LINEAR RELATION ON GENERAL ERGODIC T-FUNCTION

TAO SHI, VLADIMIR ANASHIN, AND DONGDAI LIN

ABSTRACT. We find linear (as well as quadratic) relations in a very large class of T-functions. The relations may be used in analysis of T-function-based stream ciphers.

1. INTRODUCTION

For years linear feedback shift registers (LFSRs) over a 2-element field $\mathbb{F}_2$ have been one of the most important building blocks in keystream generators of stream ciphers. LFSRs can easily be designed to produce binary sequences of the longest period (that is, of length $2^k - 1$ for a k-cell LFSR over $\mathbb{F}_2$); LFSRs are fast and easy to implement in hardware. However, sequences produced by LFSRs have linear dependencies that make easy to analyse the sequences to construct attacks on the whole cipher. To make output sequences of LFSRs more secure these linear dependencies must be destroyed by a properly chosen filter; this is the filter that carries the major cryptographical load making the whole cipher secure.

Recently, T-functions were found to be useful tools to design fast cryptographic primitives and ciphers based on usage on both arithmetic (addition, multiplication) and logical operations, see [39, 14, 15, 17, 16, 18, 21, 20, 19, 24, 29, 8, 32, 34, 26]. Loosely speaking, a T-function is a map of k-bit words into k-bit words such that each i-th bit of image depends only on low-order bit $0, ..., i$ of the pre-image. Various methods are known to construct transitive T-functions (the ones that produce sequences of the longest possible period, 2^k), see [3, 4, 6, 7, 5, 2, 1, 24, 25, 17, 16, 18, 20, 14]. Transitive T-functions have been considered as a candidate to replace LFSRs in keystream generators of stream ciphers, see e.g. [8, 39, 15, 19, 29, 32] since sequences produced by T-function-based keystream generators are proved to have a number of good cryptographic properties, e.g., high linear and 2-adic complexity, uniform distribution of subwords, etc., see [3, 23, 1, 41]. However, any word sequence produced by a transitive T-function has a well-known deficiency: the less significant is the position n of the bit in the word, the shorter is the period of the corresponding bit sequence in the output word sequence of words. To be more exact, given a transitive T-function f, consider a k-bit word sequence $x_0, x_1, \ldots$ produced by f with respect to the recurrence law

$$x_i = f(x_{i-1}) = f^i(x_0) = \underbrace{f(\ldots(f(x_0)\ldots)}_{i}, \qquad i = 0, 1, 2, \ldots,$$

(by the definition, $f^0(x_0) = x_0$); denote $\delta_n(x_i)$ the n-th bit of the word x_i, $n = 0, 1, \ldots, k-1$; then the length of the shortest period of the bit sequence $\delta_n(x_0), \delta_n(x_1), \ldots$ (the n-th coordinate sequence) is 2^{n+1}. That is, only the highest order coordinate sequence $\delta_{k-1}(x_0), \delta_{k-1}(x_1), \ldots$ reaches the longest period, of length 2^k. That is why the low-order coordinate sequences are newer used to form a keystream, there either are just deleted or serve to control other parts of the cipher.

Moreover, the second half of the period of the coordinate sequence is just the inverse of its first half:

(1.1) $$\delta_n(x_{i+2^n}) \equiv \delta_n(x_i) + 1 \pmod{2}, \text{ for all } i, n = 0, 1, 2, \ldots$$

Fortunately, the latter property does not cause big problems: speaking loosely, given arbitrary transitive T-function f, the half-periods $\delta_n(x_0), \ldots \delta_n(x_{2^n-1})$ should be considered as random and adjacent coordinate sequences $\delta_{n-1}(x_0), \delta_{n-1}(x_1), \ldots$ and $\delta_n(x_0), \delta_n(x_1), \ldots$ as independent (see Theorem 4 for exact statements).

However, it was discovered that for *certain* T-functions the said independence of adjacent coordinate sequences does not take place: these sequences satisfy linear relation of the form

(1.2) $$\delta_n(x_{i+2^{n-1}}) \equiv \delta_n(x_i) + \delta_{n-1}(x_i) + z_i \pmod{2}, \text{ for all } i = 0, 1, 2, \ldots,$$

where the length of the period of the sequence z_i is only 4 (and *not* 2^n as in a general case, for arbitrary transitive T-function). Namely, Molland and Helleseth in [30, 31] proved this for a transitive T-function $f(x) = x + (x^2 \vee C)$ suggested by Klimov and Shamir in [17]; Jin-Song Wang and Wen-Feng Qi in [38] obtained similar result for a transitive polynomial function $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$ with integer coefficients $c_0, c_1, \ldots \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Our contribution. It is fourfold:

- First we prove that relations of type (1.2) hold for a much wider class of T-functions than polynomials over $\mathbb{Z}$ and Klimov-Shamir functions $f(x) = x + (x^2 \vee C)$, $C \in \mathbb{Z}$. This wider class contains exponential T-functions (like $f(x) = 3x + 3^x$, fractional T-functions (like $f(x) = 1 + x + \frac{4}{1+2x}$) and many other T-functions that might be extremely complex compositions of numerical and logical operators, like the following one:

$$(1.3) \qquad f(x) = \frac{x}{3} + \left(\frac{1}{3}\right)^x + 4 \cdot \left(1 - 2 \cdot \frac{\neg(x \wedge x^2 + x^3 \vee x^4)}{3 - 4 \cdot (5 + 6x^5)^{x^6 \oplus x^7}}\right)^{7 + \left(\frac{8x^8}{9+10x^9}\right)}.$$

  In Theorem 5 below we prove that for the mentioned class of T-functions (which is precisely defined further) relation (1.2) holds; the length of the period of the binary sequence z_i in the relation depends on the function f and is not necessarily 4 any longer; however, it is still short.

