PSEUDORANDOM NUMBER GENERATION BY p-ADIC ERGODIC TRANSFORMATIONS: AN ADDENDUM

VLADIMIR ANASHIN

Abstract. The paper study counter-dependent pseudorandom number generators based on m-variate ($m > 1$) ergodic mappings of the space of 2-adic integers $\mathbb{Z}_2$. The sequence of internal states of these generators is defined by the recurrence law $\mathbf{x}_{i+1} = H_i^B(\mathbf{x}_i) \bmod 2^n$, whereas their output sequence is $\mathbf{z}_i = F_i^B(\mathbf{x}_i) \mod 2^n$; here $\mathbf{x}_j, \mathbf{z}_j$ are m-dimensional vectors over $\mathbb{Z}_2$. It is shown how the results obtained for a univariate case could be extended to a multivariate case.

1. Introduction

In [1] we considered counter-dependent generators that produce recurrence sequences $\{u_i \in \mathbb{Z}/2^n\}$ of n-bit words according to the following law:

$$u_i = F_i(w_i); \quad w_{i+1} \equiv f_i(w_i) \pmod{2^n}, \quad (i = 0, 1, 2, \ldots).$$

In the mentioned paper we restricted ourselves mainly to the case of univariate mappings f_i and F_i. Trivially, each univariate mapping $\mathbb{Z}/2^{mn} \to \mathbb{Z}/2^{mn}$ of the resdue ring modulo 2^{mn} could be considered as a mapping $(\mathbb{Z}/2^n)^{(m)} \to (\mathbb{Z}/2^n)^{(m)}$ of a Cartesian power $(\mathbb{Z}/2^n)^{(m)}$ of the residue ring $\mathbb{Z}/2^n$, i.e., as an m-variate mapping. It turns out, however, that in some cases it is more effective to implement a univariate mapping in its multivariate form to achieve better performance. For instance, recently in [7] there were constructed examples of multivariate T-functions with a single cycle (i.e., of compatible ergodic functions, in our terminology, see [1]), which are very fast (see theorem 6 of [7] and the text thereafter).

Below we introduce some special way to derive multivariate compatible ergodic functions from univariate ones (the mentioned mappings of [7] originate this way); in fact, we merely represent univariate mappings in a multivariate form. This immediately implies that *one could apply all the results of* [1] *to estimate important cryptographic characteristics of these multivariate mappings* (e.g., linear and 2-adic spans, distribution of k-tuples), *as well as to construct multivariate output functions that improve periods of coordinate sequences* (see [1] for definitions). Also, exploiting this multivariate representation and using techniques of wreath products of [1] we describe how to lift an arbitrary m-variate permutation with a single cycle of n-bit words to a permutation with a single cycle of $(n + K)$-bit words, and how to construct counter-dependent generators based on these multivariate mappings.

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

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

2. Multivariate ergodic mappings

Consider a bijection $B(x^0,\dots,x^{m-1})=X$ of the m^{th} Cartesian power $(\mathbb{Z}_2)^{(m)}$ of the space $\mathbb{Z}_2$ of 2-adic integers onto the space $\mathbb{Z}_2$ given by $\delta_k(X)\equiv\delta_\ell(x^r) \pmod 2$, where $r\in\{0,1,\dots,m-1\}$ is the least non-negative residue of $k\in\{0,1,2,\dots\}$ modulo m, $k=\ell\cdot m+r$, $X\in\mathbb{Z}_2$, $(x^0,\dots,x^{m-1})\in(\mathbb{Z}_2)^{(m)}$, $\delta_j(u)$ is the j^{th} bit of a canonical 2-adic representation of $u\in\mathbb{Z}_2$. [1] Consider a compatible mapping $H\colon\mathbb{Z}_2\to\mathbb{Z}_2$ and a conjugate mapping

$$H^B(x^0,\dots,x^{m-1})=(h^0(x^0,\dots,x^{m-1}),\dots,h^{m-1}(x^0,\dots,x^{m-1}))$$

