulo 2^n iff $a_0 \equiv 1 \pmod 2$, $a_1 \equiv 1 \pmod 4$, and $a_i \equiv 0 \pmod{2^{\lfloor \log_2(i+1)\rfloor+1}}$ for $i = 2, 3, \dots$. Since $i - \mathrm{wt}_2\, i < \lfloor \log_2(i+1)\rfloor + 1$ iff $i = 0, 1, 2, 3$, the number of all transitive modulo 2^n mappings of $\mathbb{Z}/2^n$ into $\mathbb{Z}/2^n$ that are induced by polynomials over $\mathbb{Z}$ is exactly $2^{\eta(n)}$, where $\eta(n) = 4n - 8 + \sum_{i=4}^{\rho(n)}(n - i + \mathrm{wt}_2\, i) = -6 + \sum_{i=0}^{\rho(n)}(n - i + \mathrm{wt}_2\, i)$ for $n > 3$, and $\eta(1) = 1$, $\eta(2) = 2$, $\eta(3) = 16$.

Now, to finish the proof of proposition 3.17 we only have to demonstrate that $\lim_{n\to\infty} \frac{2\eta(n)}{n^2} = 1$. We start with estimating $\rho(n)$.

Represent n as $n = 2^k + t$ where $0 \le t < 2^k$. Verify that $\rho(2^{k+1} - 1) = 2^{k+1} - 1$ by direct calculations. So, $\rho(n) = n$, if $n = 2^{k+1} - 1$ (i.e., if $t = 2^k - 1$), and $\rho(n) = 2^k + s$ for certain $s \ge 0$, in the opposite case (i.e., if $t < 2^k - 1$). We claim that $s < 2^k$. Indeed, the function $k - \mathrm{wt}_2\, k$, and hence, the function $\rho(n)$ are nondecreasing; thus, $s \le 2^k$. However, assuming $s = 2^k$ we get a contradiction: On the one hand, $2^k + t = n > \rho(n) - \mathrm{wt}_2\, \rho(n) = 2^k + 2^k - \mathrm{wt}_2(2^k + 2^k) = 2^{k+1} - 1$, but $t < 2^k - 1$ on the other. Thus for $t < 2^k - 1$, i.e., for $n \ne 2^{k+1} - 1$, we have that $\rho(n) = 2^k + s$ for some $t \le s \le 2^k - 1$ since obviously $\rho(n) \ge n$. Hence $n = 2^k + t > \rho(n) - \mathrm{wt}_2(\rho(n)) = 2^k + s - 1 - \mathrm{wt}_2\, s$; consequently $s = \max\{r \in \mathbb{N} : s - \mathrm{wt}_2\, s < t + 1\} = \rho(t + 1)$ by definition of the function ρ. Thus we proved the formula

$$\rho(n)=\rho(2^k+t)=\begin{cases}2^k+t, & \text{if } t=2^k-1, \text{ i.e., if } n=2^{k+1}-1;\\ 2^k+\rho(t+1), & \text{if } t<2^k-1, \text{ i.e., if } n\neq 2^{k+1}-1.\end{cases}$$

This implies an obvious recursive procedure for calculating $\rho(n)$, which halts not later than in k steps; mind that $k+1$ is the number of digits in base-2 expansion of n. We conclude finally that $n\le\rho(n)\le n+\lfloor\log_2 n\rfloor$ since the number of digits in base-2 expansion of n is exactly $\lfloor\log_2 n\rfloor+1$ and $2^r-1=\underbrace{11\ldots1}_{r}$.

Now we succesively calculate $\eta(n)=\sum_{i=0}^{n}(i+\operatorname{wt}_2 i)+\sum_{j=n+1}^{\rho(n)}(n-j+\operatorname{wt}_2 j)-6=\frac{n(n+1)}{2}+\sum_{i=1}^{n}\operatorname{wt}_2 i-\frac{(\rho(n)-n)(\rho(n)-n+1)}{2}+\sum_{j=1}^{\rho(n)-n}\operatorname{wt}_2(n+j)-6$. Finally, taking into the account that

$$\sum_{i=1}^{n}\operatorname{wt}_2 i\le\sum_{i=1}^{2^{\lfloor\log_2 n\rfloor+1}-1}\operatorname{wt}_2 i=\sum_{i=1}^{\lfloor\log_2 n\rfloor+1} i\binom{\lfloor\log_2 n\rfloor+1}{i}$$
$$=(\lfloor\log_2 n\rfloor+1)2^{\lfloor\log_2 n\rfloor}\le(1+\log_2 n)n$$

and also that $\rho(n)-n\le\log_2 n$, $\operatorname{wt}_2(a+b)\le\operatorname{wt}_2 a+\operatorname{wt}_2 b$, $\operatorname{wt}_2 a\le 1+\log_2 a$, we conclude that $\lim_{n\to\infty}\frac{2\eta(n)}{n^2}=1$. □

3.18. *Note.* During the proof of proposition 3.17 we have demonstrated that each mapping of $\mathbb{Z}/2^n$ onto $\mathbb{Z}/2^n$ induced by a polynomial over $\mathbb{Z}$ could be represented by a polynomial of degree not greater than $\rho(n)\le n+\log_2 n$, and this estimate is sharp. Moreover, from the final part of the proof it could be deduced that the number of transitive mappings of $\mathbb{Z}/2^n$ onto itself that are induced by polynomials over $\mathbb{Z}$ is $O(2^{\frac{1}{2}n(n+1)+n(1+\log_2 n)+\frac{1}{2}(1+\log_2 n)\log_2 n+(1+\log_2\log_2 n)\log_2 n})$. The case $n=2^k$ is of special interest since usually the word length of contemporary processors is a power of 2. In this case $\rho(n)=n+1$, and for $k\ge 2$ direct calculations of $\eta(n)$ (see the proof of 3.17) imply that the number of transitive modulo 2^n mappings of $\mathbb{Z}/2^n$ onto itself that are induced by polynomials over $\mathbb{Z}$ is exactly $2^{2^{2k-1}+(k+1)2^{k-1}-4}$. For instance, in the case $n=32$ this makes 2^{604} transitive mappings; all of them are induced by polynomials over $\mathbb{Z}$ of degree ≤ 33, i.e, could be expressed via arithmetic operations (2.0.3). Yet for $n=8$ this makes only 2^{44} polynomials of degree not exceeding 9. By the use of bitwise logical operations (2.0.1) along with arithmetic operations one could significantly increase the number of transitive mappings, up to 2^{2^n-n-1}. Each of these mappings could be expessed as a polynomial over $\mathbb{Q}$ (see 3.1), yet the bound for its degree d raises significantly either. Namely, from the proof of 3.17 it follows that $\lfloor\log_2(d+1)\rfloor+1<n$ for $n>2$, i.e., $d\le 2^{n-1}-2$, and this bound is sharp. For $n=8$, e.g., this makes 2^{247} transitive polynomials over $\mathbb{Q}$ of degree ≤ 126. Note that for each $1\le d\le\rho(n)$ (resp., for each $1\le d\le 2^{n-1}-2$) there exist an ergodic polynomial over $\mathbb{Z}$ (resp., a compatible and ergodic polynomial over $\mathbb{Q}$) of degree exactly d. The number of pairwise distinct modulo 2^n mappings induced by these polynomials may also be calculated using the ideas of the proof of 3.17. We omit details.

Using uniform differentiability. Now we are going to give general descriptions of equiprobable (in particular, multivariate measure-preserving) mappings following [16, section 3], [7, Section 5], [6, Section 5]. These mapping could be used as output functions of the generators assuring uniform distribution of the produced sequence, see 2.3.

To describe equiprobable (and, in particular, measure preserving) mappings we need p-adic differential calculus techniques as well as certain notions introduced in [6, 16, 7].

3.19. **Definition.** A function $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is said to be *differentiable modulo* p^k at the point $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{Z}_p^{(n)}$ if there exists a positive integer rational N and $n \times m$ matrix $F'_k(\mathbf{u})$ over $\mathbb{Q}_p$ (called *the Jacobi matrix modulo* p^k of the function F at the point $\mathbf{u}$) such that for every positive rational integer $K \ge N$ and every $\mathbf{h} = (h_1, \dots, h_n) \in \mathbb{Z}_p^{(n)}$ the inequality $\|\mathbf{h}\|_p \le p^{-K}$ implies that

$$F(\mathbf{u} + \mathbf{h}) \equiv F(\mathbf{u}) + \mathbf{h}F'_k(\mathbf{u}) \pmod{p^{k+K}}. \tag{3.19.1}$$

In case $m = 1$ the Jacobi matrix modulo p^k is called a *differential modulo* p^k. In case $m = n$ a determinant of Jacobi matrix modulo p^k is called a *Jacobian modulo* p^k. The elements of Jacobi matrix modulo p^k are called *partial derivatives modulo* p^k of the function F at the point $\mathbf{u}$.

A partial derivative (respectively, a differential) modulo p^k are sometimes denoted as $\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j}$ (respectively, as $d_k F(\mathbf{u}) = \sum_{i=1}^n \frac{\partial_k F(\mathbf{u})}{\partial_k x_i} d_k x_i$).

The definition immediately implies that partial derivatives modulo p^k of the function F are defined up to the p-adic integer summand whith p-adic norm does not exceeding p^{-k}. In cases when all partial derivatives modulo p^k at all points of $\mathbb{Z}_p^{(n)}$ are p-adic integers, we say that the function F has *integer-valued derivative modulo* p^k; in these cases we can associate to each partial derivative modulo p^k a unique element of the ring $\mathbb{Z}/p^k$, and a Jacobi matrix modulo p^k at each point $\mathbf{u} \in \mathbb{Z}_p^{(n)}$ thus can be considered as a matrix over a ring $\mathbb{Z}/p^k$. It turnes out that this is exactly the case for compatible F. Namely, the following proposition holds.

3.20. **Proposition.** ([6, Corollary 3.8], [7, Corollary 3.3]) *Let a compatible function* $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ *be uniformly differentiable modulo* p^k *at the point* $\mathbf{u} \in \mathbb{Z}_p^{(n)}$. *Then* $\left\|\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j}\right\|_p \le 1$, *i.e.,* F *has integer-valued derivatives modulo* p^k.

For the functions with integer-valued derivatives modulo p^k the ‘rules of differentiation modulo p^k’ have the same (up to congruence modulo p^k instead of equality) form as for usual differentiation. For instance, if both functions $G\colon \mathbb{Z}_p^{(s)} \to \mathbb{Z}_p^{(n)}$ and $F\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ are differentiable modulo p^k at the points, respectively, $\mathbf{v} = (v_1, \dots, v_s)$ and $\mathbf{u} = G(\mathbf{v})$, and their partial derivatives modulo p^k at these points are p-adic integers, then a composition $F \circ G\colon \mathbb{Z}_p^{(s)} \to \mathbb{Z}_p^{(m)}$ of these functions is uniformly differentiable modulo p^k at the point $\mathbf{v}$, all its partial derivatives modulo p^k at this point are p-adic integers, and $(F \circ G)'_k(\mathbf{v}) \equiv G'_k(\mathbf{v})F'_k(\mathbf{u}) \pmod{p^k}$.

By the analogy with classical case we can give the following

3.21. **Definition.** A function $F\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is said to be *uniformly differintiable modulo* p^k *on* $\mathbb{Z}_p^{(n)}$ iff there exists $K \in \mathbb{N}$ such that 3.19.1 holds simultaneously for all $\mathbf{u} \in \mathbb{Z}_p^{(n)}$ as soon as $\|h_i\|_p \le p^{-K}$, $(i = 1, 2, \dots, n)$. The least such $K \in \mathbb{N}$ is denoted via $N_k(F)$.

We recall that all partial derivatives modulo p^k of a uniformly differentiable modulo p^k function F are periodic functions with period $p^{N_k(F)}$ (see [6, Proposition 2.12]). This in particular implies that each partial derivative modulo p^k could be considered as a function defined on $\mathbb{Z}/p^{N_k(F)}$. Moreover, if a continuation $\tilde{F}$ of the function $F = (f_1, \ldots, f_m)\colon \mathbb{N}_0^{(n)} \to \mathbb{N}_0^{(m)}$ to the space $\mathbb{Z}_p^{(n)}$ is uniformly differentiable modulo p^k on the $\mathbb{Z}_p^{(n)}$, then one could continue both the function F and all its (partial) derivatives modulo p^k to the space $\mathbb{Z}_p^{(n)}$ simultaneously. This imples that we could study if necessary (partial) derivatives modulo p^k of the function $\tilde{F}$ instead of studying those of F and vise versa. For example, a partial derivative $\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j}$ modulo p^k vanishes modulo p^k at no point of $\mathbb{Z}_p^{(n)}$ (that is, $\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j} \not\equiv 0 \pmod{p^k}$ for all $u \in \mathbb{Z}_p^{(n)}$, or, the same $\left\|\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j}\right\|_p > p^{-k}$ everywhere on $\mathbb{Z}_p^{(n)}$) if and only if $\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j} \not\equiv 0 \pmod{p^k}$ for all $u \in \{0, 1, \ldots, p^{N_k(F)} - 1\}$.

To calculate a derivative of, for instance, a state transition function, which is a composition of 'elementary' functions, see 3.12, one needs to know derivatives of these 'elementary' functions, such as (2.0.1) and (2.0.3). Thus, we briefly introduce a p-adic analogon of a 'table of derivatives' of classical Calculus.

3.22. *Example.* Derivatives of bitwise logical operations.

(1) *a function* $f(x) = x \,\mathsf{AND}\, c$ *is uniformly differentiable on* $\mathbb{Z}_2$ *for any* $c \in \mathbb{Z}$*;* $f'(x) = 0$ *for* $c \geq 0$*, and* $f'(x) = 1$ *for* $c < 0$*,* since $f(x + 2^n s) = f(x)$, and $f(x + 2^n s) = f(x) + 2^n s$ for $n \geq l(|c|)$, where $l(|c|)$ is the bit length of absolute value of c (mind that for $c \geq 0$ the 2-adic representation of $-c$ starts with $2^{l(c)} - c$ in less significant bits followed by $11\ldots$: $-1 = 11\ldots$, $-3 = 10111\ldots$, etc.).

(2) *a function* $f(x) = x \,\mathsf{XOR}\, c$ *is uniformly differentiable on* $\mathbb{Z}_2$ *for any* $c \in \mathbb{Z}$*;* $f'(x) = 1$ *for* $c \geq 0$*, and* $f'(x) = -1$ *for* $c < 0$*.* This immediately follows from (1) since $u \,\mathsf{XOR}\, v = u + v - 2(x \,\mathsf{AND}\, v)$ (see (2.0.2)); thus $(x \,\mathsf{XOR}\, c)' = x' + c' - 2(x \,\mathsf{AND}\, c)' = 1 + 2 \cdot (0,\ \text{for } c \geq 0;\ \text{or } -1,\ \text{for } c < 0)$.

(3) in the same manner it could be shown that *functions* $(x \bmod 2^n)$*,* $\mathsf{NEG}(x)$ *and* $(x \,\mathsf{OR}\, c)$ *for* $c \in \mathbb{Z}$ *are uniformly differentiable on* $\mathbb{Z}_2$*, and* $(x \bmod 2^n)' = 0$*,* $(\mathsf{NEG}\, x)' = -1$*,* $(x \,\mathsf{OR}\, c)' = 1$ *for* $c \geq 0$*,* $(x \,\mathsf{OR}\, c)' = 0$ *for* $c < 0$*.*

(4) *a function* $f(x, y) = x \,\mathsf{XOR}\, y$ *is not uniformly differentiable on* $\mathbb{Z}_2^{(2)}$*, yet it is uniformly differentiable modulo* 2 *on* $\mathbb{Z}_2^{(2)}$; from (2) it follows that its partial derivatives modulo 2 are 1 everywhere on $\mathbb{Z}_2^{(2)}$.

Here how it works altogether.

Example. A function $f(x) = x + (x^2 \,\mathsf{OR}\, 5)$ is uniformly differentiable on $\mathbb{Z}_2$, and $f'(x) = 1 + 2x \cdot (x \,\mathsf{OR}\, 5)' = 1 + 2x$.

A function $F(x, y) = (f(x, y), g(x, y)) = (x \oplus 2(x \wedge y), (y + 3x^3) \oplus x)$ is uniformly differentiable modulo 2 as bivariate function, and $N_1(F) = 1$; namely

$$F(x + 2^n t, y + 2^m s) \equiv F(x, y) + (2^n t, 2^m s) \cdot \begin{pmatrix} 1 & x+1 \\ 0 & 1 \end{pmatrix} \pmod{2^{k+1}}$$

for all $m, n \geq 1$ (here $k = \min\{m, n\}$). The matrix $\begin{pmatrix} 1 & x+1 \\ 0 & 1 \end{pmatrix} = F_1'(x, y)$ is Jacoby matrix modulo 2 of F; here how we calculate partial derivatives modulo 2: for instance, $\frac{\partial_1 g(x,y)}{\partial_1 x} = \frac{\partial_1 (y+3x^3)}{\partial_1 x} \cdot \frac{\partial_1 (u \oplus x)}{\partial_1 u}\Big|_{u=y+3x^3} + \frac{\partial_1 x}{\partial_1 x} \cdot \frac{\partial_1 (u \oplus x)}{\partial_1 x}\Big|_{u=y+3x^3} = 9x^2 \cdot 1 + 1 \cdot 1 \equiv x + 1 \pmod{2}$. Note that a partial derivative modulo 2 of the function $2(x \wedge y)$ is always 0 modulo 2 because of the multiplier 2: the function

$x \wedge y$ is not differentiable modulo 2 as bivariate function, yet $2(x \wedge y)$ is. So the Jacobian of the function F is $\det F'_1 = 1 \pmod 2$.

Now let $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ and $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ be compatible functions, which are uniformly differentiable on $\mathbb{Z}_p^{(n)}$ modulo p. This is a relatively weak restriction since all uniformly differentiable on $\mathbb{Z}_p^{(n)}$ functions, as well as functions, which are uniformly differentiable on $\mathbb{Z}_p^{(n)}$ modulo p^k for some $k \geq 1$, are uniformly differentiable on $\mathbb{Z}_p^{(n)}$ modulo p; note that $\frac{\partial F}{\partial x_i} \equiv \frac{\partial_k F}{\partial_k x_i} \equiv \frac{\partial_{k-1} F}{\partial_{k-1} x_i} \pmod{p^{k-1}}$. Moreover, all values of all partial derivatives modulo p^k (and thus, modulo p) of F and f are p-adic integers everywhere on, respectively, $\mathbb{Z}_p^{(n)}$ and $\mathbb{Z}_p$ (see 3.20), so to calculate these values one can use the techniques considered above.

3.23. **Theorem.** ([16, Theorems 3.1 and 3.2; resp., 3.7 and 3.9 in the preprint], [7, 5.2 – 5.5], [6, 5.2 – 5.5]) *A function $F\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is equiprobable whenever it is equiprobable modulo p^k for some $k \geq N_1(F)$ and the rank of its Jacobi matrix $F'_1(\mathbf{u})$ modulo p is exactly m at all points $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^k)^{(n)}$. In case $m = n$ these conditions are also necessary, i.e., the function F preserves measure iff it is bijective modulo p^k for some $k \geq N_1(F)$ and $\det(F'_1(\mathbf{u})) \not\equiv 0 \pmod p$ for all $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^k)^{(n)}$. Moreover, in the considered case these conditions imply that F preserves measure iff it is bijective modulo $p^{N_1(F)+1}$.*

That is, if the mapping $\mathbf{u} \mapsto F(\mathbf{u}) \bmod p^{N_1(F)}$ is equiprobable, and if the rank of Jacobi matrix $F'_1(u)$ modulo p is exactly m at all points $\mathbf{u} \in (\mathbb{Z}/p^{N_1(F)})^{(n)}$ then *each* mapping $\mathbf{u} \mapsto F(\mathbf{u}) \bmod p^r$ of $(\mathbb{Z}/p^r)^{(n)}$ onto $(\mathbb{Z}/p^r)^{(m)}$ $(r = 1, 2, 3, \ldots)$ is equiprobable (i.e., each point $\mathbf{u} \in (\mathbb{Z}/p^r)^{(m)}$ has the same number of preimages in $(\mathbb{Z}/p^r)^{(m)}$, see 2.2).

3.24. *Example.* (see [19])

(1) *A mapping*

$$(x, y) \mapsto F(x, y) = (x \oplus 2(x \wedge y), (y + 3x^3) \oplus x) \bmod 2^r$$

of $(Z/2^r)^{(2)}$ onto $(Z/2^r)^{(2)}$ is bijective for all $r = 1, 2, \ldots$

Indeed, the function F is bijective modulo $2^{N_1(F)} = 2$ (direct verification) and $\det(F'_1(\mathbf{u})) \equiv 1 \pmod 2$ for all $\mathbf{u} \in (\mathbb{Z}/2)^{(2)}$ (see 3.22 and example thereafter).

(2) *The following mappings of $\mathbb{Z}/2^r$ onto $\mathbb{Z}/2^r$ are bijective for all $r = 1, 2, \ldots$:*

$$x \mapsto (x + 2x^2) \bmod 2^r,\ x \mapsto (x + (x^2 \vee 1)) \bmod 2^r,\ x \mapsto (x \oplus (x^2 \vee 1)) \bmod 2^r$$

Indeed, all three mappings are uniformly differentiable modulo 2, and $N_1 = 1$ for all of them. So it sufficies to prove that all three mappings are bijective modulo 2, i.e. as mappings of the residue ring $\mathbb{Z}/2$ modulo 2 onto itself (this could be checked by direct calculations), and that their derivatives modulo 2 vanish at no point of $\mathbb{Z}/2$. The latter also holds, since the derivatives are, respectively,

$$1 + 4x \equiv 1 \pmod 2,\ 1 + 2x \cdot 1 \equiv 1 \pmod 2,\ 1 + 2x \cdot 1 \equiv 1 \pmod 2$$

since $(x^2 \vee 1)' = 2x \cdot 1 \equiv 1 \pmod 2$, and $(x \oplus C)'_1 \equiv 1 \pmod 2$, (see 3.22).