of $(\mathbb{Z}_2)^{(m)}$ to $(\mathbb{Z}_2)^{(m)}$; that is, $H^B(x^0,\dots,x^{m-1})=B^{-1}(H(B(x^0,\dots,x^{m-1})))$. Obviously, the conjugate mapping H^B is compatible and ergodic whenever the mapping H is ergodic. For instance, let $H(X)=1+X$, then

$$\delta_j(H(X))\equiv\delta_j(X)+\prod_{s=0}^{j-1}\delta_s(X)\pmod 2$$

(we assume the product over the empty set is 1); then the conjugate m-variate mapping is given by

$$h^k(x^0,\dots,x^{m-1})=x^k\oplus\left(\left(\bigwedge_{s=0}^{k-1}x^s\right)\wedge\left(\bigwedge_{r=0}^{m-1}((x^r+1)\oplus x^r)\right)\right)=$$
$$x^k\oplus\left(\left(\bigwedge_{s=0}^{k-1}x^s\right)\wedge\left(\left(\left(\bigwedge_{r=0}^{m-1}x^r\right)+1\right)\oplus\left(\bigwedge_{r=0}^{m-1}x^r\right)\right)\right)$$

for $k=0,1,2,\dots,m-1$. Here, we recall, $\wedge$ (or AND) is a bitwise conjunction[2], $\oplus$ (or XOR) is a bitwise addition modulo 2 (we assume that a bitwise conjunction $\wedge$ over the empty set is -1, i.e., the string of all 1's). One could construct various multivariate compatible ergodic mappings combining this representation with the ergodicity criterion. We recall the latter:

2.1. **Theorem.** (see [1, Theorem 3.13]) *A mapping $T\colon\mathbb{Z}_2\to\mathbb{Z}_2$ is compatible and measure preserving[3] iff for each $i=0,1,\dots$ the Boolean function $\tau_i^T=\delta_i(T)$ in Boolean variables $\chi_0,\dots,\chi_i$ could be represented as Boolean polynomial of the form*

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

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 $(\varepsilon_0,\dots,\varepsilon_{i-1})$, where $\varepsilon_j\in\{0,1\}$ for $j=0,1,\dots,i-1$. The latter takes place if and only if $\varphi_0^T=1$, and the degree of the Boolean polynomial φ_i^T for $i\geq 1$ is exactly i, that is, φ_i^T contains a monomial $\chi_0\cdots\chi_{i-1}$.

For instance, theorem 2.1 implies that an arbitrary univariate compatible and ergodic mapping T gives rise to the m-variate compatible and ergodic mapping

[1] Loosely speaking, we may think of an element of a Cartesian power $(\mathbb{Z}_2)^{(m)}$ as of a table of m infinite binary rows, to which we put into the correspondence an infinite binary string (that is, an element of $\mathbb{Z}_2$) obtained by reading succesively bits of each column, from top to bottom.

[2] i.e., a bitwise multiplication modulo 2

[3] That is, T induces a permutation on $\mathbb{Z}/2^n$ for all $n=1,2,3,\dots$

$T^B = (t^0, \dots, t^{m-1})$ of the form

$$t^k(x^0, \dots, x^{m-1}) = x^k \oplus \left(\left(\bigwedge_{s=0}^{k-1} x^s \right) \wedge \left(\bigwedge_{r=0}^{m-1} ((x^r + 1) \oplus x^r) \right) \right) \oplus u^k(x^0, \dots, x^{m-1}),$$

where

$$\sum_{(x^0,\dots,x^{m-1})=(0,\dots,0)}^{(2^r-1,\dots,2^r-1)} \delta_r(u^k(x^0, \dots, x^{m-1})) \equiv 0 \pmod 2 \tag{2.1.1}$$

for all $r = 0, 1, 2, \dots$.[4] With the use of these considerations we deduce from theorem 2.1 the following