(3) *The following closely related variants of the previous mappings of $\mathbb{Z}/2^r$ onto $\mathbb{Z}/2^r$ are NOT bijective for all $r = 1, 2, \ldots$:*

$$x \mapsto (x + x^2) \bmod 2^r,\ x \mapsto (x + (x^2 \wedge 1)) \bmod 2^r,\ x \mapsto (x + (x^3 \vee 1)) \bmod 2^r,$$

since they are compatible but not bijectve modulo 2.

(4) (see [8], also [19, Theorem 1]) *Let* $P(x) = a_0 + a_1x + \cdots + a_dx^d$ *be a polynomial with integral coefficients. Then* $P(x)$ *is a permutation polynomial* (i.e., is bijective) *modulo* 2^n*,* $n > 1$ *if and only if* a_1 *is odd,* $(a_2 + a_4 + \cdots)$ *is even, and* $(a_3 + a_5 + \cdots)$ *is even.*

In view of 3.23 we have to verify whether the two conditions hold: first, whether P is bijective modulo 2, and second, whether $P'(z) \equiv 1 \pmod 2$ for $z \in \{0, 1\}$. The first condition gives that $P(0) = a_0$ and $P(1) = a_0+a_1+a_2 + \cdots a_d$ must be distinct modulo 2; hence $a_1 + a_2 + \cdots a_d \equiv 1 \pmod 2$. The second condition implies that $P'(0) = a_1 \equiv 1 \pmod 2$, $P'(1) \equiv a_1 + a_3+a_5+\cdots \equiv 1 \pmod 2$. Now combining all this together we get $a_2+a_3+\cdots a_d \equiv 0 \pmod 2$ and $a_3 + a_5 + \cdots \equiv 0 \pmod 2$, hence $a_2 + a_4 + \cdots \equiv 0 \pmod 2$.

(5) As a bonus, we can use exactly the same proof to get exactly the same characterization of bijective modulo 2^r $(r = 1, 2, \ldots)$ mappings of the form $x \mapsto P(x) = a_0 \oplus a_1x \oplus \cdots \oplus a_dx^d \bmod 2^r$ since $u \oplus v$ is uniformly differentiable modulo 2 as bivariate function, and its derivative modulo 2 is exactly the same as the derivative of $u + v$, and besides, $u \oplus v \equiv u + v \pmod 2$.

Note that in general theorem 3.23 could be applied to a class of functions that is narrower than the class of all compatible functions. However, it turnes out that for $p = 2$ this is not the case. Namely, the following proposition holds, which in fact is just a restatement of a corresponding assertion of 3.13.

3.25**. Proposition.** ([6, Corollary 4.6], [7, Corollary 4.4]) *If a compatible function* $g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *preserves measure then it is uniformly differentiable modulo* 2 *and has integer derivative modulo* 2 *(which is always* 1 *modulo* 2*).*

The techniques introduced above could also be applied to characterize ergodic functions.

3.26**. Theorem.** ([16, Theorem 3.4, resp. 3.14 in the preprint], [7, Theorem 5.7], [6, Theorem 5.7]) *Let a compatible function* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *be uniformly differentiable modulo* p^2*. Then* f *is ergodic if and only if it is transitive modulo* $p^{N_2(f)+1}$ *when* p *is an odd prime, or modulo* $2^{N_2(f)+2}$ *when* $p = 2$.

3.27*. Example.* In [19] there is stated that “...neither the invertibility nor the cycle structure of $x + (x^2 \vee 5)$ could be determined by his (*i.e., mine — V.A.*) techniques.” See however how it could be immediately done with the use of Theorem 3.26: The function $f(x) = x + (x^2 \vee 5)$ is uniformly differentiable on $\mathbb{Z}_2$, thus, it is uniformly differentiable modulo 4 (see 3.22 and an example thereafter), and $N_2(f) = 3$. Now to prove that f is ergodic, in view of 3.26 it sufficies to demonstrate that f induces a permutation with a single cycle on $\mathbb{Z}/32$. Direct calculations show that a string $0, f(0) \bmod 32, f^2(0) \bmod 32 = f(f(0)) \bmod 32, \ldots, f^{31}(0) \bmod 32$ is a permutation of a string $0, 1, 2, \ldots, 31$, thus ending the proof.

Note that both Theorems 3.23 and 3.26 share the same feature: To prove ergodicity (or measure preservation) of a certain mapping it sufficies to verify only whether this mapping is transitive (respectively, bijective) modulo p^N for a certain N. The origin of this feature is a pecularity of the p-adic distance; in fact such an effect goes back to Hensel’s lemma. By the way, using this feature, namely, the fact that a polynomial f with integer coefficients induces an ergodic mapping of $\mathbb{Z}_2$

onto itself iff f is transitive modulo 8 (see 3.5; note that 3.26 implies modulo 16), M.V.Larin proved the following theorem in a spirit of one of Rivest's 3.24(4).

3.28. **Theorem.** ([9, Proposition 21]) *Let* $P(x) = a_0 + a_1x + \cdots + a_dx^d$ *be a polynomial with integral coefficients. Then* $P(x)$ *induces a permutation with a single cycle modulo* 2^n, $n > 2$ *if and only if the following congruences hold simultaneously:*

$$\begin{gathered} a_3 + a_5 + a_7 + a_9 + \cdots \equiv 2a_2 \pmod 4; \\ a_4 + a_6 + a_8 + \cdots \equiv a_1 + a_2 - 1 \pmod 4; \\ a_1 \equiv 1 \pmod 2; \\ a_0 \equiv 1 \pmod 2. \end{gathered}$$

It would be of interest to understand whether an analogon of 3.24(5) for ergodic polynomials over $\mathbb{Z}$ could be proved: A straightforward application of the same ideas does not work since the function $x \oplus y$ is uniformly differentiable modulo 2, but not modulo 4, cf. Theorem 3.26.

4. Constructions

In this section we introduce several constructions that enable one to built pseudorandom number generators out of 'building blocks' based on ergodic and equiprobable mappings. Output sequences of these generators are always strictly uniformly distributed. Other probabilistic and cryptographic properties of these generators are discussed in further sections.

Our base construction is a finite automaton $\mathfrak{A} = \langle N, M, f, F, u_0 \rangle$ such that

- the state set N is finite;
- the state transition function $f : N \to N$ is transitive (i.e., f is a permutation with a single cycle);
- the output alphabet M is finite, and $|M|$ is a factor of $|N|$;
- the output function $F : N \to M$ is equiprobable, i.e., all preimages $F^{-1}(z)$, $z \in M$, have the same cardinality $\frac{|N|}{|M|}$;
- the initial state (a seed) u_0 is an arbitrary element of N.

Under these conditions the output sequence

$$\mathcal{S}(u_0) = \{F(u_0), F(f(u_0)), F(f^{(2)}(u_0)), \ldots, F(f^{(j)}(u_0)), \ldots\}$$

of the automaton $\mathfrak{A}$ is strictly uniformly distributed over M i.e., $\mathcal{S}(u_0)$ is a purely periodic sequence, $|N|$ is its period length, and every element $z \in M$ occurs at the period exactly $\frac{|N|}{|M|}$ times, see 2.3.

Congruential generator of a maximum period length. This corresponds to a case when $N = M$, f is compatible and transitive mapping of the residue ring $\mathbb{Z}/|N|$ onto itself, and F is an identical transformation (we identify N with $\mathbb{Z}/|N|$ in an obvious manner). This generator is said to be *congruential* since the algebraic notion of compatibility just means that f preserves all congruences of the ring $\mathbb{Z}/|N|$, i.e. for all $a, b \in N$, $a \equiv b \pmod d \Rightarrow f(a) \equiv f(b) \pmod d$ whenever $d \,\big|\, |N|$.

4.1. *Note.* In order to avoid future misunerstanding it is important to emphasize here that *our notion of a congruential generator differs from one of Krawczyk*, [14]. According to the latter paper, a (general) congruential generator is a number generator for which the i^{th} element s_i of the sequence is a $\{0,1,\ldots,m-1\}$-valued number computed by the congruence

$$s_i \equiv \sum_{j=1}^{k} \alpha_j \Phi_j(s_{-n_0},\ldots,s_{-1},s_0,\ldots,s_{i-1}) \pmod m, \tag{4.1.1}$$

where $\alpha_j \in \mathbb{Z}$, $m \in \{2,3,\ldots\}$ and Φ_j, $1 \le j \le k$ is an arbitrary integer-valued function. Note that this definition could be restated in the equivalent form: a (general) congruential generator is a number generator for which the i^{th} element s_i of the output sequence is computed by the congruence

$$s_i \equiv \Phi(s_{-n_0},\ldots,s_{-1},s_0,\ldots,s_{i-1}) \pmod m,$$

where, as Krawczyk notes (see [14, page 531]), Φ is an *arbitrary* integer-valued function that works on *finite sequences* of integers. Thus, *according to Krawczyk's definition, an arbitrary infinite sequence over* $\{0,1,\ldots,m-1\}$ *should be considered as a congruential generator*. Such a definition is too general for the purposes of our paper. Results of [14] in connection with a problem of predictability of the generators considered in this paper will be discussed later.

So *further in the paper a congruential generator is assumed to be the automaton* $\mathfrak{A}$ *such that* $M = N$*,* $F : M \to M$ *is a trivial permutation, and state transition function* f*, being considered as a mapping of the residue ring* $\mathbb{Z}/|N|$ *into itself, preserves all congruences of this ring.*

In case the number of states is composite, $|N| = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, p_j prime, $j = 1,2,\ldots,t$, this generator could obviously be represented as a direct product of congruential generators with prime power state set: $\mathbb{Z}/|N| = \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_t^{n_t}$, and $f = f_1 \times \cdots \times f_t$, where $f_j = (\tilde{f}_j) \bmod p_j^{n_j}$, $\tilde{f}_j \colon \mathbb{Z}_{p_j} \to \mathbb{Z}_{p_j}$ is a compatible and ergodic mapping, $j = 1,2,\ldots,t$.

Example. For $N = 10^k = 2^k \cdot 5^k$ the mapping $f(x) = 11x + 11^x$ is transitive modulo 10^k for all $k = 1,2,\ldots$ (see 3.3 and a note thereafter).

Thus, the case of composite number of states could be reduced to the case when a number of states is a power of a prime, i.e., when $|N| = p^n$. An obvious disadvantage of this congruential generator is that the *period length of the sequence* $\{\delta_j(f^{(i)}(u_0)) : i = 0,1,2,\ldots\}$ (where $\delta_j(z)$ stands for the j^{th} digit of the base-p expansion of z) *is exactly* p^{j+1}*, i.e., only the most significant bit of the output sequence has a maximum period length*, which is obviously equal to the period of the whole output sequence.

While being not very significant in case the output sequence is applied to simulation tasks (espesially if one uses the sequence $\left\{\frac{f^{(i)}(u_0)}{p^n}\right\}$; the latter use is common for numerical experiments), this disadvantage in general leads to a cryptographic insecurity of the generator whenever the function f is known to a cryptoanalyst. Indeed, to solve a congruence $z \equiv f(x) \pmod{p^n}$ (and as a result to find a key, which is an initial state u_0 in this case) one might use a version of p-adic Newton's method (the latter is a base of a canonical proof of Hensel's lemma).

Namely, one solves a congruence $z \equiv f(x) \pmod p$, thus finding the least significant digit $\delta_0(x)$ of x. Provided $\delta_j(x)$ for $j = 0,1,\ldots,k-1$ are already found, to find $\delta_k(x)$ one has to find a (unique) solution of a congruense $z \equiv f(\hat{x}) + p^k \check{f}_k(\hat{x}, \delta_k(x))$ $\pmod{p^{k+1}}$, where $\hat{x} = \delta_0(x) + \delta_1(x) \cdot p + \cdots + \delta_{k-1}(x) \cdot p^{k-1}$ and the mapping $\check{f}_k(\cdot,\cdot) \colon \mathbb{Z}/p^k \times \mathbb{Z}/p \to \mathbb{Z}/p$ is uniquely determined by f. Of course, to express explicitly $\check{f}_k(\cdot,\cdot)$ is a separate problem, yet it is easy in a number of important cases. For instance, $\check{f}_k(\hat{x}, \delta_k(x)) = \delta_k(x)$ in case $p = 2$ (see 3.25).

We may also consider a case when f is not is known to a cryptoanalyst: e.g., for $p = 2$ one may take $f = 1 + x + 4g(x)$, where $g(x)$ is a compatible key-dependent function, which is not known to a cryptoanalyst. Such function f is ergodic, see 3.15. This situation is a little better in comparison with a known f. However, the sequence formed of less significant bits of $f^{(i)}(u_0)$ is predictable in both directions, i.e. knowing k members of the sequence $\{f^{(i)}(u_0)\}$ a cryptoanalyst finds $\delta_j(f^{(i)}(u_0))$ for all $j < \log_2 k$ and all $i = 0, 1, 2, \dots$, stretching the corresponding periods in both directions. Thus, a good idea is to discard less significant bits of the output sequence: Note that methods of [14], as it is directly pointed out there, do not apply to generators that output only parts of the numbers generated. So we come to the notion of

Truncated congruential generator of a maximum period length. The latter is an automaton $\mathfrak{A}$ such that $|N| = p^n$, p prime, $|M| = p^m$, $m < n$, $f = (\tilde{f}) \bmod p^n$, f is a compatible and ergodic mapping of $\mathbb{Z}_p$ onto itself, $F(u) = \left\lfloor \frac{u}{p^{n-m}} \right\rfloor$, $u \in \{0, 1, \dots, p^n - 1\}$. Note that the function F is not compatible, yet equiprobable, so the output sequence, considered as a sequence over $\mathbb{Z}/p^m$, is purely periodic with period length exactly p^n, and each element of $\mathbb{Z}/p^m$ occurs at the period exactly p^{n-m} times. In this paper we are mainly focused at the case $p = 2$.

An important example of such an output function F is the mapping $\delta_j \colon \mathbb{Z}_2 \to \mathbb{Z}/2$. It returnes the j^{th} digit of z and is obviously equiprobable. We call the corresponding sequence $\{\delta_j(f^{(i)}(z)) : i = 0, 1, 2, \dots\}$ the j^{th} *coordinate sequence*, since the sequence $\{f^{(i)}(z) : i = 0, 1, 2, \dots\}$ could be thought of as a sequence of vectors $\{(\delta_0(f^{(i)}(z)), \delta_1(f^{(i)}(z)), \dots) : i = 0, 1, 2, \dots\}$ over a field $\mathbb{Z}/2$ of two elements. Of course, the use of δ_j as an output function of the automaton $\mathfrak{A}$ significantly reduces the performance, and the corresponding pseudorandom generator might be not of much practical value. Nonetheless, we have to study coordinate sequences to be able to prove certain important properties of output sequences of pseudorandom generators considered in the paper. In particular, while studying probabilstic quality of output sequences of truncated congruential generators one has to study correlations among coordinate sequences. We postpone these issues to Section 5.

A truncation usually makes generators slower but more secure: general methods that predict truncated congruential generators are not known, see [5],[12]. However, such methods exist in some particular cases, for instance, when f is a polynomial over $\mathbb{Z}$ of degree 1, and/or a relatively small part of less significant bits are discarded, see [21]. However, in general truncated congruential generators seem to be rather secure even their state transition function is relatively simple: For instance, an analysis made in [20] shows that for $f(x) = (x + (x^2 \vee C)) \bmod 2^n$ the corresponding stream cipher is quite strong against a number of attacks. Note also that in generators we study here both the state transition function and output function could be keyed.

Wreath products of congruential generators. This construction enables one to construct pseudorandom generators such that their state transition function (and output function) is being modified dynamically while working, i.e. generators with recurrence sequence of states satisfying a congruence

$$x_{i+1} \equiv f_i(x_i) \pmod{2^n}.$$

Such generators are called *counter-dependent*, see [13, Definition 2.4]. The problem here is how to guarantee period length (and statistical quality) of this sequence $\{x_i\}$. The construction we introduce below offers a certain solution to this problem; the idea of the construction goes back to wreath products of permutation groups. The exact definition (which could be found in, e.g., [22]) is not needed within a context of this paper; we note, however, that this construction is just a permutation that belongs to a wreath product of a Sylow 2-subgroup of a symmetric group on 2^n elements by a cyclic group.

The idea of the construction is the following: Consider a (finite or infinite) sequence of automata $\mathfrak{A}_j = \langle N, M, f_j, F_j\rangle$, $j \in J = \{0, 1, 2, \dots, \}$ (where J is finite, or $J = \mathbb{N}_0$). Note that all the automata $\mathfrak{A}_j$ have the same state set N and the same output alphabet M. Now produce the following sequence $\{z_i \colon i = 1, 2, \dots\}$: Choose an arbitrary $u_0 \in N$ and put

$$z_0 = F_0(u_0), u_1 = f_0(u_0); \dots z_i = F_i(u_i), u_{i+1} = f_i(u_i); \dots$$

That is, at the $(i+1)^{\text{th}}$ step the automaton $\mathfrak{A}_i$ is applied to the state u_i producing a new state $u_{i+1} = f_i(u_i)$ and outputting a symbol $z_i = F_i(u_i)$.

Now we give a more formal

4.2. **Definition.** Let $\mathfrak{A}_j = \langle N, M, f_j, F_j\rangle$ be a family of automata with the same state set N and the same output alphabet M indexed by elements of a non-empty (possibly, countably infinte) set J (members of the family are not necessarily pairwise distinct). Let $T \colon J \to J$ be an arbitrary mapping. A *wreath product* $\mathfrak{A}_j \wr_{j\in J} T$ of the family $\{\mathfrak{A}_j\}$ of the automata by the mapping T is an automaton with state set $N \times J$, state transition function $\breve{f}(j, z) = (f_j(z), T(j))$ and output function $\breve{F}(j, z) = F_j(z)$. The state transition function $\breve{f}(j, z) = (f_j(z), T(j))$ is called a *wreath product of family of mappings* $\{f_j \colon j \in J\}$ *by the mapping* T; it is denoted as $\breve{f} = f_j \wr_{j\in J} T$.

It worth noticing here that if $J = \mathbb{N}_0$ and F_i does not depend on i, this construction will give us a number of examples of counter-dependent generators in a sence of [13, Definition 2.4]. Note also that generators we consider in this subsection are counter-dependent in a broader sence: Not only their state transition functions depend on i, but their output functions as well.

In fact, we are already familiar with wreath products of mappings: See the following

Example. Let $J = \mathbb{Z}/2^n$, let $T \colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ be an arbitrary compatible permutation with a single cycle. Put $N = \{0, 1\}$, $f_z(u) = u \oplus \beta(z)$, where $u \in N$ and $\beta(z) = \beta(\delta_0(z), \dots, \delta_{n-1}(z))$ is a Boolean polynomial of degree n in n Boolean variables (so $\{f_z\}$ is a family of linear congruential generators modulo 2). Then $\breve{f} = f_z \wr_{z\in J} T$ could be considered as a mapping of $\mathbb{Z}/2^{n+1}$ onto itself (we identify $(\varepsilon, z) \in N \times J$ with $z + \varepsilon \cdot 2^n \in \mathbb{Z}/2^{n+1}$); moreover, $\breve{f}$ is a compatible permutation on $\mathbb{Z}/2^{n+1}$ with a single cycle in view of 3.13. Thus, every compatible and ergodic mapping modulo 2^k could be obtained by succesive application of wreath products. In fact, all compatible mappings of $\mathbb{Z}/2^{n+1}$ onto itself form a group $Syl_2(2^{n+1})$ with respect to a composition. This group is a Sylow 2-subgroup of a symmetric group $Sym(2^{n+1})$ on $\mathbb{Z}/2^{n+1}$; it is known (see e.g. [22]) that

$$Syl_2(2^{n+1}) = \underbrace{Sym(2) \wr Sym(2) \wr \cdots \wr Sym(2)}_{n+1 \text{ factors}}.$$

Here $\wr$ stands for the wreath product of groups.

A generalization of the above example gives the following

4.3. **Proposition.** *Let* $T\colon \mathbb{Z}/2^m \to \mathbb{Z}/2^m$*,* $m \geq 1$*, be an arbitrary permutation with a single cycle, let* $\{c_0, \ldots, c_{2^m-1}\}$ *be a finite sequence of* 2*-adic integers, and let* $\{f_0, \ldots, f_{2^m-1}\}$ *be a finite sequence of compatible mappings of* $\mathbb{Z}_2$ *onto itself. Put* $H_j(x) = c_j + x + 4 \cdot f_j(x)$*. Then the wreath product* $H_j \wr_{j=0}^{2^m-1} T$ *defines a bijective mapping* $W\colon \mathbb{Z}_2 \twoheadrightarrow \mathbb{Z}_2$

$$W(x) = T(x \bmod 2^m) + 2^m \cdot H_{x \bmod 2^m}\left(\left\lfloor \frac{x}{2^m} \right\rfloor\right);$$

this mapping is asypmtotically compatible and asymptotically ergodic (i.e., $a \equiv b \pmod{2^k} \Rightarrow W(a) \equiv W(b) \pmod{2^k}$ and W is transitive modulo 2^k for all sufficiently large k; in fact, for all $k > m$, see [7, 6, 16] for definitions) *if and only if* $\sum_{j=0}^{2^m-1} c_j \equiv 1 \pmod 2$.