2.2. **Proposition.** *Let $f_s^j \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ $(s \in \{0, 1, \dots, m-1\},\ j = 0, 1, \dots, m-1)$ be (univariate) ergodic functions, let $g_s^j \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ $(s \in \{0, 1, \dots, j-1\}\ ,\ j = 1, 2, \dots, m-1)$ be (univariate) measure-preserving functions. Then the mapping*

$$H^B(x^0, \dots, x^{m-1}) = (h^0(x^0, \dots, x^{m-1}), \dots, h^{m-1}(x^0, \dots, x^{m-1}))$$

of $(\mathbb{Z}_2)^{(m)}$ onto $(\mathbb{Z}_2)^{(m)}$ such that

$$h^0(x^0, \dots, x^{m-1}) = x^0 \oplus \left(\bigwedge_{r=0}^{m-1} (f_r^0(x^r) \oplus x^r) \right);$$

$$h^1(x^0, \dots, x^{m-1}) = x^1 \oplus \left(g_0^1(x^0) \wedge \left(\bigwedge_{r=0}^{m-1} (f_r^1(x^r) \oplus x^r) \right) \right);$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$h^{m-1}(x^0, \dots, x^{m-1}) = x^{m-1} \oplus \left(\left(\bigwedge_{s=0}^{m-2} g_s^{m-1}(x^s) \right) \wedge \left(\bigwedge_{r=0}^{m-1} (f_r^{m-1}(x^r) \oplus x^r) \right) \right)$$

is ergodic. That is, for all $n = 1, 2, \dots$ the mapping H induces modulo 2^n a permutation with a single cycle; hence the length of this cycle is 2^{mn}.

Proof. It sufficies to demonstrate that the conjugate mapping $H \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatible and ergodic. Denote $\chi_k^r = \delta_k(x^r)$; we have to represent $\delta_t(h^s(x^0, \dots, x^{m-1}))$ as a Boolean polynomial in Boolean variables χ_k^r. For $c \in \{0, 1, \dots, m-1\}$ let

$$F^c = \bigwedge_{r=0}^{m-1} (f_r^c(x^r) \oplus x^r); \qquad G^c = \bigwedge_{s=0}^{c-1} g_s^c(x^s), \quad (c > 0); \qquad G^0 = -1.$$

Now, since the functions g_s^j and f_s^j are compatible and, respectively, measure preserving/ergodic, in view of 2.1 one obtains the following representation of $\delta_k(g_s^j)$ and $\delta_k(f_s^j)$ as Boolean polynomials:

$$\delta_k(g_s^j(x^s)) = \chi_k^s + \varphi_k^j(\chi_0^s, \dots, \chi_{k-1}^s);$$

$$\delta_0(f_s^j(x^s)) = \chi_0^s + 1;$$

$$\delta_k(f_s^j(x^s)) = \chi_k^s + \chi_0^s \cdots \chi_{k-1}^s + \psi_k^j(\chi_0^s, \dots, \chi_{k-1}^s) \quad (k > 0);$$

[4] such mappings u^k are called *even parameters* in [7]

where $\deg \psi_k^j(\chi_0^s,\dots,\chi_{k-1}^s) < k$. Further, since

$$\delta_k(G^c \wedge F^c) \equiv \prod_{s=0}^{c-1} \delta_k(g_s^c(x^s)) \cdot \prod_{s=0}^{m-1} (\delta_k(f_s^c(x^s)) + \delta_k(x^s)) \pmod 2,$$

the above equations imply that

$$\delta_0(G^0 \wedge F^0) = 1;$$
$$\delta_0(G^c \wedge F^c) = \chi_0^0 \cdots \chi_0^{c-1} + \Phi_0^c, \quad (c>0);$$
$$\delta_k(G^0 \wedge F^0) = \chi_0^0 \cdots \chi_{k-1}^0 \cdots \chi_0^{m-1} \cdots \chi_{k-1}^{m-1} + \Phi_k^0, \quad (k>0);$$
$$\delta_k(G^c \wedge F^c) = \chi_k^0 \cdots \chi_k^{c-1} \cdot \chi_0^0 \cdots \chi_{k-1}^0 \cdots \chi_0^{m-1} \cdots \chi_{k-1}^{m-1} + \Phi_k^c, \quad (c>0, k>0).$$

where Φ_k^c (respectively, Φ_k^0 or Φ_0^c) is a Boolean polynomial in Boolean variables

$$\chi_k^0,\dots,\chi_k^{c-1},\chi_0^0,\dots,\chi_{k-1}^0,\dots,\chi_0^{m-1},\dots,\chi_{k-1}^{m-1}$$

(respectively, in $\chi_0^0,\dots,\chi_{k-1}^0,\dots,\chi_0^{m-1},\dots,\chi_{k-1}^{m-1}$ or $\chi_0^0,\dots,\chi_0^{c-1}$), and $\deg \Phi_k^c < mk+c$. Finally, $\delta_k(h^c(x^0,\dots,x^{m-1})) = \chi_k^c + \delta_k(G_k^c \wedge F_k^c)$, and the result follows in view of 2.1. □

2.3. *Note.* Of course, the assertion of the proposition remains true for the mappings $\hat{h}^s = h^s \oplus u^s$, $(s = 0,1,\dots,m-1)$, where u^s is an arbitrary mapping that satisfies (2.1.1), since these mappings u^s add summands of degree $< mk+s$ to each Boolean polynomial $\delta_k(h^s(x^0,\dots,x^{m-1}))$, see the proof of 2.2.

With this note we can deduce some consequences of proposition 2.2.

2.4. **Corollary.** [7, Theorem 6 and Lemma 1] *The m-variate mapping defined by*

$$h^s(x^0,\dots,x^{m-1}) = x^s \oplus ((h(x^0 \wedge \cdots \wedge x^{m-1}) \oplus (x^0 \wedge \cdots \wedge x^{m-1})) \wedge x^0 \wedge \cdots \wedge x^{s-1}),$$

$s = 0,1,\dots,m-1$, *is compatible and ergodic whenever h is a univarite compatible and ergodic function.*

Proof. Just note that both $\delta_k\big(\bigwedge_{t=0}^{m-1}(h(x^t)\oplus x^t)\big)$ and $\delta_k\big(h\big(\bigwedge_{t=0}^{m-1} x^t\big)\oplus\big(\bigwedge_{t=0}^{m-1} x^t\big)\big)$ are Boolean polynomials of the same degree $mk+s$. □

2.5. **Corollary.** *For $m>1$ under conditions of 2.2 the following m-variate mapping*

$$h^t(x^0,\dots,x^{m-1}) = x^t + \left(\left(\bigwedge_{s=0}^{t-1} g_s^t(x^s)\right) \wedge \left(\bigwedge_{r=0}^{m-1} (f_r^t(x^r) \oplus x^r)\right)\right),$$

$t = 0,1,\dots,m-1$, *is compatible and ergodic.*

Proof. Integer addition + adds carry from the $(mk+c)^{\text{th}}$ bit to $(m(k+1)+c)^{\text{th}}$ bit of the coniugate mapping $H : \mathbb{Z}_2 \to \mathbb{Z}_2$; the carry is a Boolean polynomial in variables

$$\chi_k^c, \chi_k^0,\dots,\chi_k^{c-1},\chi_0^0,\dots,\chi_{k-1}^0,\dots,\chi_0^{m-1},\dots,\chi_{k-1}^{m-1},$$

hence, integer addition just adds a Boolean polynomial in $km+c+1$ variables to the Boolean polynomial $\delta_{k+1}(h^c(x^0,\dots,x^{m-1})$ in $(k+1)m+c$ variables. So this extra summand is of degree at most $km+c+1 < (k+1)m+c$, see the proof of proposition 2.2. □

2.6. *Note.* Again, the corollary remains true for the mapping $\hat{h}^s = h^s + u^s$, $(s = 0,1,\dots,m-1)$, where u^s is an arbitrary mapping that satisfies (2.1.1).

We recall that according to [1, Proposition 3.10], a compatible univariate function $g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ (resp., $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$) preserves measure (resp., is ergodic) iff it could be represented as $g(x) = d+x+2\cdot v(x)$ (respectively as $f(x) = 1+x+2\cdot(v(x+1)-v(x))$) for suitable $d \in \mathbb{Z}_2$ and compatible $v\colon \mathbb{Z}_2 \to \mathbb{Z}_2$. In other words, one can assume v to be an arbitrary (e.g., key-dependent) composition of arithmetic operations (such as addition, multiplication, subtraction, etc.) and bitwise logical operations (such as XOR, AND, OR, etc.); see [1] for details. Thus, to obtain a cycle of length, say, 2^{256} applying the above results, one could use 8-variate mappings and work with 32-bit words, which are standard for most contemporary computers.