In other words, every recurrence sequence $\mathcal{U}_n = \{x_i\}$ *defined by the relation*

$$x_{i+1} = H_{i \bmod 2^m}(x_i) \bmod 2^n$$

is strictly uniformly distributed sequence over $\mathbb{Z}/2^n$ *of period length exactly* 2^{n+m} *if and only if* $\sum_{j=0}^{2^m-1} c_j \equiv 1 \pmod 2$*.*

Proof. Since wreath product of permutations on sets N and M is a permutation on the direct product $N \times M$ (see 4.2), the sequence $\mathcal{U}_n$ is purely periodic. Moreover, since the permutations T and $I\colon z \mapsto (z+1) \bmod 2^m$ are conjugate in $Sym(2^m)$, and thus both wreath products $(H_j \bmod 2^n) \wr_{j=0}^{2^m-1} T$ and $(H_j \bmod 2^n) \wr_{j=0}^{2^m-1} I$ have the same cycle structure (the same number of cycles of length ℓ, for all $\ell = 1, 2, \ldots$), it is suffisient to study a period of a sequence $x_{i+1} = H_i(x_i) \bmod 2^n$, assuming $H_i = H_{i \bmod 2^m}$ for $i \geq 2^m$. Further, since $W_n = (H_j \bmod 2^n) \wr_{j=0}^{2^m-1} I \in Syl_2(2^{n+m})$, the period length of the sequence $\{x_i\}$ is a power of 2. Finally, since the mapping $W_n\colon \mathbb{Z}/2^{n+m} \to \mathbb{Z}/2^{n+m}$ is compatible, it is necessary and sufficient to understand when W_n is transitive modulo 2^{n+m} for all $k = n + m$. Yet the mapping W_n could be considered as a function of a variable $z = i + 2^m \cdot x \in \mathbb{Z}/2^{m+n}$, where $i \in \{0, 1, \ldots, 2^m - 1\}$ and $x \in \{0, 1, \ldots, 2^n - 1\}$. Thus, we could apply 3.13 to study transitivity of W_n. Since $W_n(z) \equiv z + 1 \pmod{2^m}$ by the definition, we only have to calculate $\delta_j(H_i(x))$.

One has $\delta_0(c_i + x) \equiv \chi_0 + \beta(i) \pmod 2$ and

$$\delta_j(c_i + x) \equiv \chi_j + \beta(i)\chi_0 \cdots \chi_{j-1} + \gamma_{ji}(\chi_0, \ldots, \chi_{j-1}) \pmod 2 \qquad (j > 0),$$

where $\chi_j = \delta_j(x)$, $\beta(i) = \delta_0(c_i)$, $\gamma_{ji}(\chi_0, \ldots, \chi_{j-1})$ is a Boolean polynomial of degree $< j$ in Boolean variables $\chi_0, \ldots, \chi_{j-1}$. Yet $\delta_i(4 \cdot g_j(x))$ is a Boolean polynomial in Boolean variables $\chi_0, \ldots, \chi_{j-2}$ for $j \geq 2$, and is 0 otherwise. Thus,

$$\delta_j(H_i(x)) \equiv \chi_j + \beta(i)\chi_0 \cdots \chi_{j-1} + \lambda_{ji}(\chi_0, \ldots, \chi_{j-1}) \pmod 2, \tag{4.3.1}$$

where $\deg \lambda_{ji} < j$, $j = 1, 2, \ldots$, and $\delta_0(H_i(x)) \equiv \chi_0 + \beta(i) \pmod 2$.

Assuming $\zeta_r = \delta_r(z)$ for $r = 0, 1, \ldots, m + n - 1$ one can consider $\beta(i)$ for $i \in \{0, 1, \ldots, 2^m - 1\}$ as a Boolean polynomial in Boolean variables $\zeta_0, \ldots, \zeta_{m-1}$; similarly, λ_{ji} could be considered as a Boolean polynomial in Boolean variables $\zeta_0, \ldots, \zeta_{m+j-1}$. Since the degree of λ_{ji} in variables $\chi_0, \ldots, \chi_{j-1}$ is less than j (see the argument above), the degree of this polynomial in variables $\zeta_0, \ldots, \zeta_{m+j-1}$ is less than $m + j$. Thus, in view of 3.10 and (4.3.1), the mapping W_n is transitive iff $\deg\beta = m$, i.e., iff the Boolean polynomial β is of odd weight. Yet the latter is equivalent to the condition $\sum_{i=0}^{2^m-1}\beta(i)\equiv 1 \pmod 2$. This proves the proposition since $\sum_{i=0}^{2^m-1}\beta(i)\equiv\sum_{i=0}^{2^m-1}c_i \pmod 2$. □

Two important notes worth being stated here. The first of them concerns further generalizations of proposition 4.3

4.4. *Note.* The proof of 4.3 shows that *the proposition holds if H_j satisfy the following conditions: $\sum_{j=0}^{2^m-1}H_j(0)\equiv 1 \pmod 2$ and $\delta_i(H_j(x))\equiv\delta_i(x)+\rho_i(j;x) \pmod 2$ $(i=0,1,2\ldots)$, where the Boolean polynomial ρ_i in Boolean variables $\delta_r(j)$, $\delta_s(x)$ $(r\in\{0,1,\ldots,m-1\},\ s\in\{0,1,\ldots,i-1\})$ is of odd weight for $i>0$* (see the argument proving (4.3.1) and text thereafter). In oder to satisfy the latter condition of these one can take e.g. $H_j(x)=x+h_j(x)$, where every $\delta_i(h_j)$ is a Boolean polynomial of even weight in Boolean variables $\delta_0(x),\ldots,\delta_{i-1}(x)$ [6]. Also, one can assume in conditions of 4.3 that, e.g., $H_j=(c_j+x)\oplus(2\cdot g_j(x))$ (or $H_j=c_j+x+2\cdot g_j(x)$) for measure preserving g_j, etc.

Example. Let $H_j(x)=c_j+x+(x^2\vee C_j)$, where $\sum_{j=0}^{2^m-1}c_j\equiv 1 \pmod 2$ and $C_j\equiv 7 \pmod 8$, then the recurrence sequence defined by $x_{i+1}=c_{i \bmod 2^m}+x_i+(x_i^2\vee C_{i \bmod 2^m})$ is strictly uniformly distributed modulo 2^n. It is sufficient to note only that $x^2\vee 7$ is an even parameter, see [20]. This example is a variation of theme of theorem 3 there, which considers similar problem for the sequence defined by relation $x_{i+1}=(x_i+(x_i^2\vee C_{i \bmod m})) \bmod 2^n$ with odd m (the case when T acts on a set of odd order is discussed below).

The second important note relates wreath products and truncation.

4.5. *Note.* From the proof of proposition 4.3 immediately follows that *each recurrence sequence $\mathcal{X}_n$ defined by $x_{i+1}=f_{i \bmod 2^m}(x_i) \bmod 2^n$ with compatible f_i could be obtained by a truncation of m low order bits of the recurrence sequence defined by $z_{i+1}=G(z_i) \bmod 2^{n+m}$ for a suitable compatible mapping $G\colon\mathbb{Z}_2\to\mathbb{Z}_2$.* However, in practice it could be more convenient to produce the sequence according to the law $x_{i+1}=f_{i \bmod 2^m}(x_i) \bmod 2^n$ than to the law $z_{i+1}=G(z_i) \bmod 2^{n+m}$ with further truncation, since the mapping G could be extremely complicated despite all f_i are relatively simple. As a bonus we have also that *all the results that are established further in the paper for truncated congruential generators remain true for generators of form $x_{i+1}=f_{i \bmod 2^m}(x_i) \bmod 2^n$.*

Using ideas of proposition 4.3 it is possible to handle a case when T acts on a set of odd order.

4.6. **Proposition.** *Let $m>1$ be odd; let, further, $\{f_0,\ldots,f_{m-1}\}$ be a finite sequence of compatible and ergodic mappings of $\mathbb{Z}_2$ onto itself, and let $\{d_0,\ldots,d_{m-1}\}$ be a finite sequence of 2-adic integers such that*

- *$\sum_{j=0}^{m-1}d_j\equiv 0 \pmod 2$, and*
- *the sequence $\{d_{i \bmod m} \bmod 2\colon i=0,1,2,\ldots\}$ is purely periodic with period length exactly m.*

Put $H_j(x)=d_j\oplus f_j(x)$ (respectively, $H_j(x)=d_j+f_j(x)$). Then the wreath product $(H_j \bmod 2^n)\wr_{j=0}^{m-1}I$, where $I(j)=(j+1) \bmod m$, defines a permutation $W\colon\mathbb{Z}/2^nm\twoheadrightarrow\mathbb{Z}/2^nm$ with a single cycle.

---

[6] Such mappings h_j are called *even parameters* in [20]

Moreover, a recurrence sequence $\mathcal{W}_n = \{x_i \in \mathbb{Z}/2^n\}$ *defined by the relation*

$$x_{i+1} = H_{i \bmod m}(x_i) \bmod 2^n$$

is a strictly uniformly distributed purely periodic sequence with period length exactly $2^n m$ *such that every element of* $\mathbb{Z}/2^n$ *occurs at the period exactly* m *times.*

Obviously, it is sufficient to prove only the second part of the statement. We need the following

4.7. **Lemma.** *Let* $g_0, \dots, g_{m-1}$ *be a finite sequence of compatible mappings of* $\mathbb{Z}_2$ *onto itself such that*

- $g_j(x) \equiv x + c_j \pmod 2$ *for* $j = 0, 1, \dots, m-1$,
- $\sum_{j=0}^{m-1} c_j \equiv 1 \pmod 2$,
- *the sequence* $\{c_{i \bmod m} \bmod 2 \colon i = 0, 1, 2, \dots\}$ *is purely periodic with period length exactly* m,
- $\delta_k(g_j(z)) \equiv \zeta_k + \varphi_k^j(\zeta_0, \dots, \zeta_{k-1}) \pmod 2$, $k = 1, 2, \dots$, *where* $\zeta_r = \delta_r(z)$, $r = 0, 1, 2, \dots$,
- *for each* $k = 1, 2, \dots$ *an odd number of Boolean polynomials* $\varphi_k^j(\zeta_0, \dots, \zeta_{k-1})$ *in Boolean variables* $\zeta_0, \dots, \zeta_{k-1}$ *are of odd weight.*

Then a recurrence sequence $\mathcal{Y} = \{x_i \in \mathbb{Z}_2\}$ *defined by a relation* $x_{i+1} = g_{i \bmod m}(x_i)$ *is a strictly uniformly distributed sequence over* $\mathbb{Z}_2$*: it is purely periodic modulo* 2^k *for all* $k = 1, 2, \dots$ *with period length exactly* $2^k m$*, and with each element of* $\mathbb{Z}/2^k$ *occuring at the period exactly* m *times. Moreover,*

1. $2^{s+1}m$ *is a* (not necessarily exact, see definition 2.4) *period length of the sequence* $\mathcal{D}_s = \{\delta_s(x_i) \colon i = 0, 1, 2, \dots\}$ $(s = 0, 1, \dots, k-1)$,
2. $\delta_s(x_{i+2^s m}) \equiv \delta_s(x_i) + 1 \pmod 2$ *for all* $s = 0, 1, \dots, k-1$, $i = 0, 1, 2, \dots$,
3. *for each* $t = 1, 2, \dots, k$ *and each* $r = 0, 1, 2, \dots$ *the sequence*

   $$x_r \bmod 2^t, x_{r+m} \bmod 2^t, x_{r+2m} \bmod 2^t, \dots$$

   is a purely periodic sequence of period length exactly 2^t*, and each element of* $\mathbb{Z}/2^t$ *occurs at the period exactly once.*

Note. In view of 3.13 the conditions of the lemma imply that all the mappings g_j preserve measure.

Proof of lemma 4.7. Since every g_j induces a permutation modulo 2^n (see 3.13), the wreath product $(g_j \bmod 2^k) \wr_{j=0}^{m-1} I$ is a permutation R_k on $\mathbb{Z}/m \times \mathbb{Z}/2^k$; hence, the recurrence sequence $\mathcal{Y}_k$ defined by a relation $x_{i+1} = g_{i \bmod m}(x_i) \bmod 2^k$ is purely periodic.

We continue the proof of the lemma with induction on k. For $k = 1$ one has

$$x_{i+1} = (c_{i \bmod m} + x_i) \bmod 2,$$

Thus, $x_i \equiv x_0 + \sum_{j=0}^{i-1} c_{j \bmod m} \pmod 2$, and we have to calculate an exact length P of a period of a sequence $b_i = (\sum_{j=0}^{i-1} c_{j \bmod m}) \bmod 2$ (see definition 2.4). Yet $0 \equiv \sum_{j=i}^{P+i-1} c_{j \bmod m} \pmod 2$ for all i; this means that the sequence $\mathcal{C} = \{c_{j \bmod m} \bmod 2\}$ is a linear recurrence sequence over a field $\mathbb{Z}/2$ with characteristic polynomial $1 + y + \cdots + y^{P-1} \in (\mathbb{Z}/2)[y]$ (see e.g. [17] for definitions). Since the latter polynomial is a factor of a polynomial $y^P - 1$, P is a period length of the sequence $\mathcal{C}$. Yet m is an exact period length of the sequence $\mathcal{C}$, so m must be a factor of P. Yet $x_{i+m} \equiv x_0 + \sum_{j=0}^{m-1} c_{j \bmod m} \equiv x_0 + 1 \pmod 2$, and $x_{i+2m} \equiv x_0 + 2 \cdot \sum_{j=0}^{m-1} c_{j \bmod m} \equiv x_0$

(mod 2); thus, $P = 2m$. This proves the lemma for $k = 1$, since $\mathcal{D}_0 = \mathcal{Y}_1$ in this case.

Now let the lemma be true for $k = n$; consider $k = n + 1$. Denote $\delta_n(x_i) = \chi_n^i$, then

$$\chi_n^i \equiv \chi_n^0 + \sum_{j=0}^{i-1} \varphi_n^j(\chi_0^j, \dots, \chi_{n-1}^j) \pmod 2. \tag{4.7.1}$$

Since by the induction hypothesis the period length of the sequence $\mathcal{Y}_n$ is exactly $2^n m$, and since all g_j are compatible, the period length of $\mathcal{Y}_{n+1}$ is a multiple of $2^n m$; thus only two cases are possible: the exact period length of $\mathcal{Y}_{n+1}$ is either $2^{n+1}m$, or it is $2^n m$. We shall prove that the latter case does not take place. To do this we only have to demonstrate that $\chi_n^{2^m n} \not\equiv \chi_n^0 \pmod 2$. In view of the induction hypothesis one has

$$\chi_n^{2^n m+r} \equiv \chi_n^r + \sum_{j=r}^{2^n m-1+r} \varphi_n^j(\chi_0^j, \dots, \chi_{n-1}^j) \equiv \\ \chi_n^r + \sum_{j=0}^{m-1} \sum_{z\in\mathbb{Z}/2^n} \varphi_n^j(\zeta_0, \dots, \zeta_{n-1}) \equiv \chi_n^r + 1 \pmod 2, \tag{4.7.2}$$

for all $r = 0, 1, 2, \dots$, since an odd number of Boolean polynomials $\varphi_n^0, \varphi_n^1, \dots \varphi_n^{m-1}$ are of odd weight. This proves (2) of the lemma's statement; also, as (4.7.2) implies $\chi_n^{2^m n} \not\equiv \chi_n^0 \pmod 2$, the exact period length of $\mathcal{Y}_{n+1}$ is $2^{n+1}m$ in view of the above note. Morover, congruence (4.7.2) implies $\chi_n^{2^{n+1}m+r} \equiv \chi_n^r \equiv \pmod 2$, thus proving claim (1) of the lemma. Last, by claim (3) of the induction hypothesis the following string of $2^n m$ numbers

$$x_r \bmod 2^n, x_{r+m} \bmod 2^n, x_{r+2m} \bmod 2^n, \dots, x_{r+(2^n-1)m} \bmod 2^n$$

is a permutation of $0, 1, 2, \dots, 2^n - 1$. Hence, all the numbers

$$x_r, x_{r+m}, x_{r+2m}, \dots, x_{r+(2^n-1)m}$$

are pairwise distict modulo 2^{n+1}. Thus, for each $z \in \{0, 1, \dots, 2^n - 1\}$ among the numbers

$$x_r, x_{r+m}, x_{r+2m}, \dots, x_{r+(2^{n+1}-1)m} \tag{4.7.3}$$

there exist exactly two numbers (say, x_u and x_v) such that $u \neq v$ and $z \equiv x_u \equiv x_v \pmod{2^n}$. Thus, $u \equiv v \pmod{2^n m}$ in view of claim (3) of the induction hypothesis. Hence necessarily $v = u + \cdot 2^n m$. But then $x_u \not\equiv x_v \pmod{2^{n+1}}$, since $\delta_n(x_v) \equiv \delta_n(x_v) + 1 \pmod 2$ in view of (4.7.2). Thus, all 2^{n+1} numbers of (4.7.3) are pairwise distinct modulo 2^{n+1}. This proves claim (3) of the lemma.

Since, as we have already proved, the sequence $\mathcal{Y}_{n+1}$ is purely periodic with period length exactly $2^{n+1}m$, a finite sequence

$$x_0 \bmod 2^{n+1}, x_1 \bmod 2^{n+1}, \dots, x_{2^{n+1}-1} \bmod 2^{n+1}$$

is a period of $\mathcal{Y}_{n+1}$. But according to already proven claim (3), among these numbers there exist exactly m numbers that are congruent to z modulo 2^{n+1} for each given $z \in \{0, 1, \dots, 2^{n+1} - 1\}$. This completes the proof of the lemma. □

Note. Nowhere in the proof of lemma 4.7 we used that m is odd. Hence, the lemma holds for arbitrary, and not necessarily odd $m > 1$.

Proof of proposition 4.6. The proof of proposition 4.6 for a case $H_j(x) = d_j \oplus f_j(x)$ is now obvious in view of 3.13 and lemma 4.7: Note only that the sequence $\{d_j + 1\colon j = 0, 1, 2, \dots\}$ satisfies conditions of the lemma. So to finish the proof we only have to consider a case $H_j = d_j + f_j(x)$.

The proof in the latter case goes along the lines similar to those of lemma 4.7. Namely, for $n = 1$ one has $x_{i+1} = (d_{i \bmod m} + x_i + 1) \bmod 2$, since every ergodic mapping modulo 2 is equivalent to the mapping $x \mapsto x + 1$, see 3.10; so putting $c_i = d_i + 1$ returns us to the situation of lemma 4.7 whenever $n = 1$.

Assuming the proposition is true for $n = k$ prove it for $n = k + 1$. In view of 3.13 we have that for $s > 0$

$$\delta_s(H_j(x)) \equiv \chi_s + (d_j + 1)\chi_0 \cdots \chi_{s-1} + \psi_s^j(\chi_0, \dots, \chi_{s-1}) \pmod 2,$$

where $\deg \psi_s^j < s$ (this congruence could be easily proved by induction on s: the coefficient of the monomial $\chi_0 \cdots \chi_{s-1}$ in the Boolean polynomial that represents a carry to s^{th} digit is $\delta_0(d_j)$). Thus, for $k \ge 1$ one obtains

$$\chi_k^{2^k m} \equiv \chi_k^0 + \sum_{j=0}^{2^k m-1} (d_{j \bmod m} + 1)\chi_0^j \cdots \chi_{k-1}^j + \sum_{j=0}^{2^k m-1} \psi_k^j(\chi_0^j, \dots, \chi_{k-1}^j) \equiv$$

$$\chi_k^0 + \sum_{j=0}^{m-1} (d_j + 1) \sum_{z \in \mathbb{Z}/2^k} \zeta_0 \cdots \zeta_{k-1} + \sum_{j=0}^{m-1} \sum_{z \in \mathbb{Z}/2^k} \psi_k^j(\zeta_0, \dots, \zeta_{k-1}) \equiv$$

$$\chi_k^0 + 1 \pmod 2,$$

since all Boolean polynomials $\psi_k^j(\zeta_0, \dots, \zeta_{k-1})$ are of even weight. This completes the proof of the proposition. □

Example. A mapping $g_j(x) = x + (x^2 \vee C_j)$ is ergodic iff $\delta_0(C_j) = 1$ and $\delta_2(C_j) = 1$ (see 3.14). Let a sequence $\{d_j\colon j = 0, 1, 2, \dots\}$ satisfy conditions of proposition 4.6. Then the sequence $\{x_{i+1} = x_i + d_i + (x_i^2 \vee C_i) \bmod 2^n\colon i = 0, 1, 2, \dots\}$ is purely periodic modulo 2^k for all $k = 1, 2, \dots$ with period length $2^k m$, and each element of $\mathbb{Z}/2^k$ occurs at the period exactly m times.

This is another variation of theme of [20, Theorem 3]. Note that we prove a somewhat stronger claim: Not only a sequence of pairs (y_i, x_i) defined by $y_{i+1} = (y_i + 1) \bmod m$; $x_{i+1} = (x_i + d_i + (x_i^2 \vee C_{y_i})) \bmod 2^n$ is periodic with period length $2^n m$, yet the period length of the sequence $\{x_i\}$ is $2^n m$. The latter could never be achieved under the conditions of Theorem 3 of [20]: They imply that the period length of the sequence $\{x_i \pmod 2\}$ is 2, and not $2m$.

Note. Obviously, after corresponding restatement proposition 4.6, as well as lemma 4.7, remain true for arbitrary permutation $I\colon \mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/m$ with a single cycle.