We note, however, that similarly to a univariate case, only senior bits of output sequence achieve maximum period length: To be more exact, if x_i^j is the value of the j^{th} variable at the i^{th} step, $(x_{i+1}^0, \ldots, x_{i+1}^{m-1}) = H^B(x_i^0, \ldots, x_i^{m-1})$, then the period length of the bit sequence $\{\delta_s(x_i^j)\colon i = 0, 1, 2, \ldots\}$ is 2^{ms+j+1}, for $s \in \{0, 1, \ldots\}$, $j \in \{0, 1, \ldots, m-1\}$. This could be improved by the use of multivariate output functions in a manner of [1, Proposition 4.13], namely:

2.7. **Proposition.** *Let H^B andF^B be m-variate ergodic mappings that satisfy conditions of proposition 2.2, and let $\pi\colon \mathbb{Z}/n \to \mathbb{Z}/n$ be an arbitrary permutation of bits of n-bit word $z \in \mathbb{Z}/2^n$ such that $\delta_0(\pi(z)) = \delta_{n-1}(z)$* (e.g., π could be a bit order reversing permutation, or a 1-bit cyclic shift towards senior bits). *Consider a recurrence sequence $\mathcal{Y} = \{\mathbf{y}_i\colon i = 0, 1, 2\ldots\}$ over $(\mathbb{Z}/2^n)^{(m)}$ defined by the laws*

$$\mathbf{x}_{i+1} = H^B(\mathbf{x}_i) \bmod 2^n; \quad \mathbf{y}_i = F^B(\pi(x_i^{m-1}), x_i^0, \ldots, x_i^{m-2}) \bmod 2^n,$$

where $\mathbf{x}_j = (x_j^0, \ldots, x_j^{m-1}), \mathbf{y}_j = (y_j^0, \ldots, y_j^{m-1}) \in (\mathbb{Z}/2^n)^{(m)}$. Then the output sequence $\mathcal{Y}$ is purely periodic, its period length is exactly 2^{nm}, each element of $(\mathbb{Z}/2^n)^{(m)}$ occurs at the period exactly once, and the period length of each coordinate sequence $\delta_k(\mathcal{Y}^s) = \{\delta_k(y_i^s)\colon i = 0, 1, 2, \ldots\}$ is exactly 2^{nm}. [5]

Proof. Immediately follows by application of [1, Proposition 4.13] to (univariate) conjugate mappings H and F; we just note that Proposition 4.13 of [1], as it easily follows from its proof, holds for arbitrary permutation π that satisfies conditions of our proposition 2.7. □

2.8. *Note.* As it follows from the proof of [1, Proposition 4.13], to provide maximum period length of all coordinate sequences of output sequence it is sufficient only to apply output function in such a way, that the most significant bit of a state transition function substitutes for the least significant bit of argument of the output function. Thus, the proposition 2.7 remains true if one permutes variables $x^0, \ldots, x^{m-2}$ of the function F^B in arbitrary order, or permutes bits in these varibles, or apply arbitrary bijections to these variables, etc.

It turnes out that with the use of techniques of wreath products of [1] it is possible to "lift" an arbitrary permutation on $(\mathbb{Z}/2^n)^{(m)}$ with a single cycle to $(\mathbb{Z}_2)^{(m)}$, i.e. to obtain "really multivariate" permutations with a single cycle (in a somewhat "univariate manner", of course). Recall the following theorem, which is a generalization of theorem 2.1:

[5] Recall that according to [1] the term "exactly" within this context means that the purely periodic binary sequence $\delta_k(\mathcal{Y}^s)$ has no periods of lengths less than 2^{nm}.

2.9. **Theorem.** ([1, 4.3 and 4.4; or 4.10]) *Let $T\colon \mathbb{Z}/2^M \to \mathbb{Z}/2^M$, $M \geq 1$, be an arbitrary permutation with a single cycle, and let the mappings $H_z(\cdot)\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, $(z \in \mathbb{Z}/2^M)$ satisfy the following conditions:*

(1) *$\delta_i(H_z(x)) \equiv \delta_i(x) + \rho_i(z;x) \pmod 2$ $(i = 0, 1, 2\ldots)$, where ρ_i are Boolean functions in Boolean variables $\delta_r(z)$, $\delta_s(x)$ $(r \in \{0, 1, \ldots, M-1\}$, $s \in \{0, 1, \ldots, i-1\})$, and $\rho_0(z;x) = \rho_0(z)$ does not depend on x;*

(2) *$\sum_{z=0}^{2^M-1} \rho_0(z) \equiv 1 \pmod 2$;*

(3) *$\sum_{z=0}^{2^M-1} \sum_{x=0}^{2^i-1} \rho_i(z;x) \equiv 1 \pmod 2$, $i = 1, 2, \ldots$*

Then the mapping

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

is transitive modulo 2^k (that is, induces a permutation with a single cycle on the residue ring $\mathbb{Z}/2^k$ modulo 2^k) *for all $k \geq M$.*

From here we deduce the following

2.10. **Proposition.** *Let $T\colon (\mathbb{Z}/2^n)^{(m)} \to (\mathbb{Z}/2^n)^{(m)}$ be an arbitrary* (not necessarily compatible) *m-variate mapping with a single cycle, let $H^B\colon (\mathbb{Z}_2)^{(m)} \to (\mathbb{Z}_2)^{(m)}$ be any m-variate compatible ergodic mapping mentioned above* (see 2.2, 2.3, 2.4, 2.5, 2.6). *Then the m-variate mapping $W^B(\mathbf{x}) = T(\mathbf{x} \bmod 2^n) + (H^B(\mathbf{x}) \wedge ((-2^n)^{(m)}))$ of $(\mathbb{Z}_2)^{(m)}$ onto $(\mathbb{Z}_2)^{(m)}$ induces a permutation with a single cycle modulo 2^N for all $N \geq n$.*

Recall that a 2-adic representation of -2^n is an infinite binary string such that first n bits of it are 0, and the rest are 1. In other words, $H^B(\mathbf{x}) \wedge ((-2^n)^{(m)})$ takes $\mathbf{x} = (x^0, \ldots, x^{m-1})$ to $(h^0(\mathbf{x}) \wedge (-2^n), \ldots, h^{m-1}(\mathbf{x}) \wedge (-2^n))$, thus sending to 0 the first n low order bits, whereas $\mathbf{x} \bmod 2^n = (x^0 \bmod 2^n, \ldots, x^{m-1} \bmod 2^n)$ sends to 0 all senior order bits, starting with the n^{th} bit (we start enumerate bits with 0).

Proof of proposition 2.10. The conjugate mapping W satisfies 2.9 for $M = nm$ since all Boolean polynomials $\delta_j(h^s(\mathbf{x}))$ are of odd weight, see the proof of 2.2. □

Concluding the section we just note that it is clear now how to construct counter-dependent generators with the use of the above multivariate ergodic mappings. Take, for instance, $M > 1$ odd, and take a finite sequence[6]

$$\{\mathbf{c}_j = (c_j^0, \ldots, c_j^{M-1})\colon j = 0, 1, \ldots, M-1\}$$

of m-dimensional vectors over $\mathbb{Z}/2^n$ such that the sequence of its first coordinates satisfy conditions of proposition 4.3 of [1]; that is, $\sum_{j=0}^{M-1} c_j^0 \equiv 0 \pmod 2$, and the sequence $\{c^0_{j \bmod M} \bmod 2\colon j = 0, 1, \ldots\}$ is purely periodic of period length exactly M. Then take arbitrary m-variate ergodic mappings H_j^B and F_j^B, $j = 0, 1, \ldots, M-1$ described above and consider recurrence sequences defined by the laws

$$\begin{aligned} \mathbf{x}_{i+1} &= (\mathbf{c}_{i \bmod M} \oplus H^B_{i \bmod M}(\mathbf{x}_i)) \bmod 2^n; \\ \mathbf{y}_i &= (\mathbf{F}^B_{i \bmod M}(\pi(x_i^{m-1}), x_i^0, \ldots, x_i^{m-2})) \bmod 2^n, \end{aligned}$$

for $i = 0, 1, 2, \ldots$, where π satisfies conditions of 2.7. Then the sequence of internal states $\{\mathbf{x}_i\}$ is purely periodic of period length exactly $M \cdot 2^{nm}$, and each