In connection with proposition 4.6 there arises a natural question: how to construct a sequence $\{d_j\}$ that satisfies its conditions?

4.8. **Proposition.** *Let $m > 1$ be odd, and let $u\colon \mathbb{Z}/m \to \mathbb{Z}/m$ be an arbitrary permutation with a single cycle. Choose arbitrary $z \in \mathbb{Z}/m$ and set $d_i = u^{(i)}(z) \bmod m$, if $m \equiv 1 \pmod 4$, or set $d_i = (u^{(i)}(z) + 1) \bmod m$ otherwise $(i = 0, 1, 2, \dots)$. Then the sequence $\mathcal{D} = \{d_i\}$ satisfies conditions of proposition 4.6: that is, $\mathcal{D}$ is purely periodic with period length exactly m, and $\sum_{j=0}^{m-1} d_j \equiv 0 \pmod 2$.*

Proof. Obviously, the sequence $\mathcal{D}$ is purely periodic. Let P be the period length of $\mathcal{D}$. Thus, P is a factor of m. Note that since $m = 2s + 1$, exactly s numbers of

$0, 1, \dots, m-1$ are odd. Denote r_0 (respectively, r_1) the number of even (respectively, odd) numbers at the period of $\mathcal{D}$: so $\frac{m}{P}r_1 = s$, and $\frac{m}{P}r_0 = s+1$. Thus, $\frac{m}{P}(r_0 - r_1) = 1$; hence $\frac{m}{P} = 1$. So, the period length of $\mathcal{D}$ is exactly m. The result now follows since $\sum_{i=0}^{m-1} i \equiv 0 \pmod 2$ iff $s \equiv 0 \pmod 2$. □

4.9. *Note.* Thus, to construct a sequence $\{d_j\}$ of proposition 4.6 it is sufficient to construct a permutation with a single cycle modulo m. Of course, this could be done in various ways, depending on extra conditions the whole generator should satisfy. For instance, if one intends to use maximum of memory calls instead of computations on the fly, he can merely take an arbitrary array of $\{0, 1, \dots, m-1\}$ in arbitrary order. On the contrary, if one needs to produce d_j on the fly, he could construct a corresponding generator modulo m with a compatible state transition function and a bijective modulo m output function. This could be done e.g. with the use of 3.5, 3.7, 3.8, and 3.10. In case $m = 2^k - 1$ an alternative way is to use linear recurrence sequences of maximum period over $\mathbb{Z}/2$: note that often sequences of this kind could be constructed with the use of XOR's and left-right shifts only, see e.g. [23].

The above results of this subsection show how to construct a sequence $x_{i+1} = f_{i \bmod m}(x_i) \bmod 2^n$ of maximum period length $2^n m$ in two cases: when m is odd, and when $m = 2^k$. Now we consider a general case of arbitrary $m > 1$.

4.10. **Theorem.** *Let $\mathcal{G} = \{g_0, \dots, g_{m-1}\}$ be a finite sequence of compatible measure preserving mappings of $\mathbb{Z}_2$ onto itself such that*

1. *the sequence $\{(g_{i \bmod m}(0)) \bmod 2 \colon i = 0, 1, 2, \dots\}$ is a purely periodic sequence with period length exactly m;*
2. *$\sum_{i=0}^{m-1} g_i(0) \equiv 1 \pmod 2$;*
3. *$\sum_{j=0}^{m-1} \sum_{z=0}^{2^k-1} g_j(z) \equiv 2^k \pmod{2^{k+1}}$ for all $k = 1, 2, \dots$.*

Then the recurrence sequence $\mathcal{Z}$ defined by the relation $x_{i+1} = g_{i \bmod m}(x_i)$ is strictly uniformly distributed modulo 2^n for all $n = 1, 2, \dots$: i.e., modulo each 2^n it is a purely periodic sequence with period length exactly $2^n m$ and with each element of $\mathbb{Z}/2^n$ occuring at the period exactly m times.

Note. Since in view of 3.13 a compatible mapping $g_i \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ preserves measure iff

$$\delta_k(g_i(x)) \equiv \chi_k + \varphi_k^i(\chi_0, \dots, \chi_{k-1}) \pmod 2,$$

where $\chi_s = \delta_s(x)$ $(s = 0, 1, 2, \dots)$, the *condition* (3) *of theorem 4.10 could be replaced by the equivalent condition*

$$\sum_{j=0}^{m-1} \operatorname{wt} \varphi_k^j \equiv 1 \pmod 2 \qquad (k = 1, 2, \dots),$$

where $\operatorname{wt} \varphi_k^j$ is a weight of the Boolean polynomial φ_k^j in variables $\chi_0, \dots, \chi_{k-1}$. In turn, since for every Boolean polynomial φ in variables $\chi_0, \dots, \chi_{k-1}$ holds $\operatorname{wt} \varphi \equiv \operatorname{Coef}_{0,\dots,k-1}(\varphi) \pmod 2$, where $\operatorname{Coef}_{0,\dots,k-1}(\varphi)$ stands for a coefficient of the monomial $\chi_0 \cdots \chi_{k-1}$ in the Boolean polynomial φ, the *latter condition could be also replaced by*

$$\sum_{j=0}^{m-1} \operatorname{Coef}_{0,\dots,k-1}(\varphi_k^j) \equiv 1 \pmod 2 \qquad (k = 1, 2, \dots),$$

or by

$$\sum_{j=0}^{m-1}\left\lfloor\frac{\deg\varphi_k^j}{k}\right\rfloor\equiv 1 \pmod 2 \qquad (k=1,2,\ldots).$$

Proof of theorem 4.10. Practically everything is already done during the proof of 4.7: we just note that congruence (4.7.2) now holds in view of condition (3) of the theorem. □

Note. For $m=1$ theorem 4.10 turns into ergodicity criterion 3.13: so theorem 4.10 could be considered as a generalization of this criterion.

Theorem 4.10 is our main technical tool in constructing automata with strictly uniformly distributed recurrence sequences $x_{i+1}=f_i(x_i)$ of internal states outputting strictly uniformly distributed sequences of the form $F_0(x_0), F_1(x_1), \ldots$. The above mentioned results (e.g. 4.4and 4.6) could be derived from theorem 4.10, as well as new results for even m that is not power of 2 could also be obtained with the use of it:

Example. For instance, take odd s, $1\le s<m$, and take s arbitrary compatible and ergodic mappings $g_j\colon\mathbb{Z}_2\to\mathbb{Z}_2$, $(j=0,1,\ldots,s-1)$. Take $m-s$ arbitrary compatible and measure preserving mappings $h_k\colon\mathbb{Z}_2\to\mathbb{Z}_2$, and set $g_k(x)=x\oplus 2h_k(x)$ $(k=s,s+1,\ldots,m-1)$. Then in view of 3.13 it is easy to see that a finite sequence $\{g_i\colon i=0,1,\ldots,m-1\}$ satisfies conditions of theorem 4.10, and thus the recurrence sequence $x_{i+1}=g_{i \bmod m}(x_i)$ is strictly uniformly distributed modulo 2^n for all $n=1,2,\ldots$.

4.11. *Note.* During the proof of theorem 4.10 and of lemma 4.7 we have demonstrated that *every j^{th} coordinate sequence* $\mathcal{D}_j=\{\delta_j(x_i)\colon i=0,1,2,\ldots\}$ $(j=0,1,2,\ldots)$ *is a purely periodic binary sequence of period length $2^{j+1}m$, and the second half of the period is a bitwise negation of the first half*: $\delta_j(x_{i+2^jm})\equiv\delta_j(x_i)+1 \pmod 2$, $i=0,1,2,\ldots$ (see claims (1)–(2) of lemma 4.7). Note, however, that *the exact period length P of the sequence $\{\delta_j(x_i)\colon i=0,1,2,\ldots\}$ could actually be less than* $2^{j+1}m$, i.e., $P\big|2^{j+1}m$, yet not necessarily $P=2^{j+1}m$ (however, P is always a multiple of 2^{j+1}, see 5.6). Indeed, the sequence $101010\ldots$ is a purely periodic sequence with period 10 of length 2; at the same time it could be considered as a purely periodic sequence with period 101010 of length 6. Note that in both cases the second half of the period is a bitwise negation of its first half. Such an effect could never occur for $j=0$, since $\mathcal{D}_0=\mathcal{Y}_1$, and the latter sequence has period length exactly $2m$ in view of lemma 4.7. However, this effect could occur for senior coordinate sequences. For instanse, let $\mathcal{D}_0$ be a purely periodic sequence with period 111000; let $\mathcal{D}_1$ be a purely periodic sequence with period 110011001100. The exact period length of $\mathcal{D}_1$ is 4; yet it could be considered as a sequence of period 12, and the second half of the period is a bitwise negation of the first half. The sequence $\mathcal{Y}_2$ in this case is a purely periodic sequence with period 331022113200. It is not difficult to demonstrate that this sequence $\mathcal{Y}_2$ satisfy lemma 4.7, i.e., one could construct mappings g_0, g_1, g_2 satisfying the lemma, such that outputted sequence $\mathcal{Y}_2$ is our sequence with period 331022113200. A characterization of possible output sequences is given by theorem 5.10 further.

Finally we consider a case of wreath products of automata with non-identity output functions.

4.12**. Corollary.** *Let a finite sequence of mappings* $\{f_0, \ldots, f_{m-1}\}$ *of* $\mathbb{Z}_2$ *into itself satisfy conditions of theorem 4.10, and let* $\{F_0, \ldots, F_{m-1}\}$ *be an arbitrary finite sequence of equiprobable* (*and not necessarily compatible*) *mappings of* $\mathbb{Z}/2^n$ $(n \geq 1)$ *onto* $\mathbb{Z}/2^k$, $1 \leq k \leq n$. *Then the sequence* $\mathcal{F} = \{F_{i \bmod m}(x_i) \colon i = 0, 1, 2 \ldots\}$, *where* $x_{i+1} = f_{i \bmod m}(x_i) \bmod 2^n$, *is strictly uniformly distributed over* $\mathbb{Z}/2^k$: *It is purely periodic with period length* $2^n m$, *and each element of* $\mathbb{Z}/2^k$ *occurs at the period exactly* $2^{n-k}m$ *times.*

Proof. Obvious: combine claim (3) of lemma 4.7 and proposition 2.3. □

Note that the results of this subsection could be extended to cover the case p odd, that is, to the case of wreath products of the form $H_j \wr_{j=0}^{p^m-1} T$, where $T \colon \mathbb{Z}/p^m \to \mathbb{Z}/p^m$ (and even for $H_j \wr_{j=0}^{m-1} T$, where $T \colon \mathbb{Z}/m \to \mathbb{Z}/m$, $m > 1$ arbitrary rational integer). This case is also of cryptographic importance: the corresponding techniques could be used e.g. to construct sequences of type $\mathcal{D}$ of proposition 4.8. However, this is an issue of a forthcoming paper.

Equalizing period lengths of coordinate sequences. All the generators with the identity output function considered above demonstrate a property, which is already mentioned at the beginning this section, and which in loose terms could be stated as follows: *Less significant bits of output have smaller periods.* To be more exact, despite for any of these automata the corresponding output sequence $\mathcal{S} = \{s_0, s_1, \ldots\}$ over $\mathbb{Z}/2^n$ is always purely periodic of period length exactly $2^n\ell$ (where $\ell = 2^m$ for sequences outputted by wreath products of automata described by 4.3 or 4.5, $\ell = m$ in case the wreath products are of 4.6, 4.7, or 4.10, and $\ell = 1$ for congruential generators of a maximum period length), the j^{th} coordinate sequence $\delta_j(\mathcal{S}) = \{\delta_j(s_0), \delta_j(s_1), \ldots\}$ could be of smaller period length (see e.g. note 4.11 above). In fact, as it is shown further, the exact period length of the j^{th} coordinate sequence of congruential generator of a maximum period length is 2^{j+1} (see 5.1); it is a factor of $2^{j+1}\ell$ and a multiple of (which is possibly equal to) 2^{j+1} for wreath products of generators (see 5.6). So only senior coordinate sequence $\delta_{n-1}(\mathcal{S})$ may achieve exact period length $2^n\ell$; at least, the exact period length of it is not less than 2^n. Nothing more could be said either if we use general non-identity equiprobable output functions (see 2.3 and 4.12). However, such a "disbalance" of periods could be cured if we apply non-identity output functions in some special way.

Namely, let $\pi = \pi_n^1$ be a bit order reversing permutation on $\mathbb{Z}/2^n$, which was defined in section 2, and let h_i $(i = 0, 2, \ldots, m-1)$ be compatible and ergodic mappings of $\mathbb{Z}_2$ onto itself. Then the composition $F_i(x) \colon x \mapsto (h_i(\pi(x))) \bmod 2^n$ $(x \in \{0, 1, \ldots, 2^n - 1\})$ is a bijective mapping of $\mathbb{Z}/2^n$ onto itself. We argue that if we take F_i as an output function, then the sequence $\mathcal{F}$ of 4.12 is free of less significant bit effect mentioned above. To be more exact, the following proposition holds:

4.13**. Proposition.** *Let* h_i, $i = 0, 1, 2, \ldots, m-1$, *be compatible and ergodic mappings of* $\mathbb{Z}_2$ *onto itself. Define* $F_i \colon \mathbb{Z}/2^n \to \mathbb{Z}/2^n$ *by* $F_i(x) = (h_i(\pi(x))) \bmod 2^n$ $(x \in \{0, 1, \ldots, 2^n - 1\})$, *where* $\pi = \pi_n^1$ *is a bit order reversing permutation on* $\mathbb{Z}/2^n$ (see Section 2 for the definition of the latter). *Consider a sequence* $\mathcal{F}$ *over* $\mathbb{Z}/2^n$ *defined in 4.12. Then the exact period length of the* j^{th} *coordinate sequence* $\delta_j(\mathcal{F})$ $(j = 0, 1, 2, \ldots, n-1)$ *is* $2^n k_j$, *where* $1 \leq k_j \leq \ell$.

Moreover, the same holds if $m = 1$ *(and whence* $\ell = 1$*), i.e., when* $\mathcal{F}$ *is an output sequence of the automaton* $\mathfrak{A} = \langle N, M, \bar{f}, F, u_0\rangle$*, where* $N = M = \mathbb{Z}/2^n$*,* $\bar{f} = f \bmod 2^n$*,* f *and* h *are compatible and ergodic mappings of* $\mathbb{Z}_2$ *onto itself,* $F(x) = (h(\pi(x))) \bmod 2^n$*,* $x \in \{0, 1, \dots, 2^n - 1\}$*: The exact period length of the* j^{th} *coordinate sequence* $\delta_j(\mathcal{F})$ *is* 2^n *for all* $j = 0, 1, 2, \dots, n-1$*.*

Note. Hence, $\mathcal{F}$ is a purely periodic sequence of period length exactly $2^n m$, and with each element of $\mathbb{Z}/2^n$ occuring at the period exactly m times (see 4.12,2.3).

To prove this proposition we need the following easy

4.14**. Lemma.** *Let* $\mathcal{X} = \{x_i : i = 0, 1, 2, \dots\}$ *and* $\mathcal{Y} = \{y_i : i = 0, 1, 2, \dots\}$ *be purely periodic sequences over* $\mathbb{Z}/2$ *with exact period lengths* 2^u *and* 2^v*, respectively, and let* $u > v$*. Then the sequence* $\mathcal{X} \oplus \mathcal{Y} = \{x_i \oplus y_i : i = 0, 1, 2, \dots\}$ *is purely periodic with period length exactly* 2^u*.*

If, additionally, $x_{i+2^{u-1}} \equiv x_i + 1 \pmod 2$ *for all* $i = 0, 1, 2, \dots$*, and if* $\mathcal{Y}$ *is a non-zero sequence, then the sequence* $\mathcal{X} \odot \mathcal{Y} = \{x_i \cdot y_i : i = 0, 1, 2, \dots\}$ *is purely periodic with period length exactly* 2^u*.*

Proof of lemma 4.14. The first assertion of the lemma is obvious. To prove the second one assume P is the exact period length of the sequence $\{x_i \cdot y_i : i = 0, 1, 2, \dots\}$. Then $P = 2^s$ for suitable $s \le u$. Yet if $s < u$, then $x_{i+2^{u-1}} \cdot y_{i+2^{u-1}} \equiv x_i \cdot y_i \pmod 2$ for all $i = 0, 1, 2, \dots$; thus $(x_i + 1) \cdot y_i \equiv x_i \cdot y_i \pmod 2$ and hence $y_i \equiv 0 \pmod 2$ for all $i = 0, 1, 2, \dots$. A contradiction. □

Proof of proposition 4.13. In view of assertions (2) and (3) of lemma 4.7, each subsequence $\mathcal{F}(r) = \{z_{r+tm} : t = 0, 1, 2, \dots\}$, $r = 0, 1, \dots, m-1$, of the sequence $\mathcal{F} = \{z_i : i = 0, 1, 2, \dots\}$ satisfies the following condition: Each coordinate sequence $\delta_j(\mathcal{F}(r))$ is a purely periodic sequence of period length exactly 2^{j+1}, and the second half of the period is a bitwise negation of the first half, i.e., $\delta_j(z_{r+(t+2^j)m}) \equiv \delta_j(z_{r+tm}) + 1 \pmod 2$ for all $t = 0, 1, 2, \dots$. Thus, in view of theorem 5.9, which is proved further, the sequence $\mathcal{F}(r)$ is an output sequence of a suitable automaton $\mathfrak{B} = \langle \mathbb{Z}_2, \mathbb{Z}/2^n, f, \mathrm{mod} 2^n, z_r\rangle$, where f is a compatible and ergodic mapping of $\mathbb{Z}_2$ onto itself. Thus, the first assertion of the proposition follows from the second one, i.e., it is sufficient to consider only a case $m = 1$.

Now represent h in a Boolean form according to 3.13. So,

$$\delta_j(h(x)) \equiv \chi_j + \varphi_j(\chi_0, \dots, \chi_{j-1}) \pmod 2,$$

where $\chi_k = \delta_k(x)$, and φ_j is a Boolean polynomial of odd weight in Boolean variables $\chi_0, \dots, \chi_{j-1}$ for $j > 0$, $\varphi_0 = 1$. Note that for $j > 0$

$$\text{(4.14.1)} \quad \delta_j(h(x)) \equiv \chi_j + \chi_0 \cdot \chi_1 \cdots \chi_{j-1} + \psi_j(\chi_0, \dots, \chi_{j-1}) \equiv \\ \chi_j + \chi_0 \cdot \alpha_j(\chi_1, \dots, \chi_{j-1}) + \beta_j(\chi_1, \dots, \chi_{j-1}) \pmod 2,$$

where $\psi_j, \alpha_j, \beta_j$ are Boolean polynomials of corresponding Boolean variables, and $\deg \psi_j < j$, so α_j is a non-zero polynomial.

For binary sequences $\mathcal{U}, \mathcal{V}, \mathcal{W}, \dots$ (which could be treated as 2-adic integers) and a Boolean polynomial $\gamma(\upsilon, \nu, \omega, \dots)$ of Boolean variables $\upsilon, \nu, \omega, \dots$ denote $\gamma(\mathcal{U}, \mathcal{V}, \mathcal{W}, \dots)$ a binary sequence $\mathcal{S}$ (thus, a 2-adic integer) such that

$$\delta_j(\mathcal{S}) \equiv \gamma(\delta_j(\mathcal{U}), \delta_j(\mathcal{V}), \delta_j(\mathcal{W}), \dots) \pmod 2,$$

for all $j = 0, 1, 2, \dots$. Loosely speaking, we just substitute, respectively, XOR and AND for $+$ and $\cdot$ in the Boolean polynomial γ and let variables $\upsilon, \nu, \omega, \dots$ run through the space $\mathbb{Z}_2$ of 2-adic integers. Thus we obtain a well defined multivariate function γ on $\mathbb{Z}_2$ valuated in $\mathbb{Z}_2$. Since there is a natural one-to-one correspondence between infinite binary sequences and 2-adic integers, the sequence $\gamma(\mathcal{U},\mathcal{V},\mathcal{W},\ldots)$ is well defined. Note also that treating binary sequences as 2-adic integers enables one to produce infinite sequences of n-bit rational integers out of n infinite binary sequences in an obvious manner: Say, $\mathcal{U}+2\cdot\mathcal{V}+4\mathcal{W}$ is a sequence $\mathcal{N}=\{n_0,n_1,\ldots\in\mathbb{N}_0\}$ such that $n_j=\delta_j(\mathcal{U})+2\cdot\delta_j(\mathcal{V})+4\cdot\delta_j(\mathcal{W})$ for $j=0,1,2\ldots.$ For instance, if $\mathcal{U}=101\ldots$, $\mathcal{V}=110\ldots$, and $\mathcal{W}=010\ldots$, then $\mathcal{N}=361\ldots$ is a sequence over $\{0,1,\ldots,7\}=\mathbb{Z}/8$.

Proceeding with these conventions, let $\mathcal{C}_j$ (respectively, $\mathcal{D}_j$) be the j^{th} output sequence of the automaton $\mathfrak{B}$ (respectively, $\mathfrak{A}$). Let $\mathcal{E}=111\ldots.$ Then in view of (4.14.1) one has:

$$\mathcal{D}_0=\mathcal{C}_{n-1}\oplus\mathcal{E};$$
$$\mathcal{D}_1=\mathcal{C}_{n-2}\oplus\mathcal{C}_{n-1}\oplus\mathcal{B};$$
$$\mathcal{D}_j=\mathcal{C}_{n-j-1}\oplus\mathcal{C}_{n-1}\odot\alpha_j(\mathcal{C}_{n-2},\ldots,\mathcal{C}_{n-j})\oplus\beta_j(\mathcal{C}_{n-2},\ldots,\mathcal{C}_{n-j})\qquad(j\le 2),$$

where $\mathcal{B}=\beta_1\beta_1\beta_1\ldots$ is a constant binary sequence. Note that $\mathcal{C}_i$ is purely periodic binary sequence of period length exactly 2^{i+1}, and the second half of the period is a bitwise negation of the first half, see 5.1 further. This completes the proof of proposition 4.13 in view of lemma 4.14 and conventions made above, if we prove that the sequence $\alpha_j(\mathcal{C}_{n-2},\ldots,\mathcal{C}_{n-j})$, $2\le j\le n-1$, is a non-zero binary sequence.

Consider a sequence $\mathcal{G}_j=2^{n-2}\cdot\mathcal{C}_{n-2}+\cdots+2^{n-j}\cdot\mathcal{C}_{n-j}$ over $\mathbb{Z}/2^{j-1}$. The latter sequence is just an output sequence of the automaton $\mathfrak{G}_j=\langle\mathbb{Z}/2^{n-1},\mathbb{Z}/2^{j-1},f \bmod 2^{n-1},T_{n-j-1},u\rangle$, where T_{n-j-1} is a truncation of the first $n-j$ low order bits: $T_{n-j-1}(z)=\lfloor\frac{z}{2^{n-j}}\rfloor$. Thus, $\mathcal{G}_j$ is a purely periodic sequence of period length exactly 2^{n-1} and with each element of $\mathbb{Z}/2^{j-1}$ occuring at the period the same number of times. Yet α_j is a non-zero Boolean polynomial (see above); thus it takes value 1 at least at one $(j-1)$-bit word of $\mathbb{Z}/2^{j-1}$. Consequently, at least one member of the sequence $\alpha_j(\mathcal{C}_{n-2},\ldots,\mathcal{C}_{n-j})$ is 1. $\square$

Note. There are other methods that improve periods of coordinate sequences. For insatnce, using the ideas of the proof of 4.13 it is not difficult to demonstrate that *if a recurrence sequence is defined by a relation* $x_{i+1}=f(x_i)$, *where* $f\colon\mathbb{Z}_2\to\mathbb{Z}_2$ *is compatible and ergodic mapping, then a binary sequence* $\{\delta_k(x_i+2^j\cdot\delta_s(x_i))\colon i=0,1,2,\ldots\}$ *is purely periodic with period length exactly* 2^s *whenever* $j\le k<s$. From here it could be deduced that e.g. the sequence

$$\mathcal{Z}=\left\{\left(x_i+\pi_k^1\left(\left\lfloor\frac{x_i}{2^k}\right\rfloor \bmod 2^k\right)\right) \bmod 2^k\colon i=0,1,2,\ldots\right\}$$

is a purely periodic sequence over $\mathbb{Z}/2^k$ of period length exactly 2^{2k}, such that each element of $\mathbb{Z}/2^k$ occurs at the period exactly 2^k times, and that each coordinate sequence of $\mathcal{Z}$ is purely periodic binary sequence of period length exactly 2^{2k}. Note that $\mathcal{Z}$ is obtained according to a very simple rule: at the i^{th} step take $(2k)$-bit output of congruential generator of a maximum period length with state transition function f, read the second half of this output as a k-bit number in reverse bit order and add this number modulo 2^k to the k-bit number that agrees with the first half of the output.

5. Properties

In this section we study common probabilistic, cryptographic and other properties of output sequences of the generators considered in preceeding sections: Linear and 2-adic spans of these sequences, their structure, distribution of k-tuples in them, etc. We begin our study with properties of coordinate sequences of the automata considered above, that is, of the sequences $\{\delta_j(s_i)\colon i=0,1,2,\dots\}$, where $\{s_i\}$ is the output sequence of the automaton.

Properties of coordinate sequences. To study coordinate sequences it is convenient to consider an automaton $\mathfrak{A}'$ with a state set $\mathbb{Z}_2$, compatible and ergodic state transition function $f\colon\mathbb{Z}_2\to\mathbb{Z}_2$ and with identity output function $F(z)=z$. We also consider an automaton $\mathfrak{A}'_j$ which differs from $\mathfrak{A}'$ only by the output function, which is $\delta_j(z)$ in this case. Thus the output sequence of $\mathfrak{A}'_j$ is just the j^{th} coordinate sequence $\mathcal{S}_j=\{s_i=\delta_j(f^{(i)}(z)) : i=0,1,2,\dots\}$ of the automaton $\mathfrak{A}'$ (here $z\in\mathbb{Z}_2$ is the initial state of the automaton $\mathfrak{A}'$). Note that since f is compatible, we may assume if necessary that $z\in\mathbb{Z}/2^{j+1}$, i.e., that all but possibly the first $j+1$ junior bits of 2-adic representation of z are 0. That is, the output sequence of the automaton $\mathfrak{A}'_j$ is the same as the one of the automaton $\mathfrak{A}=\langle\mathbb{Z}/2^{j+1},\mathbb{Z}/2,f \bmod 2^{j+1},\delta_j,z \bmod 2^{j+1}\rangle$, see Section 2.

It turnes out that the j^{th} coordinate sequence has rather specific structure. Namely, the following theorem holds.

5.1. **Theorem.** *The j^{th} coordinate sequence is purely periodic, and 2^{j+1} is the length of its period. The second half of the period is a bitwise negation of its first half, i.e., $s_{i+2^j}\equiv s_i+1 \pmod 2$ for each $i=0,1,2,\dots$.*

Proof. Since the mapping $f\colon\mathbb{Z}_2\to\mathbb{Z}_2$ is compatible and ergodic, the sequence $\{x_{i+1}=f(x_i) \bmod 2^{j+1} : i=0,1,2,\dots\}$ is purely periodic, with 2^{j+1} being the length of its period, whereas the sequence $\{x_{i+1}=f(x_i) \bmod 2^j : i=0,1,2,\dots\}$ is purely periodic, and the length of its period is exactly 2^j. Yet $x_{i+1} \bmod 2^{j+1} = x_{i+1} \bmod 2^j + 2^j\delta_j(x_{i+1})$, and the first assertion of 5.1 follows.

Supposing $\delta_j(x_{i+1})=\delta_j(x_{i+1+2^j})$ for some i, from the preceeding equality one obtains $x_{i+1+2^j}\equiv x_{i+1} \pmod{2^{j+1}}$, and hence $x_{i+t+1+2^j}\equiv f^{(t)}(x_{i+1+2^j})\equiv f^{(t)}(x_{i+1})\equiv x_{i+t+1} \pmod{2^{j+1}}$ for all $t=0,1,2,\dots$, in view of compatibility of f. So the length of the period of the sequence $\{x_i \bmod 2^{j+1} : i=0,1,2,\dots\}$ does not exceed 2^j, in contradiction with the ergodicity of f, see 2.2. □

5.2. *Note.* Theorem 5.1 could be generalized in two directions. First, to output sequences of wreath products of automata (this is already done, see 4.11), and second, to the case p odd.

In the latter case provided transformation $f\colon\mathbb{Z}_p\to\mathbb{Z}_p$ is compatible and ergodic, the j^{th} coordinate sequence $\{\delta_j(f^{(i)}(z)) : i=0,1,2,\dots\}$ is purely periodic, with p^{j+1} being the length of its period (here and further within this remark $\delta_j(z)$ stands for the j^{th} digit in base-p expansion of z). Each subsequence $\{\delta_j(f^{(i+p^t)}(z)) : t=0,1,2,\dots\}$ is a purely periodic sequence with p being the length of period; moreover, for $j>0$ it is generated by a linear congruential generator modulo p, i.e., by a polynomial $a+x$ for appropriate $a\in\{1,2,\dots,p-1\}$. So this sequence is strictly uniformly distributed modulo p: each $u\in\mathbb{Z}/p$ occurs at the period exactly once. The generator $\delta_0(f^{(i)}(z))$ is a (generally speaking, nonlinear) congruential generator of the form $v_{i+1} \equiv g(v_i) \pmod p$ for an appropriate transitive modulo p polynomial $g(x)$ over a field Z/p of residues modulo p.

A proof of this assertion could be deduced from the proof of theorem 3.4 of [16] since in view of the p-adic Weierstrass theorem (see [3]) a transformation $z \mapsto f(z) \bmod p^{j+1}$ of the residue ring $\mathbb{Z}/p^{j+1}$ may be considered as a polynomial transformation $z \mapsto w(z) \bmod p^{j+1}$ induced by an integer-valued and compatible polynomial $w(x) \in \mathbb{Q}[x]$, i.e., by a polynomial of the form mentioned in 3.1. Thus the mapping $z \mapsto f(z) \bmod p^{j+1}$ could be considered as a reduction modulo p^{j+1} of the compatible and ergodic mapping $w \colon \mathbb{Z}_p \to \mathbb{Z}_p$; the latter mapping is uniformly differentiable everywhere on $\mathbb{Z}_p$. Hence the assumptions of theorem 3.4 of [16] are satisfied. We omit further details.

We recall that a linear complexity $\Psi_F(\mathcal{S})$ of the sequence $\mathcal{S} = \{s_i \colon i = 0, 1, 2, \ldots\}$ over a field F is the smallest $n \in \mathbb{N}$ such that every n succesive members of the sequence satisfy some non-trivial linear relation of length $n+1$, i.e., there exist $a_0, a_1, \ldots, a_n$, not all equal to 0, such that $a_0 s_i + a_1 s_{i+1} + \cdots + a_n s_{i+n} = 0$ for all $i = 0, 1, 2, \ldots$. In this case we also say that the polynomial $a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ *annihilates* $\mathcal{S}$ [7]. In other words, linear complexity is just a degree of the minimal polynomial of $\mathcal{S}$ (the minimum degree nonzero polynomial that annihilates $\mathcal{S}$; a polynomial $g(x) \in F[x]$ annihilates $\mathcal{S}$ iff the minimal polynomial of $\mathcal{S}$ is a factor of $g(x)$ — see e.g. [17] or [24] for references). In case $F = \mathbb{Z}/p$ is a field of p elements we use for linear complexity over F the notation Ψ_p rather than $\Psi_{\mathbb{Z}/p}$.

Linear complexity is one of crusial for cryptography properties: Pseudorandom generators that produce sequences of low linear complexity are not secure, since having relatively short segment of output sequence and solving a corresponding system of linear equations over F a cryptoanalyst could find $a_0, a_1, \ldots, a_n$ and thus predict with probability 1 the rest of the members of the sequence. Of course, high linear complexity per se does not guarantee security.

5.3. **Theorem.** *The linear complexity $\Psi_2(\mathcal{S}_j)$ of the j^{th} coordinate sequence $\mathcal{S}_j$ is exactly $2^j + 1$.*

We need the following lemma:

5.4. **Lemma.** *Let p be a prime, and let $\mathcal{S}$ be a purely periodic sequence over $\mathbb{Z}/p$ of period length exactly p^{j+1}. Then $\Psi_p(\mathcal{S}) > p^j$.*

Proof of lemma 5.4. Since p^{j+1} is the length of the period of the sequence $\mathcal{S}$, the polynomial $x^{p^{j+1}} - 1$ over a field $\mathbb{Z}/p$ annihilates $\mathcal{S}$. Yet $x^{p^{j+1}} - 1 = (x-1)^{p^{j+1}}$; thus, the minimal polynomial $m(x)$ of $\mathcal{S}$ is of the form $(x-1)^r$, where $r \le p^{j+1}$. However, the polynomial $x^{p^j} - 1 = (x-1)^{p^j}$ does not annihilate $\mathcal{S}$, since otherwise the length of some period of $\mathcal{S}$ is a factor of p^j; yet $\mathcal{S}$ has no periods of length less than p^{j+1} (see definition 2.4). Hence, $\deg m(x) = r > p^j$, since otherwise the polynomial $(x-1)^{p^j}$ annihilates $\mathcal{S}$. ☐

Proof of the theorem 5.3. Since $s_{i+2^j} \equiv s_i + 1 \pmod 2$ for all $i = 0, 1, 2, \ldots$ (see 5.1), the congruence $s_{i+1+2^j} + s_{i+2^j} + s_{i+1} + s_i \equiv 0 \pmod 2$ holds for all $i = 0, 1, 2, \ldots$. Hence, the polynomial $x^{2^j+1} + x^{2^j} + x + 1 = (x+1)^{2^j+1}$ annihilates the j^{th} coordinate sequence $\mathcal{S}_j = \{s_0, s_1, \ldots\}$. Now the assertion of 5.3 follows from 5.4. ☐

---

[7] A polynomial that annihilates $\mathcal{S}$ is also called a *characteristic polynomial of the sequence* $\mathcal{S}$.

Theorem 5.3 could be generalized to the case of output sequences of wreath products of automata. Namely, the following proposition holds.

5.5. **Proposition.** *Let* $\mathcal{S} = \{s_i \colon i = 0, 1, 2, \ldots\}$ *be any of the sequences* $\mathcal{U}_n$, $\mathcal{X}_n$, $\mathcal{W}_n$, $\mathcal{Y}_n$, *and* $\mathcal{Z}$ *defined, respectively, in 4.3, 4.5, 4.6, 4.7, and 4.10. Then the linear complexity of the* $(n-1)^{th}$ *coordinate sequence* $\delta_{n-1}(\mathcal{S}) = \{\delta_{n-1}(s_i) \colon i = 0, 1, 2, \ldots\}$ *exceeds* 2^{n-1}.

Proof. Since the period length of the sequence $\delta_{n-1}(\mathcal{S})$ is $2^n\ell$, where $\ell = 2^m$ for $\mathcal{S} \in \{\mathcal{U}_n, \mathcal{X}_n\}$, or $\ell = m$ otherwise (see corresponding statements), the polynomial $u(x) = x^{2^n\ell} - 1 = (x^\ell - 1)^{2^n}$ annihilates $\delta_{n-1}(\mathcal{S})$. Thus, the minimal polynomial $m(x)$ of $\delta_{n-1}(\mathcal{S})$ is a factor of $u(x)$. On the other hand $m(x)$ is not a factor of $w(x) = (x^\ell - 1)^{2^{n-1}}$ since otherwise the sequence $\delta_{n-1}(\mathcal{S})$ has period of length $2^{n-1}\ell$; however, this is impossible since the second half of the period of length $2^n\ell$ of this sequence is a bitwise negation of the first half, see 4.11. Since both polynomials $u(x)$, $w(x)$ have the same set of roots in their splitting field, at least one of these roots is a root of $m(x)$ with multiplicity exceeding 2^{n-1}. Thus, $\deg m(x) > 2^{n-1}$. □

Speaking formally, proposition 5.5 holds for $\ell = 1$ either, turning into theorem 5.1 in this case. Thus, we may say that the estimate of $\Psi_2(\delta_{n-1}(\mathcal{S}))$ given by proposition 5.5 is sharp. However, it could be improved for particular classes of ℓ. For instance, if $\ell = 2^m$, i.e., if $\mathcal{S} = \mathcal{X}_n$, then $\Psi_2(\delta_{n-1}(\mathcal{S})) = 2^{n-1}\ell + 1$ in view of note 4.5 and theorem 5.3. Also, if $\ell = 2^k m_1$, where m_1 is odd, then the proof of proposition 5.5 shows that $\Psi_2(\delta_{n-1}(\mathcal{S})) > 2^{n-1+k}$ in this case.

So it seems possible to improve significantly the estimate of linear complexity that gives proposition 5.5 for various classes of wreath products described by 4.3, 4.5, 4.6, 4.7, and 4.10, i.e., for arbitrary $\ell > 1$. To do this now we have to run a bit ahead and to use theorem 5.10, which is proved further. With the use of this theorem, the general case could be reduced to the case $\ell > 1$ odd. Namely, in view of theorem 5.10, every purely periodic binary sequence of period length $2^n\ell$, $n > 1$, such that the second half of the period of this sequence is a bitwise negation of the first part of the period, could be considered as $(n-1)^{\text{th}}$ coordinate sequence of a certain wreath product of automata that is described by theorem 4.10. Thus, if $\ell = 2^k m_1$, where m_1 odd, this sequence in view of theorem 5.10 could be considered as $(n-1+k)^{\text{th}}$ coordinate sequence of a suitable wreath product of automata mentioned in theorem 4.10 for $m = m_1$ odd. So we can assume that ℓ is odd.

Proceeding with this note and using the congruence $\delta_{n-1}(s_{i+2^{n-1}\ell}) \equiv \delta_{n-1}(s_i) + 1 \pmod 2$ (see 4.11) we obtain that the minimal polynomial $m_{n-1}(x)$ of the sequence $\delta_{n-1}(\mathcal{S})$ is a factor of the polynomial

$$x^{2^{n-1}\ell+1} + x^{2^{n-1}\ell} + x + 1 = \\ (x^\ell + 1)^{2^{n-1}}(x+1) = (x^{\ell-1} + \cdots + x + 1)^{2^{n-1}}(x+1)^{2^{n-1}+1}.$$

Thus, the root of multiplicity $> 2^{n-1}$ of the proof of 4.11 is 1 (since the polynomial $x^{\ell-1} + \cdots + x + 1$ is a factor of $x^\ell - 1$; yet $x^\ell - 1$ has no roots of multiplicity > 1 in its splitting field, as ℓ is odd). Hence,

$$m_{n-1}(x) = v(x)(x+1)^{2^{n-1}+1}, \tag{5.5.1}$$

where $v(x)$ is a factor of $(x^{\ell-1}+\cdots+x+1)^{2^{n-1}}$. Thus,

$$2^{n-1}\ell+1 \geq \deg m_{n-1}(x)=\Psi_2(\delta_{n-1}(\mathcal{S})) \geq 2^{n-1}+1. \tag{5.5.2}$$

We shall show now that for $n>1$ the both bounds are sharp.

Consider a finite sequence $\mathcal{T}$ of length $2^{n-1}\ell$ consisting of gaps and blocks (alternating runs of 0's and 1's, respectively) of length 2^{n-1} each. Take this sequence as the first half of a period of a sequence $\mathcal{S}'$, and take a bitwise negation $\hat{\mathcal{T}}$ of $\mathcal{T}$ as a second half of a period of $\mathcal{S}'$ (of course $\hat{\mathcal{T}}=(\mathcal{T})\,\mathsf{XOR}(2^{2^{n-1}\ell}-1)$, where we consider $\mathcal{T}$ as a base-2 expansion of a suitable rational integer $\gamma_{n-1}>0$). Obviously, $\mathcal{S}'$ is a purely periodic sequence of period length $2^n\ell$, and the second half of its period is a bitwise negation of the first half. Thus, as it is shown by theorem 5.10, the sequence $\mathcal{S}'$ could be outputted as $(n-1)^{\text{th}}$ coordinate sequence of a suitable wreath product of automata, which is described by theorem 4.10. Yet obviously $\mathcal{S}'$ is a sequence of gaps and blocks of length 2^{n-1} each; thus, the exact period length of the sequence $\mathcal{S}'$ is 2^n. So linear complexity of $\mathcal{S}'$ is $2^{n-1}+1$ (see the proof of theorem 5.3).

Now we prove that the upper bound in (5.5.2) is also sharp. Consider a sequence $\mathcal{U}$ of gaps and blocks of length 2^{n-1} each, and a purely periodic sequence $\mathcal{V}$ with period of length $2^{n-1}\ell$; let this period consists of a block of length $2^{n-1}(\ell-1)$ followed by a gap of length 2^{n-1}. Let $m_{\mathcal{U}}(x), m_{\mathcal{V}}(x)$ be minimal polynomials of corresponding sequences.

Since $\mathcal{U}$ is a purely periodic sequence with period length exactly 2^n, and a second half of its period is a bitwise negation of the first half, a polynomial $m_1(x)=x^{2^{n-1}+1}+x^{2^{n-1}}+x+1=(x+1)^{2^{n-1}+1}$ annihilates $\mathcal{U}$ (see the argument above); so $m_{\mathcal{U}}(x)$ is a factor of $m_1(x)$. However, the first 2^{n-1} overlapping (2^{n-1})-tuples considered as vectors of dimension 2^{n-1} over a field $\mathbb{Z}/2$ are obviously linearly independent. Thus, $\deg m_{\mathcal{U}}(x)>2^{n-1}$ (see [24, Theorem 8.51]). Finally we conclude that $m_{\mathcal{U}}(x)=m_1(x)$. A similar argument proves that $m_{\mathcal{V}}(x)=x^{2^{n-1}(\ell-1)}+x^{2^{n-1}(\ell-2)}+\cdots+x^{2^{n-1}}+1$.

Now consider a sum $\mathcal{R}$ of these two sequences. i.e., $\mathcal{R}=\mathcal{U}\,\mathsf{XOR}\,\mathcal{V}$. Obviously, $m_{\mathcal{U}}(x)$ and $m_{\mathcal{V}}(x)$ are coprime, since 1 is the only root of $m_{\mathcal{U}}(x)$, yet 1 is not a root of $m_{\mathcal{V}}(x)$ (recall ℓ odd). Thus, $m_{\mathcal{U}}(x)\cdot m_{\mathcal{V}}(x)$ is the minimal polynomial of $\mathcal{R}$ (see [24, Theorem 8.57]). Hence $\Psi_2(\mathcal{R})=2^{n-1}\ell+1$.

Since ℓ is odd, $\mathcal{R}$ is obviously a purely periodic sequence of period length exactly $2^n\ell$, and the second half of the period is a bitwise negation of its first half. Consequently, $\mathcal{R}$ is the $(n-1)^{\text{th}}$ coordinate sequence of a suitable wreath product of automata, which is described by theorem 4.10 (see 5.10).