[6] which may be stored in memory, or may be generated on the fly while implementing the corresponding generator

m-dimensional vector over $\mathbb{Z}/2^n$ occurs at the period exactly M times. The output sequence $\mathcal{Y} = \{\mathbf{y}_i\}$ is also purely periodic of period length exactly $M \cdot 2^{nm}$, and each m-dimensional vector over $\mathbb{Z}/2^n$ occurs at the period exactly M times; moreover, the period length of each coordinate sequence $\delta_k(\mathcal{Y}^s) = \{\delta_k(y_i^s)\colon i = 0, 1, 2, \ldots\}$ is a multiple of 2^{nm}, which is not less than 2^{nm} and does not exceed $M \cdot 2^{nm}$. This conclusion follows immediately by application of [1, Propositions 4.6 and 4.13] to conjugate mappings H_j and F_j. The other counter-dependent generators (for $M = 2^k$ or arbitrary M) based on [1, 4.3, 4.4, 4.6 and 4.10] could be constructed by the analogy.

3. Skew shifts and wreath products: a discussion

The aim of this section is to make more transparent the core mapping underlying the constructions introduced in [1], [2], [3], [4], [8], [9], [7], as well as [5] and even [6]. This mapping is wreath product[7] of permutations; wreath product of permutations is a special case of a skew product transformation[8]. We recall the most abstract definiton:

3.1. **Definition.** Given two non-empty sets X, Y, a mapping $h\colon X \to X$, and a mapping $H\colon X \to Y^Y$, where Y^Y [9] is a set of all mappings of Y into Y. Denote the action of H as $(H(x))(y) = H_x(y)$ for $x \in X, y \in Y$. Then the *skew product transformation* $H \wr h$ is a mapping of a direct product $X \times Y$ into itself such that $(H \wr h)(x, y) = (h(x), H_x(y))$.

It is obvious that if h is a bijection and all H_x, $x \in X$ are bijections, then $H \wr h$ is a bijection. For instance, if $\star$ is a quasigroup operation on Y [10], $F\colon X \to Y$ is an arbitrary mapping and $H_x(y) = y \star F(x)$, then $H \wr h$ is bijective whenever h is bijective. A classical example in ergodic theory is skew shift on torus, which takes $(x, y) \in (\mathbb{T})^{(2)}$ to $(x \boxplus \gamma, y \boxplus \alpha(x))$, where $(\mathbb{T})^{(2)}$ is a 2-dimensional torus (i.e., a Cartesian product of a real interval $[0, 1]$ onto itself); $\gamma, \alpha(x) \in [0, 1]$, and $\boxplus$ is addition modulo 1 of reals of $[0, 1]$.

Another example of imporance to cryptography is an i^{th} round permutation $R_i(k)$ of a Feistel network: This permutation takes $(x, y) \in (\mathbb{Z}/2^n)^{(2)}$ to $(y \oplus f_i(k, x), x)$ (with k being a key). Obviously, $R_i(k)$ is a composition of a skew shift $(x, y) \mapsto (x, y \oplus f_i(k, x))$ and a permutation $\tau(x, y) = (y, x)$, which merely changes positions of two concatented n-bit subwords in a $2n$-bit word. By the way, we used a construction somewhat resembling this permutation $R_i(k)$ in 2.7: In fact, from 2.1 it is clear that a compatible mapping (or a T-function, in terminology of [8]) of $\mathbb{Z}/2^N$ into $\mathbb{Z}/2^N$ is a composition of N skew product transformations of $\mathbb{Z}/2$, and that a measure preserving mapping (or invertible T-function) is a skew shift on N-dimensional discrete torus $(\mathbb{Z}/2)^{(N)}$. The skew products seems to become popular in cryptography: Boaz Tsaban noted that a construction of a counter-dependent generator of [11] is just an ergodic-theoretic skew-product of a counter (or any automata) with the given automata. In particular, if the counter is replaced by any ergodic transformation, then the resulting cipher will be ergodic, [12]. All these observations lead to a suggestion that there are tight connections between ergodic

[7] this notion is more common for group theory

[8] the latter notion is well known in dynamical systems and ergodic theory

[9] i.e., a Cartesian power of Y

[10] that is, for all $a, b \in Y$ both equations $y \star a = b$ and $a \star y = b$ have unique solutions in y

theory and cryptography. In fact, in this pper we use the notions of ergodicity and measure preservation just because the corresponding mappings are ergodic or measure-preserving in exact sence of ergodic theory.