As a bonus we have that the exact period length P of the $(n-1)^{\text{th}}$ coordinate sequence $\delta_{n-1}(\mathcal{S})$ for odd ℓ is a multiple of 2^n: Since x^P+1 annihilates $\delta_{n-1}(\mathcal{S})$, $m_{n-1}(x)$ is a factor of x^P+1. Yet $x^P+1=(x^s+1)^{2^t}=(x+1)^{2^t}(x^{s-1}+\cdots+1)^{2^t}$, where $P=2^ts$, s odd, and 1 is not a root of $x^{s-1}+\cdots+1$ since s is odd. Thus, necessarily $2^t\geq 2^{n-1}+1$ in view of (5.5.1). Hence, $t\geq n$. So we conclude that $P=2^ns$; yet $P\leq 2^n\ell$ since the output sequence $\mathcal{Z} \bmod 2^n$ is purely periodic of period length exactly $2^n\ell$ (see 4.10). Thus, $P=2^ns$, where $1\leq s\leq \ell$. As demonstrate examples of sequences $\mathcal{S}'$ and $\mathcal{R}$, both extreme cases $s=1$ and $s=\ell$ are possible.

We summarize the above considerations in the following

5.6. **Theorem.** *Let $\mathcal{Z}_j$, $j>0$, be the j^{th} coordinate sequence of a wreath product of automata* (described by any of 4.3, 4.5, 4.6, 4.7, and 4.10: thus $\mathcal{Z}_j$ is a purely periodic binary sequence of period length $2^{j+1}\ell$, where $\ell = 2^m$ for wreath products described by 4.3 or 4.5, and $\ell = m$ otherwise). *Represent* $\ell = 2^k r$, *where* r *is odd. Then the exact period length of* $\mathcal{Z}_j$ *is* $2^{k+j+1}s$ *for some* $s \in \{1, 2, \ldots, r\}$, *and both extreme cases* $s = 1$ *and* $s = r$ *occur: for every sequence* $s_1, s_2, \ldots$ *over a set* $\{1, r\}$ *there exists a wreath product of automata such that the period length of the* j^{th} *coordinate sequence of its output is exactly* $2^{k+j+1}s_j$, $(j = 1, 2, \ldots)$.

Moreover, a linear complexity $\Psi_2(\mathcal{Z}_j)$ *of the sequence* $\mathcal{Z}_j$ *satisfies the following inequality:*

$$2^{k+j} + 1 \leq \Psi_2(\mathcal{Z}_j) \leq 2^{k+j}r + 1.$$

Both these bounds are sharp: For every sequence $t_1, t_2, \ldots$ *over a set* $\{1, r\}$ *there exists a wreath product of automata such that the linear complexity of the* j^{th} *coordinate sequence of its output is exactly* $2^{k+j}t_j + 1$, $(j = 1, 2, \ldots)$.

Proof. Nearly everything is already done by the preceeding arguments. We only note that in view of mentioned theorem 5.10, we can choose coordinate sequences independently one of another. That is, for each sequence of purely periodic binary sequences $\mathcal{Z}_1, \mathcal{Z}_2, \ldots$, such that period length of the j^{th} sequence $\mathcal{Z}_j$ $(j = 1, 2, \ldots)$ is $2^{j+1}\ell$, and the second part of this period is a bitwise negation of the first part, there exist a wreath product of automata, that satisfies 4.10, and such that the j^{th} coordinate sequence of its output is exactly $\mathcal{Z}_j$ for all $j = 1, 2, \ldots$. □

With the use of theorem 5.1 it is possible to estimate two other measures of complexity of the coordinate sequence, which were introduced in [10]: namely, 2-*adic complexity* and 2-*adic span*. Whereas linear complexity (also known as *linear span*) is the number of cells in a linear feedback shift register outputting a given sequence $\mathcal{S}$ over $\mathbb{Z}/2$, the 2-adic span is the number of cells in both memory and register of a feedback with carry shift register (FCSR) that outputs $\mathcal{S}$, and the 2-adic complexity estimates the number of cells in the register of this FCSR. To be more exact, the 2-adic complexity $\Phi_2(\mathcal{S})$ of the (eventually) periodic sequence $\mathcal{S} = \{s_0, s_1, s_2, \ldots\}$ over $\mathbb{Z}/2$ is $\log_2(\Phi(u, v))$, where $\Phi(u, v) = \max\{|u|, |v|\}$ and $\frac{u}{v} \in \mathbb{Q}$ is the irreducible fraction such that its 2-adic expansion agrees with $\mathcal{S}$, that is, $\frac{u}{v} = s_0 + s_1 2 + s_2 2^2 + \cdots \in \mathbb{Z}_2$. The number of cells in the register of FCSR producing $\mathcal{S}$ is then $\lceil \log_2(\Phi(u, v)) \rceil$, the least rational integer not smaller than $\log_2(\Phi(u, v))$. Thus, we only need to estimate $\Phi_2(\mathcal{S})$.

5.7. **Theorem.** *Let* $\mathcal{S}_j = \{s_0, s_1, s_2, \ldots\}$ *be the* j^{th} *coordinate sequence. its* 2-*adic complexity* $\Phi_2(\mathcal{S}_j)$ *is* $\log_2\left(\frac{2^{2^j}+1}{\gcd(2^{2^j}+1, \gamma+1)}\right)$, *where* $\gamma = s_0 + s_1 2 + s_2 2^2 + \cdots + s_{2^j-1}2^{2^j-1}$.

Note. We note that γ is a non-negative rational integer, $0 \leq \gamma \leq 2^{2^j} - 1$; also we note that for each γ of this range there exists an ergodic mapping such that the first half of the period of the j^{th} coordinate sequence of the corresponding output is a base-2 expansion of γ (see 5.9). Thus, to find all possible values of 2-adic complexity of the j^{th} coordinate sequence one has to decompose the j^{th} Fermat number $2^{2^j} + 1$. It is known that j^{th} Fermat number is prime for $0 \leq j \leq 4$ and that it is composite for $5 \leq j \leq 23$. For each Fermat number outside this range it is not known whether it is prime or composite. The complete decomposition of j^{th} Fermat number is not known for $j > 11$. Assuming for some $j \geq 2$ the j^{th} Fermat number is composite, all its factors are of the form $t2^{j+2} + 1$, see e.g. [15]

for further references. So, *the following bounds for* 2*-adic complexity* $\Phi_2(\mathcal{S}_j)$ *of the* j^{th} *coordinate sequence* $\mathcal{S}_j$ *hold:*

$$j+3 \le \lceil \Phi_2(\mathcal{S}_j) \rceil \le 2^j + 1,$$

yet to prove whether the lower bound is sharp for a certain $j > 11$, *or whether* $\lceil \Phi_2(\mathcal{S}_j) \rceil$ *could be actually less than* 2^j+1 *for* $j > 23$ *is as difficult as to decompose the* j^{th} *Fermat number or, respectively, to determine whether the* j^{th} *Fermat number is prime or composite.*

Proof of theorem 5.7. We only have to express $s_0+s_12+s_22^2+\dots$ as an irreducible fraction. Denote $\gamma = s_0 + s_1 2 + s_2 2^2 + \cdots + s_{2^j-1}2^{2^j-1}$. Then using the second identity of (2.0.2) we in view of 5.1 obtain that $s_0+s_12+s_22^2+\cdots+s_{2^{j+1}-1}2^{2^{j+1}-1} = \gamma + 2^{2^j}(2^{2^j} - \gamma - 1) = \gamma'$ and hence $s_0+s_12+s_22^2+\cdots = \gamma' + \gamma' 2^{2^{j+1}} + \gamma' 2^{2\cdot 2^{j+1}} + \gamma' 2^{3\cdot 2^{j+1}} + \cdots = \frac{\gamma+1}{2^{2^j}+1} - 1$. This completes the proof in view of the definition of 2-adic complexity of a sequence. □

5.8. *Note.* Similar estimates of $\Phi_2(\delta_{n-1}(\mathcal{S}))$ could be obtained for the sequence $\mathcal{S} \in \{\mathcal{W}_n, \mathcal{Y}_n, \mathcal{Z}\}$ of 4.6, 4.7, and 4.10, respectively (for $\mathcal{S} \in \{\mathcal{U}_n, \mathcal{X}_n\}$ of 4.3 and 4.5 this estimate is already given by 5.7 in view of 4.5). In view of 4.11 the argument of the proof of 5.7 gives that the representation of the binary sequence $\delta_{n-1}(\mathcal{S})$ as a 2-adic integer is $\frac{\gamma+1}{2^{2^{n-1}m}+1} - 1$, so we have only to study a fraction $\frac{\gamma+1}{2^{2^{n-1}m}+1}$, where $\gamma = s_0 + s_1 2 + s_2 2^2 + \cdots + s_{2^{n-1}m-1}2^{2^{n-1}m-1}$, and m is of statements of 4.6, 4.7, and 4.10. Representing $m = 2^k m_1$ with $m_1 > 1$ odd, we can factorize $2^{2^{n-1}m} + 1 = (2^{2^{n-1+k}} + 1)(2^{2^{n-1+k}(m_1-1)} - 2^{2^{n-1+k}(m_1-2)} + \cdots - 2^{2^{n-1+k}} + 1)$, but the problem does not become much easier because of the first multiplier. We omit further details.

Both theorems 5.3 and 5.7 show that all three measures of complexity of a sequence (linear and 2-adic spans and 2-adic complexity) are not too sensitive. For instance, assuming $f(x) = x+1$ to be a state transition function and 0 to be an initial state of the automaton $\mathfrak{A}'$, we see that values of both linear and 2-adic complexity of the j^{th} coordinate sequence $\mathcal{S}_j$ of this automaton depend on j exponentially: $\Psi_2(\mathcal{S}_j) = \Phi_2(\mathcal{S}_j) = 2^j + 1$. However, in this case $\mathcal{S}_j$ is merely a sequence of alternating runs of 0's and 1's of length 2^j each.

Looking through the proofs of the corresponding theorems it is easy to observe that such big figures for linear and 2-adic complexity in the above example are due to a very simple law the j^{th} coordinate sequence obeys: The second half of the period is the bitwise negation of the first half (see 5.1, 4.11). This means that, intuitively, the j^{th} coordinate sequence is as complex as the first half of its period. Thus we have to understand what sequences of length 2^j could be outputted as the first half of the period of the j^{th} coordinate sequence, that is, what values takes the rational integer γ of 5.7.

In other words, let $\gamma_j(f,z) \in \mathbb{N}_0$ be such a number that its base-2 expansion agrees with the first half of the period of the j^{th} coordinate sequence produced by the automaton $\mathfrak{A}'_j$, i.e., let

$$\gamma_j(f,z) = \delta_j(f^{(0)}(z)) + 2\delta_j(f^{(1)}(z)) + 4\delta_j(f^{(2)}(z)) + \cdots + 2^{2^j-1}\delta_j(f^{(2^j-1)}(z)).$$

Obviously, $0 \le \gamma_j(f,z) \le 2^{2^j} - 1$. A natural question arises:

Given a compatible and ergodic mapping $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *and a* 2*-adic integer* $z \in \mathbb{Z}_2$*, what infinite string* $\gamma_0 = \gamma_0(f,z), \gamma_1 = \gamma_1(f,z), \gamma_2 = \gamma_2(f,z), \dots$ *(where* $\gamma_j \in \{0,1,\dots,2^{2^j}-1\}$ *for* $j = 0,1,2,\dots$*) could be obtained?*

The answer is: *any one.*

Namely, the following theorem holds.

5.9**. Theorem.** *Let* $\Gamma = \{\gamma_j \in \mathbb{N}_0\colon j = 0,1,2,\dots\}$ *be an arbitrary sequence of non-negative rational integers that satisfy* $0 \le \gamma_j \le 2^{2^j} - 1$ *for* $j = 0,1,2,\dots$ *, then there exist a compatible and ergodic mapping* $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *and a* 2*-adic integer* $z \in \mathbb{Z}_2$ *such that* $\delta_j(z) = \delta_0(\gamma_j)$*,* $\delta_0(f^{(i)}(z)) \equiv \gamma_0 + i \pmod 2$*, and*

$$\delta_j(f^{(i)}(z)) \equiv \delta_{i \bmod 2^j}(\gamma_j) + \left\lfloor \frac{i}{2^j} \right\rfloor \pmod 2$$

for all $i, j \in \mathbb{N}$*.*

Note. The sequence $\left\{ \left\lfloor \frac{i}{2^j} \right\rfloor \bmod 2\colon i = 1,2,\dots \right\}$ is merely a binary sequence of alternating gaps and blocks (i.e., runs of consequtive 0's or 1's, respectively) of length 2^j each.

Proof of theorem 5.9. Put $z = z_0 = \sum_{j=0}^{\infty} \delta_0(\gamma_j)2^j$ and

$$z_i = (\gamma_0 + i) \bmod 2 + \sum_{j=1}^{\infty} \left(\left(\delta_{i \bmod 2^j}(\gamma_j) + \left\lfloor \frac{i}{2^j} \right\rfloor \right) \bmod 2 \right) \cdot 2^j$$

for $i = 1,2,3,\dots$. Consider a sequence $Z = \{z_i\colon i = 0,1,2,\dots\}$. Speaking informally, we are filling a table with countable infinite number of rows and columns in such a way that the first 2^j entries of the j^{th} column represent γ_j in its base-2 expansion, and the other entries of this column are obtained from these by applying recursive relation of theorem 5.1. Then each i^{th} row of the table is a 2-adic canonical representation of $z_i \in Z$.

We shall prove that Z is a dense subset in $\mathbb{Z}_2$, and then define f on Z in such a way that f is compatible and ergodic on Z. This will imply the assertion of the theorem.

Proceeding along this way we claim that $Z \bmod 2^k = \mathbb{Z}/2^k$ for all $k = 1,2,3,\dots$, i.e., a natural ring homomorphism $\bmod 2^k\colon z \mapsto z \bmod 2^k$ maps Z onto the residue ring $\mathbb{Z}/2^k$. Indeed, this trivially holds for $k = 1$. Assuming our claim holds for $k < m$ we prove it for $k = m$. Given arbitrary $t \in \{0,1,\dots,2^m-1\}$ there exists $z_i \in Z$ such that $z_i \equiv t \pmod{2^{m-1}}$. If $z_i \not\equiv t \pmod{2^m}$ then $\delta_{m-1}(z_i) \equiv \delta_{m-1}(t) + 1 \pmod 2$ and thus $\delta_{m-1}(z_{i+2^{m-1}}) \equiv \delta_{m-1}(t) \pmod 2$. However, $z_{i+2^{m-1}} \equiv z_i \pmod{2^{m-1}}$. Hence $z_{i+2^{m-1}} \equiv t \pmod{2^m}$.

A similar argument shows that for each $k \in \mathbb{N}$ the sequence $\{z_i \bmod 2^k\colon i = 0,1,2,\dots\}$ is purely periodic with period length 2^k, and each $t \in \{0,1,\dots,2^k-1\}$ occurs at the period exactly once (in particular, all members of Z are pairwise distinct 2-adic integers). Moreover, $i \equiv i' \pmod{2^k}$ iff $z_i \equiv z_{i'} \pmod{2^k}$. Consequently, Z is dence in $\mathbb{Z}_2$ since for each $t \in \mathbb{Z}_2$ and each $k \in \mathbb{N}$ there exists $z_i \in Z$ such that $\|z_i - t\|_2 \le 2^{-k}$. Moreover, if we define $f(z_i) = z_{i+1}$ for all $i = 0,1,2,\dots$ then $\|f(z_i) - f(z_{i'})\|_2 = \|z_{i+1} - z_{i'+1}\|_2 = \|(i+1) - (i'+1)\|_2 = \|i - i'\|_2 = \|z_i - z_{i'}\|_2$. Hence, f is well defined and compatible on Z; it follows that the continuation of f to the whole space $\mathbb{Z}_2$ is compatible. Yet f is transitive modulo 2^k for each $k \in \mathbb{N}$, so its continuation is ergodic. □

Theorem 5.9 could be extended to coordinate sequences of wreath products of automata (see Section 4), i.e., to the sequences $\delta_j(\mathcal{Z})=\{\delta_j(x_i)\colon i=0,1,2,\dots\}$, where $\mathcal{Z}=\{x_i\colon i=0,1,2,\dots\}$ is a recurrence sequence over $\mathbb{Z}_2$ defined in 4.10. Speaking loosely, *each first half of a period of each* i^{th} $(i\ge 1)$ *coordinate sequence of wreath products of automata could be arbitrary and independent of others*. Now we give a formal statement and a proof of it.

Recall that $\delta_j(\mathcal{Z})$ is a purely periodic binary sequence of period length $2^{j+1}m$, and the second half of the period is a bitwise negation of its first half, see 4.11. Thus, the sequence $\delta_j(\mathcal{Z})$ could be identified with a rational number (which will be denoted by the same symbol $\delta_j(\mathcal{Z})$) such that its canonical 2-adic representation is $\delta_j(x_0)+\delta_j(x_1)2+\delta_j(x_2)2^2+\dots$. Hence in view of note 5.8,

$$\frac{2^{2^j m}-\gamma_j}{2^{2^j m}+1}=\delta_j(\mathcal{Z}), \tag{5.9.1}$$

where $\gamma_j=\delta_j(x_0)+\delta_j(x_1)2+\delta_j(x_2)2^2+\dots+\delta_j(x_{2^j m-1})2^{2^j m-1}$, and m and x_i are of the statement of 4.10. In other words, $\gamma_j\in\mathbb{N}_0$ is such a number that its base-2 expansion agrees with the first $2^j m$ terms of the sequence $\{\delta_j(x_i)\colon i=0,1,2,\dots\}$, where $x_{i+1}=g_{i \bmod m}(x_i)$, and $\mathcal{G}=\{g_0,\dots,g_{m-1}\}$ is a finite sequence of compatible measure preserving mappings of $\mathbb{Z}_2$ onto itself, see 4.10. Thus, $\gamma_j\in\{0,1,\dots,2^{2^j m}-1\}$, and γ_j depends on x_0 and on $\mathcal{G}$. Yet an arbitrary purely periodic sequence of period length $2^{j+1}m$ such that the second half of its period is a bitwise negation of the first half (the latter could be considered as a base-2 expansion of rational integer γ_j), being treated as a 2-adic reresentation of a rational number could be represented as (5.9.1) (see the proof of 5.8). So we wonder what sequences of such kind could be represented by coordinate sequences of wreath products of automata described by theorem 4.10.

In other words, to each sequence $\mathcal{Z}$ described by theorem 4.10 we associate a sequence $\Gamma(\mathcal{Z})=\{\gamma_0,\gamma_1,\dots\}$ of non-negative raional integers γ_j such that $0\le\gamma_j\le 2^{2^j m}-1$ iff (5.9.1) holds for all $j=0,1,2,\dots$. Now we take an arbitrary sequence Γ of this type and wonder whether this sequence could be associated to some sequence $\mathcal{Z}$ described by theorem 4.10. Generally speaking, the answer is *no*, since according to 4.10 the sequence $\delta_0(\mathcal{F})$ is purely periodic with period length *exactly* $2m$. However, a purely periodic sequence $\mathcal{S}$ of period length $2^n m$ such that the second half of its period is a bitwise negation of the first half, i.e., such that $\mathcal{S}$ could be represented in a form (5.9.1) as $\mathcal{S}=\frac{2^{2m}-\gamma_0}{2^{2m}+1}$ for suitable $0\le\gamma_0\le 2^{2m}-1$, *not necessrily has exact period length* $2^n m$ (see note 4.11). However, according to 4.11, senior coordinate sequences $\delta_j(\mathcal{Z})$ $(j\ge 1)$ could have exact periods smaller than $2^{j+1}m$. So it is reasonable to ask whether an arbitrary sequence $\Gamma=\{\gamma_1,\gamma_2,\dots\}$ of non-negative rational integers γ_j such that $0\le\gamma_j\le 2^{2^j m}-1$ corresponds in the above meaning to a certain sequence $\mathcal{Z}$ described by theorem 4.10. In this case the answer is *yes*. Namely, the following theorem holds.

5.10**. Theorem.** *Let* $m>1$ *be a rational integer, and let* $\Gamma=\{\gamma_0,\gamma_1,\dots\}$ *be an arbitrary sequence over* $\mathbb{N}_0$ *such that* $\gamma_j\in\{0,1,\dots,2^{2^j m}-1\}$ *for all* $j=0,1,2,\dots$. *Then there exist a finite sequence* $\mathcal{G}=\{g_0,\dots,g_{m-1}\}$ *of compatible measure preserving mappings of* $\mathbb{Z}_2$ *onto itself and a* 2*-adic integer* $x_0\in\mathbb{Z}_2$ *such that* $\mathcal{G}$ *satisfies conditions of theorem 4.10, and* $\delta_j(\mathcal{Z})$ *satisfies* (5.9.1) *for all* $j=1,2,\dots,$ *where* *the recurrence sequence* $\mathcal{Z} = \{x_0, x_1, \ldots \in \mathbb{Z}_2\}$ *is defined by the recurrence relation* $x_{i+1} = g_{i \bmod m}(x_i)$, $(i = 0, 1, 2, \ldots)$.

Proof. According to 3.13, a mapping $g_i\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatble and measure preserving iff each $\delta_j(g_i(x))$ is a Boolean polynomial in Boolean veriables $\chi_0 = \delta_0(x), \chi_1 = \delta_1(x), \ldots$ that is linear with respect to χ_j, i.e., $\delta_j(g_i(x))$ could be represented as

$$\delta_j(g_i(x)) = \chi_j + \varphi_j^i(\chi_0, \ldots, \chi_{j-1}),$$

where $\varphi_j^i = \varphi_j^i(\chi_0, \ldots, \chi_{j-1})$ is an arbitrary Boolean polynomial in Boolean variables $\chi_0, \ldots, \chi_{j-1}$. Thus, a compatible and measure preserving mapping g_i is completely determined by a sequence $\varphi_0^i, \varphi_1^i, \ldots$ of corresponding Boolean polynomials. So, given a sequence Γ we have to determine $x_0 \in \mathbb{N}_0$ and a family $\{\varphi_j^i\colon i = 0, 1, \ldots, m-1; j = 0, 1, 2, \ldots\}$ of Boolean functions such that the respective measure preserving mappings g_k $(k = 0, 1, \ldots, m-1)$ satisfy theorem 4.10 and that $\delta_j(\mathcal{Z})$ satisfies (5.9.1) for all $j = 1, 2, \ldots$, where the recurrence sequence $\mathcal{Z} = \{x_0, x_1, \ldots \in \mathbb{Z}_2\}$ is defined by the recurrence relation $x_{i+1} = g_{i \bmod m}(x_i)$, $(i = 0, 1, 2, \ldots)$.

To start with, we set $x_0 = \delta_0(\gamma_0) + \delta_0(\gamma_1) \cdot 2 + \delta_0(\gamma_2) \cdot 2^2 + \cdots \in \mathbb{Z}_2$. Further we describe an inductive procedure to determine φ_j^i successively for j=0,1,2,. . . .

For $j = 0$ we fix arbitrary $g_0(0) = \varphi_0^0, \ldots, g_{m-1}(0) = \varphi_0^{m-1} \in \{0, 1\}$ that satisfy conditions (1) and (2) of theorem 4.10. Note that thus we have determined all the mappings g_i $(i = 0, 1, \ldots, m-1)$ modulo 2. Note also that a recurrence sequence $\mathcal{X}_0 = \{\xi_0^0, \xi_0^1, \ldots\}$ defined by relations $\xi_0^0 = x_0 \bmod 2$, $\xi_{k+1}^0 = g_{k \bmod m}(\xi_k^0) \bmod 2$ is a purely periodic sequence over $\mathbb{Z}/2 = \{0, 1\}$ with period length exactly $2m$, that each element of $\mathbb{Z}/2$ occurs at the period exactly m times, and that $\xi_{k+m}^0 \equiv \xi_k^0 + 1 \pmod 2$ (see the very beginning of the proof of 4.7).

Suppose that we have already determined Boolean polynomials φ_j^i for $j = 0, 1, \ldots, n-1$, $i = 0, 1, \ldots, m-1$ in such a way that all the members of a recurrence sequence $\mathcal{X}_{n-1} = \{\xi_0^{n-1}, \xi_1^{n-1}, \ldots\}$ defined by relations $\xi_0^{n-1} = x_0 \bmod 2^n$, $\xi_{k+1}^{n-1} = g_{k \bmod m}(\xi_k^{n-1}) \bmod 2^n$, satisfy a congruence $\delta_j(\xi_{k+2^{n-1}m}^{n-1}) \equiv \delta_j(\xi_k^{n-1}) + 1 \pmod 2$ for all $j = 0, 1, \ldots, n-1$ and $k = 0, 1, 2, \ldots$. Note that then easy induction on j (which actually is already done during the proof of claim (3) of lemma 4.7) shows that for any k

$$|\{\xi_{k+sm}^{n-1}\colon s = 0, 1, \ldots, 2^n - 1\}| = 2^n. \tag{5.10.1}$$

Hence, $\mathcal{X}_{n-1}$ is a purely periodic sequence over $\mathbb{Z}/2^n$ of period length exactly $2^n m$, with each element of $\mathbb{Z}/2^n$ occuring at the period exactly m times. Now we define Boolean polynomials φ_n^i for $i = 0, 1, \ldots, m-1$.

For a Boolean polynomial φ in Boolean variables $\chi_0, \ldots, \chi_s$ and for $z \in \mathbb{Z}_2$ denote $\varphi(z) = \varphi(\delta_0(z), \ldots, \delta_s(z))$. Proceeding with this notation, set

$$\varphi_n^{k \bmod m}(\xi_k^{n-1}) \equiv \delta_k(\gamma_n) + \delta_{k+1}(\gamma_n) \pmod 2, \tag{5.10.2}$$

for $k = 0, 2, \ldots, 2^n m - 2$. Set also

$$\varphi_n^{m-1}(\xi_{2^n m-1}^{n-1}) \equiv \delta_{2^n m-1}(\gamma_n) + \delta_0(\gamma_n) + 1 \pmod 2. \tag{5.10.3}$$

Note that in view of (5.10.2) and (5.10.1) the Boolean functions φ_n^i of n variables (and whence, corresponding Boolean polynomials) for $i = 0, 1, \ldots, m-2$ are well defined; Also, the Boolean polynomial φ_n^{m-1} is well defined in view of (5.10.3), (5.10.2), and (5.10.1).

Consider now a recurrence sequence $\mathcal{E}_n = \{\varepsilon_k \colon k = 0, 1, 2, \dots\}$ over $\mathbb{Z}/2$ defined by relations $\varepsilon_0 = \delta_0(\gamma_n)$, $\varepsilon_{k+1} = \varepsilon_k + \varphi_n^{k \bmod m}(\xi_k^{n-1}) \pmod 2$. In view of (5.10.2) one has $\varepsilon_k = \delta_k(\gamma_n)$ for $k = 0, 2, \dots, 2^n m - 1$, and $\varepsilon_{2^n m} \equiv \delta_0(\gamma_n) + 1 \pmod 2$ in view of (5.10.3). Yet $\mathcal{X}_{n-1}$ is a purely periodic sequence over $\mathbb{Z}/2^n$ of period length exactly $2^n m$; proceeding with this we obtain succesively in view of (5.10.3) and (5.10.2):

$$\begin{aligned}
&\varepsilon_{2^n m} \equiv \delta_0(\gamma_n) + 1 \pmod 2, && \dots, && \varepsilon_{2^n m + (2^n m - 1)} \equiv \delta_{2^n m - 1}(\gamma_n) + 1 \pmod 2,\\
&\varepsilon_{2 \cdot 2^n m} \equiv \delta_0(\gamma_n) \pmod 2, && \dots, && \varepsilon_{2 \cdot 2^n m + (2^n m - 1)} \equiv \delta_{2^n m - 1}(\gamma_n) \pmod 2,\\
&\varepsilon_{3 \cdot 2^n m} \equiv \delta_0(\gamma_n) + 1 \pmod 2, && \dots
\end{aligned}$$

Note that in view of the definition of ε_k one has

$$\varepsilon_{2^n m} = \delta_0(\gamma_n) + \sum_{k=0}^{2^n m - 1} \varphi_n^{k \bmod m}(\xi_k^{n-1}).$$

But the sum in the right hand side must be 1 modulo 2 since $\varepsilon_{2^n m} \equiv \delta_0(\gamma_n) + 1 \pmod 2$, as it was proved above. So, in view of (5.10.1) one has

$$\sum_{k=0}^{2^n m - 1} \varphi_n^{k \bmod m}(\xi_k^{n-1}) \equiv \sum_{i=0}^{m-1} \sum_{\xi \in \mathbb{Z}/2^n} \varphi_n^i(\xi) \equiv 1 \pmod 2.$$

With the note that $\sum_{\xi \in \mathbb{Z}/2^n} \varphi_n^i(\xi)$ is just a weight of a Boolean polynomial φ_n^i, we conclude that an odd number of Boolean polymomials of $\varphi_n^0, \dots, \varphi_n^{m-1}$ must be of odd weight (cf. conditions of lemma 4.7).

Now setting $\xi_k^n = \xi_k^{n-1} + 2^n \cdot \varepsilon_k$ for $k = 0, 1, 2, \dots$ we obtain a sequense $\mathcal{X}_n = \{\xi_0^n, \xi_1^n, \dots\}$ over $\mathbb{Z}/2^{n+1}$ such that members of $\mathcal{X}_n$ satisfy the following relations

$$\begin{aligned}
&\xi_0^n = x_0 \bmod 2^{n+1},\\
&\xi_{k+1}^n = g_{k \bmod m}(\xi_k^n) \bmod 2^{n+1},\\
&\delta_j(\xi_{k+2^n m}^n) \equiv \delta_j(\xi_k^n) + 1 \pmod 2
\end{aligned}$$

for all $j = 0, 1, \dots, n$ and $k = 0, 1, 2, \dots$. Moreover, $\mathcal{X}_n$ is a purely periodic sequence with period length $2^{n+1} m$ (in view of the third of preceeding congruences, since the sequence $\mathcal{X}_{n-1}$ is purely periodic with period length exactly $2^n m$ by the above assumption), and each element of $\mathbb{Z}/2^{n+1}$ occurs at the period exactly $2^{n+1} m$ times. Finally, $\delta_n(\mathcal{X}_n) = \{\varepsilon_0, \varepsilon_1, \dots\} = \frac{2^{2^n m} - \gamma_n}{2^{2^n m} + 1}$.

With the use of this inductive procedure we construct for $n = 1, 2, \dots$ well defined mappings g_i modulo 2^{n+1} ($i = 0, 1, \dots, m-1$) that are compatible and bijective modulo 2^{n+1}; moreover, a corresponding recurrence sequence $\mathcal{X}_n$ defined by relation $x_{i+1} = g_{i \bmod m}(x_i) \bmod 2^{n+1}$ satisfy (5.9.1) for $j = 1, \dots, n$. The mappings g_i satisfy condition (3) of 4.10 for $k = 1, 2, \dots, n+1$ since, as it was noted above, the odd number of Boolean polymomials of $\varphi_k^0, \dots, \varphi_k^{m-1}$ are of odd weight for all $k = 1, 2, \dots, n$. From the definition of g_i modulo 2 it follows that these mappings g_i satisfy conditions (1) and (2) of 4.10. This completes the proof in view of the notices that were made at the very beginning of it. □

Distribution of k-tuples. In this subsection we study a distribution of overlapping binary k-tuples in output sequences of automata introduced above. As it was shown, an output sequence of any of these automata with output alphabet $\{0, 1, 2, \dots, 2^n - 1\} = \mathbb{Z}/2^n$ is strictly uniformly distributed as a sequence over

$\mathbb{Z}/2^n$. That is, it is purely periodic, and each element of $\mathbb{Z}/2^n$ occurs at the period the same number of times. However, one could consider the same sequence as a binary sequence, and ask what is a distribution of n-tuples in such a sequence. *Strict uniform distribution of an arbitrary sequence $\mathcal{T}$ as a sequence over $\mathbb{Z}/2^n$ does not necessarily imply uniform distribution of overlapping n-tuples, if this sequence is considered as a binary sequence!*

For instance, let $\mathcal{T}$ be the following strictly uniformly distributed sequence over $\mathbb{Z}/4$ with perid length exactly 4: $\mathcal{T} = 023102310231\ldots$. Then its representation as a binary sequence is $\mathcal{T} = 0001111000011110000111 10\ldots$ (recall that according to our conventions in Section 2 we write senior bits right, and not left; i.e., $2 = 01$, $1 = 10$, etc.) Obviously, when we consider $\mathcal{T}$ as a sequence over $\mathbb{Z}/4$, then each number of $\{0, 1, 2, 3\}$ occurs in the sequence with the same frequency $\frac{1}{4}$. Yet if we consider $\mathcal{T}$ as a binary sequence, then 00 (as well as 11) occurs in this sequence with frequency $\frac{3}{8}$, whereas 01 (and 10) occurs with frequency $\frac{1}{8}$. Thus, the sequence $\mathcal{T}$ is uniformly distributed over $\mathbb{Z}/4$, and it is not uniformly distributed over $\mathbb{Z}/2$.

In this subsection we show that such an effect does not take place for output sequences of automata described in 4.3, 4.5, 4.6, 4.7, and 4.10: *Considering any of these sequences as a binary sequence, a distribution of k-tuples is uniform, for all $k \le n$.* Now we state this property more formally.

Consider a (binary) *n-cycle* $C = (\varepsilon_0\varepsilon_1 \ldots \varepsilon_{n-1})$; that is, an oriented graph with vertexes $\{a_0, a_1, \ldots, a_{n-1}\}$ and edges

$$\{(a_0, a_1), (a_1, a_2), \ldots, (a_{n-2}, a_{n-1}), (a_{n-1}, a_0)\},$$

where each vertex a_j is labelled with $\varepsilon_j \in \{0, 1\}$, $j = 0, 1, \ldots, n-1$. (Note that then $(\varepsilon_0\varepsilon_1 \ldots \varepsilon_{n-1}) = (\varepsilon_{n-1}\varepsilon_0 \ldots \varepsilon_{n-2}) = \ldots$, etc.).

Clearly, each purely periodic sequence $\mathcal{S}$ over $\mathbb{Z}/2$ with period $\alpha_0 \ldots \alpha_{n-1}$ of length n could be related to a binary n-cycle $C(\mathcal{S}) = (\alpha_0 \ldots \alpha_{n-1})$. Conversly, to each binary n-cycle $(\alpha_0 \ldots \alpha_{n-1})$ we could relate n purely periodic binary sequences of period length n: They are n shifted versions of the sequence

$$\alpha_0 \ldots \alpha_{n-1}\alpha_0 \ldots \alpha_{n-1} \ldots,$$

that is

$$\begin{aligned}
&\alpha_1 \ldots \alpha_{n-1}\alpha_0\alpha_1 \ldots \alpha_{n-1}\alpha_0 \ldots,\\
&\alpha_2 \ldots \alpha_{n-1}\alpha_0\alpha_1\alpha_2 \ldots \alpha_{n-1}\alpha_0\alpha_1 \ldots,\\
&\ldots \qquad \ldots \qquad \ldots\\
&\alpha_{n-1}\alpha_0\alpha_1\alpha_2 \ldots \alpha_{n-2}\alpha_{n-1}\alpha_0\alpha_1\alpha_2 \ldots \alpha_{n-2} \ldots
\end{aligned}$$

Further, *a k-chain in a binary n-cycle C* is a binary string $\beta_0 \ldots \beta_{k-1}$, $k < n$, that satisfies the following condition: There exists $j \in \{0, 1, \ldots, n-1\}$ such that $\beta_i = \varepsilon_{(i+j) \bmod n}$ for $i = 0, 1, \ldots, k-1$. Thus, a k-chain is just a string of length k of labels that corresponds to a chain of length k in a graph C.

We call a binary n-cycle C *k-full*, if each k-chain occurs in the graph C the same number $r > 0$ of times.

Clearly, if C is k-full, then $n = 2^k r$. For instance, a well-known De Bruijn sequence is an n-full 2^n-cycle, see e.g. [25] for further references. Clearly enough that a k-full n-cycle is $(k-1)$-full: Each $(k-1)$-chain occurs in C exactly $2r$ times, etc. Thus, if an n-cycle $C(\mathcal{S})$ is k-full, then each m-tuple (where $1 \le m \le k$)

occurs in the sequence $\mathcal{S}$ with the same probability (limit frequency) $\frac{1}{2^m}$. That is, the sequence $\mathcal{S}$ is *k-distributed*, see [2, Section 3.5, Definition D].

5.11. **Definition.** A purely periodic binary sequence $\mathcal{S}$ with period length exactly N is said to be *strictly k-distributed* iff a corresponding N-cycle $C(\mathcal{S})$ is k-full.

Thus, if a sequence $\mathcal{S}$ is strictly k-distributed, then it is strictly s-distributed, for all positive $s \le k$.

A k-distribution is a good "indicator of randomness" of an infinite sequence: The larger k, the better the sequence, i.e., "more random". The best case is when a sequence is k-distibuted for all $k = 1, 2, \ldots$. Such sequences are called ∞-distributed. Obviuosly, a periodic sequence can not be ∞-distributed.

On the other hand, a periodic sequence is just an infinite repetition of a finite sequence, the period. A common requirement in applications is that the period length must be large, and the whole period is never used in practice. For instance, in cryptography normally a relatively small part of a period is used. So we are interested of "how random" is a finite sequence, namely, the period. Of course, it seems very reasonable to consider a period of length n as an n-cycle and to study a distribution of k-tuples in n-cycle; for instance, if this n-cycle is k-full, the distribution of k-tuples is strictly uniform. However, other approaches also exist.

In [2, Section 3.5, Definition Q1] there is considered the following "indicator of randomness" of a finite sequence over a finite alphabet A (we formulate the corresponding definition for $A = \{0, 1\}$): A finite binary sequence $\varepsilon_0\varepsilon_1 \ldots \varepsilon_{N-1}$ of length N is said to be random, iff

$$\left| \frac{\nu(\beta_0 \ldots \beta_{k-1})}{N} - \frac{1}{2^k} \right| \le \frac{1}{\sqrt{N}} \tag{5.11.1}$$

for all $0 < k \le \log_2 N$, where $\nu(\beta_0 \ldots \beta_{k-1})$ is the number of occurences of a binary word $\beta_0 \ldots \beta_{k-1}$ in a binary word $\varepsilon_0\varepsilon_1 \ldots \varepsilon_{N-1}$. If a finite sequence is random in a sence of this Definition Q1 of [2], we shall say that it has *a property* Q1, or *satisfies* Q1. We shall also say that an *infinite periodic sequence satisfy* Q1 iff its exact period satisfies Q1. Note that, constrasting to the case of strict k-distribution, which implies strict $(k-1)$-distribution, it is not enough to demonstrate only that (5.11.1) holds for $k = \lfloor \log_2 N \rfloor$ to prove a finite sequence of length N satisfies Q1: For instance, a sequence 1111111100000111 satisfies (5.11.1) for $k = \lfloor \log_2 n \rfloor = 4$, and does not satisfy (5.11.1) for $k = 3$. Note that an analogon of property Q1 for odd prime p could be stated in an obvious way.

Now we are able to state the following

5.12. **Theorem.** *Let a sequence $\mathcal{Z}$ over $\mathbb{Z}/2^n$ be any of output sequences of wreath products of automata* (described in 4.3, 4.5, 4.6, 4.7, and 4.10; hence $\mathcal{Z}$ is a purely periodic sequence of period length $2^n\ell$, where $\ell = 2^m$ for wreath products described by 4.3 or 4.5, and $\ell = m$ otherwise) *or, in particular, of a congruential generator of a maximum period length* (this corresponds to the case $\ell = m = 1$)*. Let $\mathcal{Z}'$ be a binary representation of $\mathcal{Z}$* (hence $\mathcal{Z}'$ is a purely periodic binary sequence of period length exactly $2^n\ell n$)*. Then the sequence $\mathcal{Z}'$ is strictly n-distributed.*

Moreover, if $\mathcal{Z}'$ is a binary output sequence of a congruential generator of a maximum period length, then this sequence satisfies Q1.

Proof. The sequence $\mathcal{Z} = z_0z_1\ldots$ is a recurrence sequence over $\{0,1,\ldots,n-1\}$ that satisfy the following recurrence relation:

$$z_{i+1} = f_i(z_i) \bmod 2^n \qquad (i = 0,1,2,\ldots),$$

where f_i is compatible and measure preserving mapping of $\mathbb{Z}_2$ onto itself. Here and further in the proof we assume that subscript i of f is always reduced modulo ℓ for $\ell > 1$ and is empty symbol for $\ell = 1$ (the latter case corresponds to congruential generator of a maximum period length with state transition function $f \bmod 2^n$, where f is ergodic). Let $\mathcal{Z}' = \zeta_0\zeta_1\ldots$ be a binary representation of the sequence $\mathcal{Z}$. Take an arbitrary binary word $\mathbf{b} = \beta_0\beta_1\ldots\beta_{n-1}$, $\beta_j \in \{0,1\}$, and for $k \in \{0,1,\ldots,n-1\}$ denote

$$\nu_k(\mathbf{b}) = |\{r\colon 0 \le r < 2^n\ell n;\ r \equiv k \pmod n;\ \zeta_r\zeta_{r+1}\ldots\zeta_{r+n-1} = \beta_0\beta_1\ldots\beta_{n-1}\}|$$

Obviously, $\nu_0(\mathbf{b})$ is the number of occurences of a rational integer z with base-2 expansion $\beta_0\beta_1\ldots\beta_{n-1}$ at the exact period of the sequence $\mathcal{Z}$. Hence, $\nu_0(\mathbf{b}) = \ell$ since the sequence $\mathcal{Z}$ is strictly uniformly distributed modulo 2^n. Now consider $\nu_k(\mathbf{b})$ for $0 < k < n$.

Fix $k \in \{1,2\ldots,n-1\}$ and let $r = k + tn$. As all f_i are compatible, then $\zeta_r\zeta_{r+1}\ldots\zeta_{r+n-1} = \beta_0\beta_1\ldots\beta_{n-1}$ holds if and only if the following two relations hold simultaneously:

$$\zeta_{tn+k}\zeta_{tn+k+1}\ldots\zeta_{tn+n-1} = \beta_0\beta_1\ldots\beta_{n-k-1} \tag{5.12.1}$$

$$f_t(\overline{\zeta_{tn}\zeta_{tn+1}\ldots\zeta_{tn+k-1}}) \equiv \overline{\beta_{n-k}\beta_{n-k+1}\ldots\beta_{n-1}} \pmod{2^k}. \tag{5.12.2}$$

Here $\overline{\gamma_0\gamma_1\ldots\gamma_s} = \gamma_0 + \gamma_1\cdot 2 + \cdots + \gamma_s\cdot 2^s$ for $\gamma_0,\gamma_1,\ldots,\gamma_s \in \{0,1\}$ is a rational integer with base-2 expansion $\gamma_0\gamma_1\ldots\gamma_s$.