Of course, the most intriguing is a question, which naturally arises in this connection, whether an ergodic theory could give something to prove (or to give strong evidence of) cryptographic security of a corresponding schemes. Might be, it is too early to put such a question now, yet note that one of one-way candidates, namely, DES with a fixed message, is a composition of skew shifts with a permutation τ. Note that in a corresponding construction [10] DES is assumed to be a family of pseudorandom functions. In [1] we conjectured that a mapping $F\colon \mathbb{Z}/2^n \to \mathbb{Z}/2^k$ defined by k randomly and independently choosen Boolean polynomials (with polynomially restricted number of monomials) in n variables is a one-way function, and gave some evidence that among the generators we studied there may exist ones that are provably strong against a known plaintext attack. A stronger assumption that F is a pseudorandom function[11](how plausible this asumption is?) may lead to a proof that a corresponding generator is pseudorandom. For instance, forming of output sequence $\{y_i\}$ (see [1, Section 6] for notations) a sequence $y_0, y_0 \oplus y_1, \dots, y_{m-2} \oplus y_{m-1}, \dots$ with probability $1-\epsilon$ one obtains that[12]

$$y_0 = F(z), y_0 \oplus y_1 = F(z+1), \dots, y_{m-2} \oplus y_{m-1} = F(z+m-1), \dots$$

Yet under assumptions that are made, this sequence, as well as the output sequence must be pseudorandom.

More "ergodic-theoretic common features" could be seen while analysing proofs of corresponding reslts. The mappings defined by compositions of arithmetic and bitwise logical operations turnes out to be continuous on $\mathbb{Z}_2$, and moreover, rather close to uniformly differentiable mappings, see [3], [2], [1], [4]. To study certain important cryptographic properties of these mapping we approximate them (with respect to a 2-adic distance) by uniformly differentiable functions; we have to calculate derivatives of these functions to check whether a given mapping is a permutation, or whether it is equiprobable. On the other hand, to study similar questions for other algebraic systems, e.g., discrete groups, we have also to study derivatives, namely, Fox derivatives of mappings of groups, see [6], [5] for details. Thus, we have to use "continuous" techniques to study "discrete" problems. We could continue such observations. At our view, all this is more than a mere analogy between ergodic-theoretic and cryptographical constructions.

References

[1] V. Anashin, *Pseudorandom Number Generation by p-adic Ergodic Transformations*, 2004. A preprint available from http://arXiv.org/abs/cs.CR/0401030 1, 2, 5, 6, 7, 8

[11]to be more exact, assuming that it is possible to construct with these mappings F a family of pseudorandom functions; the corresponding construction, which is under study now, is based on skew shifts

[12]we are using an opportunity here to fix a misprint in [1]

[2] 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 7, 8

[3] 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.) 7, 8

[4] 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. 7, 8

[5] V. S. Anashin *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. 7, 8

[6] V. S. Anashin, *Solvable groups with operators and commutative rings admitting transitive polynomials*, Algebra and Logic **21**(1982), 627–646 7, 8

[7] A. Klimov and A. Shamir, *New Cryptographic Primitives Based on Multiword T-functions*, 2004, (to appear). 1, 3, 4, 7

[8] 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. 7

[9] A. Klimov, A. Shamir. 'Cryptographic applications of T-functions', in: *Selected Areas in Cryptography -2003* 7

[10] M. Luby, C. Rackoff. *A study of password sequrity*, In: Proc. Crypto'87, LNCS **293**, Springer-Verlag, 1998., pp. 392–397 8

[11] A. Shamir, B. Tsaban. *Guaranteeing the diversity of number generators*, Information and Computation **171** (2001), 350–363. Available from http: //arXiv.org/ abs/ cs.CR/ 0112014 7

[12] B. Tsaban, private communication. 7

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