We consider a case $\ell = 1$ first; so $f_t = f$. Then for a given $\mathbf{b} = \beta_0\beta_1\ldots\beta_{n-1}$ congruence (5.12.2) has exactly one solution $\overline{\alpha_0\alpha_1\ldots\alpha_{k-1}}$ modulo 2^k, since f is ergodic, whence, bijective modulo 2^k. Thus, in view of (5.12.1) and (5.12.2) we conclude that $\zeta_r\zeta_{r+1}\ldots\zeta_{r+n-1} = \beta_0\beta_1\ldots\beta_{n-1}$ holds if and only if

$$\zeta_s\zeta_{s+1}\ldots\zeta_{s+n-1} = \alpha_0\alpha_1\ldots\alpha_{k-1}\beta_0\beta_1\ldots\beta_{n-k-1}, \tag{5.12.3}$$

where $s = tn$. Yet there exists exactly one $s \equiv 0 \pmod n$, $0 \le s < 2^n n$ such that (5.12.3) holds, since every element of $\mathbb{Z}/2^n$ occurs at the period of $\mathcal{Z}$ exactly once. We conclude now that if $\ell = 1$ then $\nu_k(\mathbf{b}) = 1$ for all $k \in \{0,1,\ldots,n-1\}$; thus, $\nu(\mathbf{b}) = \sum_{j=0}^{n-1}\nu_j(\mathbf{b}) = n$ for all $\mathbf{b}$. This means that $(2^n n)$-cycle $C(\mathcal{Z}')$ is n-full, whence, the sequence $\mathcal{Z}'$ is strictly n-distributed.

A similar argument is applied to the case $\ell > 1$. Namely, for a given $j \in \{0,1,\ldots,\ell-1\}$ consider those $r = k + tn < 2^n\ell n$ where $t \equiv j \pmod \ell$ and denote

$$\nu_k^j(\mathbf{b}) = |\{r\colon 0 \le r < 2^n\ell n;\ r = k + tn;\ t \equiv j \pmod \ell;\ \zeta_r\zeta_{r+1}\ldots\zeta_{r+n-1} = \mathbf{b}\}|.$$

Now $\zeta_r\zeta_{r+1}\ldots\zeta_{r+n-1} = \beta_0\beta_1\ldots\beta_{n-1}$ holds if and only if (5.12.3) holds, where $\overline{\alpha_0\alpha_1\ldots\alpha_{k-1}}$ is a unique solution of congruence (5.12.2) modulo 2^k. This solution exists since all f_j are measure preserving, see theorem 4.10. Yet (5.12.3) is equivalent to the condition

$$z_t = \overline{\alpha_0\alpha_1\ldots\alpha_{k-1}\beta_0\beta_1\ldots\beta_{n-k-1}},$$

where $t \in \{j, j+\ell, \ldots, j+(2^n-1)\ell\}$. But in view of claim (3) of lemma 4.7 for a given $\overline{\alpha_0\alpha_1\ldots\alpha_{k-1}\beta_0\beta_1\ldots\beta_{n-k-1}}$ there exist exactly one $t \in \{j, j+\ell, \ldots, j+(2^n-1)\ell\}$ such that the latter equality holds. So we conclude that $\nu_k^j(\mathbf{b}) = 1$, hence $\nu_k(\mathbf{b}) =$

$\sum_{j=0}^{\ell-1}\nu_k^j(\mathbf{b})=\ell$, and finally $\nu(\mathbf{b})=\sum_{k=0}^{n-1}\nu_k(\mathbf{b})=n\ell$ for all $\mathbf{b}$. This completes the proof of the first assertion of the theorem.

To prove the second assertion note that we return to the case $\ell=1$; hence, in view of the first assertion every m-tuple for $1\le m\le n$ occurs at the $2^n n$-cycle $C(\mathcal{Z}')$ exactly $2^{n-m}n$ times. Thus, every such m-tuple occurs $2^{n-m}n-c$ times at the finite binary sequence $\hat{\mathcal{Z}}=\hat z_0\hat z_1\ldots\hat z_{2^n-1}$, where $\hat z$ for $z\in\{0,1,\ldots,2^n-1\}$ is an n-bit sequence that agrees with base-2 expansion of z. Note that c depends on the m-tuple, yet $0\le c\le m-1$ for every m-tuple. Easy algebra shows that (5.11.1) holds for these m-tuples.

Now to prove that $\mathcal{Z}'$ satisfies Q1 we have only to demonstrate that (5.11.1) holds for m-tuples with $m=n+d$, where $0<d\le\log_2 n$. We claim that such an m-tuple occurs at the sequence $\hat{\mathcal{Z}}$ not more than n times.

Indeed, in this case $\zeta_r\zeta_{r+1}\ldots\zeta_{r+n+d-1}=\beta_0\beta_1\ldots\beta_{n+d-1}$ holds iff besides the two relations (5.12.1) and (5.12.2) the following extra congruence holds:

$$f(\overline{\zeta_{tn}\zeta_{tn+1}\ldots\zeta_{tn+k-1}\beta_0\beta_1\ldots\beta_{d-1}})\equiv\overline{\beta_{n-k}\beta_{n-k+1}\ldots\beta_{n+d-1}}\pmod{2^{k+d}},$$

where $k=r\bmod n$. Yet this extra congruence may or may not have a solution in unknowns $\zeta_{tn},\zeta_{tn+1},\ldots,\zeta_{tn+k-1}$; this depends on $\beta_0\beta_1\ldots\beta_{n+d-1}$. But if such a solution exists, it is unique for a given $k\in\{0,1,\ldots,n-1\}$, since f is ergodic, whence, bijective modulo 2^s for all $s=1,2,\ldots$. This proves our claim. Now easy exercise in inequalities shows that (5.11.1) holds in this case, thus completing the proof of the theorem. □

5.13. *Note.* The first asssertion of theorem 5.12 remains true for *wreath products of truncated automata*, i.e. for the sequence $\mathcal{F}$ of corollary 4.12, where $F_j(x)=\left\lfloor\frac{x}{2^{n-k}}\right\rfloor\bmod 2^k$, $j=0,1,\ldots,\ell-1$, a truncation of $n-k$ low order bits. Namely, *a binary representation $\mathcal{F}'$ of the sequence $\mathcal{F}$ is a purely periodic strictly k-distributed binary sequence of period length $2^n\ell k$.*

The second assertion of theorem 5.12 holds for arbitrary prime p. Namely, *a base-p representation of an output sequence of a congruential generator over $\mathbb{Z}/p^n$ of a maximum period length is strictly n-distributed sequence over $\mathbb{Z}/p$ of period length exactly $p^n n$, which satisfies Q1.*

Moreover, the first assertion of 5.12 holds for truncated congruential generators with output function $F(x)=\left\lfloor\frac{x}{p^{n-k}}\right\rfloor\bmod p^k$. Namely, *a base-$p$ representation of an output sequence of a truncated congruential generator over $\mathbb{Z}/p^n$ of a maximum period length is a purely periodic strictly k-distributed sequence over $\mathbb{Z}/p$ of period length $p^n k$.*

The second assertion for this generator holds whenever $2+p^k>kp^{n-k}$; thus, *one could truncate $\le\left(\frac{n}{2}-\log_p\frac{n}{2}\right)$ lower order digits without affecting property Q1.*

All these statements could be proved by slight modifications of the proof of theorem 5.12. We omit details.

6. Some cryptanalysis

A main goal of this section is to demonstrate that with the use of constructions described in Section 4 it might be possible to design stream ciphers such that the problem of their key recovery is intractable up to some plausible conjectures.

Consider a "known plaintext" attack. That is, a cryptanalyst obtains a plaintext and a corresponding encrypted text and tries to recover a key. Since the encryption with stream cipher is just bitwise XORing of a plaintext with a binary output sequence of a generator, a cryptanalyst obtains an output sequence and try to recover a key. Note that the constructions we considered above enables one to make both the initial state, state transition function and output function to be key-dependent, so in general a cryptanalst has to recover a key from a known recurrence sequence $\{y_s, y_{s+1}, \ldots\}$ that corresponds to the recurrence law $x_{i+1} = f_i(x_i) \bmod 2^n$, $y_{i+1} = g_i(x_i)$. Thus, in general a cryptoanalyst has to recover an initial state x_0, a family of state transition functions $\{f_j\}$, a family of output functions $\{g_j\}$, and the order these state transition and output functions are used while producing the output sequence.

Of course, an analysis in such a general form is senseless. On the one hand it is obvious that nothing can be recovered in case f_i and g_i are arbitrary mappings that satisfy conditions of 4.12, and no extra information is known to a cryptoanalyst. On the other hand, it is obvious that there exist degenerate cases that everything can be easily recovered even without extra information available.

For instance, let $m = 4k - 1$; put $f_i(x) = x + 1$ if $i \in \{0, 1, \ldots, m-1\}$ is odd, and put $f_i(x) = 1 \oplus (x + 1)$ for even $i \in \{0, 1, \ldots, m-1\}$. Let all $g_i = \lfloor \frac{x}{2} \rfloor \bmod 2^n$ be truncations of the least significant bit. Note that this case satisfies conditions of 4.12; thus, the corresponding output sequence modulo 2^n is purely periodic of period length $2^n m$, and each element of $\mathbb{Z}/2^n$ occurs at the period exactly twice. Yet the structure of the output sequence is so specific (exact description of it could easily be obtained by a reader) that it is absolutely no problem to break such a scheme.

Thus, one can say nothing definite on how strong are generators considerd in the paper against even a single attack without considering a concrete scheme. We are not going to study concrete schemes in this paper, yet we demonstrate by a corresponding example that among the generators we study there could exist ones that are provably strong against certain attacks, say, against a known plaintext attack.

To describe such an example we have to make some preliminary assumptions. Choose (randomly and independently) k Boolean polynomials

$$\psi_i(\chi_0, \ldots, \chi_{n-1}) \qquad (i = 0, 1, \ldots, k-1)$$

in n Boolean variables $\chi_0, \ldots, \chi_{n-1}$ each, such that the number of non-zero monomials in each ψ_i is a polynomial in n (k could be fixed, or could be a polynomial in n either). Consider a mapping $F\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^k$ defined by

$$F(\chi_0, \ldots, \chi_{n-1}) = \psi_0(\chi_0, \ldots, \chi_{n-1}) + \cdots + \psi_{k-1}(\chi_0, \ldots, \chi_{n-1}) 2^{k-1},$$

where $\chi_j = \delta_j(x)$ for $x \in \mathbb{Z}/2^n$. We conjecture that *this function F could be considered as one-way*, that is, one could invert it (i.e., find an F-preimage in case it exists) only with negligible in n probability. Note that to find any F-preimage, i.e. to solve an equation $F(x) = y$ in unknown x one has to solve a system of k Boolean equations in n variables. However, *to determine whether a given system of k Boolean polynomials in n variables have a common zero is an NP-complete problem*, see e.g. [26, Appendix A, Section A7.2, Problem ANT-9]. So, at our view, the conjecture that the function F is one-way is as plausible as the one concerning any other “candidate to one-wayness” (for the short list of the latter see e.g. [27]):

Nobody today can solve a system of Boolean equations even if it is known that a solution exists (unless the system is of some special form).[8]

Proceeding with this plausible conjecture, to each Boolean polynomial ψ_i, $i = 0, 1, 2, \dots, k-1$ we relate a mapping $\Psi_i \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ in the following way: $\Psi_i(x) = \psi_i(\delta_0(x), \dots, \delta_{n-1}(x)) \in \{0, 1\} \subset \mathbb{Z}_2$. Now to each above mapping F we relate a mapping

$$f_F(x) = (1 + x) \oplus (2^{n+1}\Psi_0(x) + 2^{n+2}\Psi_1(x) + \cdots + 2^{n+k}\Psi_{k-1}(x))$$

of $\mathbb{Z}_2$ onto itself.

By the way, despite it is not very important, note that this mapping is a composition of bitwise logical and arithmetic operations: To a monomial $\chi_{r_1} \cdots \chi_{r_s}$, where $r_1, \dots, r_s \in \{0, 1, \dots, n-1\}$, $r_1 < \ldots < r_s$ we relate a binomial coefficient $\binom{x}{2^{r_1}+\cdots+2^{r_s}}$, then to a Boolean polynomial we relate a sum of corresponding binomial coefficients. For instance, to the Boolean polynomial $\psi = 1 + \chi_0 + \chi_0\chi_1 + \chi_1\chi_3$ we relate an integer valued polynomial $1 + x + \binom{x}{3} + \binom{x}{10}$. Since

$$\binom{x}{2^{r_1} + \cdots + 2^{r_s}} \equiv \delta_{r_1}(x) \cdots \delta_{r_s}(x) \pmod 2$$

in view of Lucas' congruence[9], $\Psi_j(x) \equiv P_j(x) \pmod 2$, where $P_j(x)$ is a polynomial over a field of rational integers $\mathbb{Q}$ that corresponds to the Boolean polynomial ψ_j in the above sence. Thus, $\Psi_j(x) = P_j(x) \ \mathsf{AND}\ 1$, and the result follows.

Clearly,

$$\delta_j(f_F(x)) = \begin{cases} 1 \oplus \delta_0(x), & \text{if } j = 0; \\ \delta_j(x) \oplus \delta_0(x) \cdots \delta_{j-1}(x), & \text{if } 0 < j \le n; \\ \delta_j(x) \oplus \delta_0(x) \cdots \delta_{j-1}(x) \oplus \psi_{j-n-1}(\delta_0(x), \dots, \delta_{n-1}(x)), & \text{otherwise.} \end{cases}$$

In view of 3.13 the mapping $f_F \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatible and ergodic for any choice of Boolean polynomials $\psi_0, \dots, \psi_{k-1}$.

Consider a truncated congruential generator

$$\mathfrak{F} = \langle \mathbb{Z}/2^{n+k+1}, \mathbb{Z}/2^k, f_F \bmod 2^{n+k+1}, g, x_0 \rangle,$$

where $g(x) = \lfloor \frac{x}{2^{n+1}} \rfloor \bmod 2^k$, a truncation of $n+1$ low order bits of x. Since the state transition function is transitive and the output function is equiprobable, the output sequence of this generator is purely periodic with period length exactly 2^{n+k+1}, and each element of $\mathbb{Z}/2^k$ occurs at the period exactly 2^{n+1} times.

Let $x_0 \in \{0, 1, \dots, 2^n - 1\}$ be a key; in other words, the key length of a stream cipher is n, and we always take a key $z \in \{0, 1, \dots, 2^n - 1\}$ as an initial state (a seed). Thus, senior $k+1$ bits of an initial state are always zero. The key z is the only information that is not known to a cryptanalyst. Everything else, i.e., n, k, f_F, and g are known, as well as the first m members of the output sequence $\{y_i\}$ of the automaton.

Since $\delta_0(x) \cdots \delta_{j-1}(x) = 1$ iff $x \equiv -1 \pmod{2^j}$, the first m members of the output sequence with probability $1 - \epsilon$ (where ϵ is negligible if m is a polynomial

---

[8] However, the author does not know whether it is difficult to solve a *randomly choosen* system of Boolean equations and conjectures that it is.

[9] $\binom{n}{m} \equiv \binom{n_0}{m_0} \cdots \binom{n_s}{m_s} \pmod p$, where $n = n_0 + \cdots + n_s p^s$, $m = m_0 + \cdots + m_s p^s$ are base-p expansions of, respectively, n and m; p prime.

in n) are:

$$y_0 = \Psi_0(z) + 2\Psi_1(z) + \cdots + 2^{k-1}\Psi_{k-1}(z) = F(z);$$
$$\dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots$$
$$y_{m-1} = \Psi_0(z+m-1) + \cdots + 2^{k-1}\Psi_{k-1}(z+m-1) = F(z+m-1).$$

To find z a cryptanalist may solve any of the above equations; he could do it with negligible probability of success, since F is one-way. On the other hand, an assumption that a cryptanalist could find z with non-negligible probability means that he could invert F with non-negligible probability (see the first of the above equations). This contradicts our conjecture that F is one-way. Thus, the problem of key recovery of this scheme might be intractable up to the conjecture that F is one-way. Of course, here we have an overdefined system of equations, so in general one-wayness of F is not enough to prove that the problem is intractable.

Note. This construction could be extended to counter-dependent generators in an obvious way. We also note that the restriction the state transition function of the above generator is $1 + x$ modulo 2^{n+1} is imposed only to make the idea of the construction more transparent: It is possible to construct a corresponding stream cipher, which could be provably secure against a known plaintext attack, without this assumption. Note, however, that in stream chiphers presented in the paper both state transition function and output function are key dependent (like in the example mentioned in Introduction), so a cryptoanalyst has to solve a system of the form $F_i(x_i) = z_i \pmod 2)^n$ in indeterminates x_i where F_i are not known to him.

References

[1] L. Kuipers, H. Niederreiter. *Uniform Distribution of Sequences*, John Wiley & Sons, N.Y., etc. 1974 9

[2] D. Knuth. *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, (Third edition) Addison-Wesley, Reading M.A. 1998. 3, 48

[3] Mahler K. *p-adic numbers and their functions* (2nd edition) Cambridge Univ. Press, Cambridge: 1981. 6, 10, 17, 38

[4] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Springer-Verlag, New York, etc. 1977 6, 12, 17

[5] E. F. Brickell, A. M. Odlyzko 'Cryptanalysis: A Survey of Recent Results', *Proc. IEEE* ,**76** (1988), No 5, 578–593. 25

[6] V. S. Anashin 'Uniformly distributed sequences over p-adic integers', *Mat. Zametki*, **55** (1994), No 2, 3–46 (in Russian; English transl. in *Mathematical Notes*, **55**,(1994), No 2, 109–133.) 1, 6, 8, 10, 11, 14, 17, 18, 19, 21, 22, 27

[7] Anashin V. S. 'Uniformly distributed sequences over p-adic integers', *Number theoretic and algebraic methods in computer science. Proceedings of the Int'l Conference (Moscow, June–July, 1993)* (A. J. van der Poorten, I. Shparlinsky and H. G. Zimmer, eds.), World Scientific, 1995, 1–18. 1, 10, 11, 18, 19, 21, 22, 27

[8] Rivest R. 'Permutation polynomials modulo 2^w' *Finite fields and appl.* **7** (2001), No 2, pp. 287–292 22

[9] M. V. Larin 'Transitive polynomial transformations of residue class rings' *Diskret. Mat.* **14**(2002), No 2, pp. 20–32 (Russian) 11, 13, 23

[10] Klapper A., Goresky M. 'Feedback shift registers, 2-adic span, and combiners with memory', *J. Cryptology*, **10** (1997), 111–147. 41

[11] Anashin V. S. 'Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers', *J. Math. Sci.* (Plenum Publishing Corp., New York), **89** (1998), No 4, 1355 – 1390. 1

[12] Menezes A., van Oorshot P., Vanstone S. *Handbook of Applied Cryptography*, CRC Press, 1996. 25

[13] Shamir A., Tsaban B. *Guaranteeing the diversity of number generators.* Available from http://arXiv.org/ abs/ cs.CR/ 0112014 2, 26

[14] Krawczuk H. 'How to predict congruential generators', *J. Algorithms*, **13** (1992), No 4, 527–545. 23, 24, 25

[15] Brent R. P. 'Factorization of the tenth Fermat number' *Math. Comput.* **68** (1999), No 225. 41

[16] V. S. Anashin. 'Uniformly distributed sequences of p-adic integers, II', (Russian) *Diskret. Mat.* **14** (2002), no. 4, 3–64; English translation in *Discrete Math. Appl.* **12** (2002), no. 6, 527–590. A preprint in English available from http://arXiv.org/math.NT/0209407 1, 6, 7, 8, 10, 11, 12, 13, 18, 19, 21, 22, 27, 38

[17] G. Everest, A. van der Poorten, I. Shparlinsky. *Recurrence Sequences*, American Mathematical Society Surveys, Vol. 104, 2003. 10, 29, 38

[18] R. Rivest, M. Robshaw, R. Sidney, and Y. L. Yin. *The RC6 block cipher* . Available from http://www.rsa.com/rsalabs/rc6/ 11

[19] A. Klimov, A. Shamir. 'A new class of invertible mappings', in: *Cryptographic Hardware and Embedded Systems 2002* (B.S.Kaliski Jr.et al., eds.)), Lect. Notes in Comp. Sci.,Vol. 2523, Springer-Verlag, 2003, pp.470–483. 13, 14, 15, 21, 22

[20] A. Klimov, A. Shamir. 'Cryptographic applications of T-functions', in: *Selected Areas in Cryptography -2003* 25, 28, 31

[21] A. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir. 'Reconstructing truncated integer variables satisfying linear congruences'. *SIAM J. Comput.*,**17**(1988), No 2, pp. 262–280. 25

[22] D. Passman. *Permutation groups*, W. A. Benjamin, Inc., NY–Amsterdam, 1968. 26

[23] G. Marsaglia. 'Xorshift RNGs'. *Journal of Statistical Software* (electronic), **08**(2003), No. 14. Available from http://www.jstatsoft.org/v08/i14/xorshift.pdf 32

[24] R. Lidl, H. Niederreiter. *Finite Fields*, Addison-Wesley Publ. Co., 1983 38, 40

[25] Marshall Hall, Jr. *Combinatorial theory*, Blaisdell Publ. Co., 1967 47

[26] M. R. Garey, D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-completeness.* W.H. Freeman and Co., 1979 3, 51

[27] O. Goldreich, *Foundations of Cryptography. Basic Tools.* Cambridge Univ. Press, Cambridge, 2001. 51

Faculty of Information Security, Russian State University for the Humanities,, Kirovogradskaya Str., 25/2, Moscow 113534, Russia

E-mail address: `anashin@rsuh.ru, vladimir@anashin.msk.su`