- Second, for a slightly narrower class of T-functions than the previous one, we prove that a *quadratic relation holds for any three consecutive coordinate sequences*, see Theorem 6 further. Earlier a relation of this sort was known only for Klimov-Shamir T-function, see paper [27] by Yong-Long Luo and Wen-Feng Qui.

- Third, we show that both linear and quadratic relations of this sort hold not only for univariate T-functions, but *also for multi-word T-functions and even for cascaded compositions of T-functions with other generators.*

- Finally we demonstrate how using the mentioned relations between coordinate sequences one can recover the rest coordinate sequences of lower orders *even if a T-function from the mentioned class has not been specified.* That is, for instance, if f is a polynomial with integer coefficients, there is needless to know its coefficients to recover low-order coordinate sequences $(\delta_{n-2}(x_i)), (\delta_{n-3}(x_i)), \ldots$, given only a pair of coordinate sequences $(\delta_n(x_i))$ and $(\delta_{n-1}(x_i))$. This is an important conclusion since in some stream ciphers (see e.g., [8, 9]) coefficients of a T-function are formed during a 'warming-up' stage; i.e., the coefficients are obtained from a key and an initial vector by a special complicated procedure and thus are not known to a cryptanalyst.

The paper serves a sort of a warning to a designer of a T-function-based stream cipher to avoid possible flaws: both the choice of T-function and the way it is used must guarantee that either there are no relations of this sort among coordinate sequences or they are hidden deep enough (e.g., by a proper filter) to prevent using them by a cryptanalyst. Even truncation of low-order bits may not be a remedy!

Last, but not least: we obtain our results by using techniques of 2-adic analysis; that is, we we expand T-functions on the whole space $\mathbb{Z}_2$ of 2-adic integers and study the corresponding dynamics. That is why we need to introduce some notions and results from 2-adic analysis (and the 2-adic ergodic theory) before stating our results. It worth noting here that the approach based on 2-adic dynamics (and wider, on p-adic dynamics and on algebraic dynamics) recently proved its effectiveness in various cryptographic applications, see corresponding monograph [3] for further details.

The paper is organized as follows:

- Section 2 concerns basics of the non-Archimedean theory for T-functions;
- Section 3 states our main two results (see Appendix **??** for proofs);
- Section 4 discusses applications to T-function-based stream ciphers;
- we conclude in Section 5.

2. The 2-adic theory of T-functions: brief survey

In this section we introduce basics of what can be called a non-Archimedean approach to T-functions. We start with a definition of a T-function and show that T-functions can be treated as continuous functions defined on and valued in the space of 2-adic integers. Therefore we introduce basics of 2-adic arithmetic and of 2-adic Calculus that we will need to state and prove our main result. There are many comprehensive

monographs on p-adic numbers and p-adic analysis that contain all necessary definitions and proofs, see e.g. [22, 28, 36] or introductory chapters in [3]; so further in the section we introduce 2-adic numbers in a somewhat informal manner.

It worth noting here that the theory of T-functions (which actually are functions that satisfy a Lipschitz condition with a constant 1 w.r.t. 2-adic metric) was developed by mathematicians during decades prior to first publication of Klimov and Shamir on T-functions [17] in 2003, and in a much more general setting, for arbitrary prime p, and not only for $p = 2$. Moreover, various criteria of invertibility and single cycle property of T-functions were obtained within p-adic ergodic theory (see e.g. [7, 4]) nearly a decade prior to the first publication of Klimov and Shamir on T-functions [17]: Actually a T-function f is invertible if and only if it preserves Haar measure on 2-adic integers, and f has a single cycle property if and only if it is ergodic w.r.t. the Haar measure. Unfortunately, cryptographic community were not aware of that work done by mathematicians although in various papers there was directly pointed out that these functions might be useful to cryptography, see e.g. [4, 7, 5, 6]. To the moment, there exists a well developed mathematical discipline, the p-adic ergodic theory, a part of the non-Archimedean dynamics, and various crucial cryptographic properties of T-functions can be studied, properly understood and explained within this theory. Moreover, the theory has a well-developed tools to study cascaded compositions that include T-functions along with other standard cryptographic primitives (e.g., LFSRs): the compositions can be treated as wreath products of dynamical systems, and single cycle property of the composition is just ergodicity of the corresponding dynamical system, the wreath product. So the present paper serves an example of how effective are tools of the mentioned theory in a study of concrete cryptographical properties. For further reading on the theory as well as on its applications to cryptography (and to other sciences) readers are referred to monograph [3].

2.1. **T-functions.** An n-variate T-function is a mapping

$$(2.1) \qquad \left(\alpha_0^\downarrow, \alpha_1^\downarrow, \alpha_2^\downarrow, \ldots\right) \mapsto \left(\Phi_0^\downarrow\left(\alpha_0^\downarrow\right), \Phi_1^\downarrow\left(\alpha_0^\downarrow, \alpha_1^\downarrow\right), \Phi_2^\downarrow\left(\alpha_0^\downarrow, \alpha_1^\downarrow, \alpha_2^\downarrow\right), \ldots\right),$$

where $\alpha_i^\downarrow \in \mathbb{F}_2^n$ is a Boolean columnar n-dimensional vector over a 2-element field $\mathbb{F}_2 = \{0, 1\}$, and

$$\Phi_i^\downarrow \colon (\mathbb{F}_2^n)^{i+1} \to \mathbb{F}_2^m$$

maps $(i+1)$ Boolean columnar n-dimensional vectors $\alpha_0^\downarrow, \ldots, \alpha_i^\downarrow$ to m-dimensional columnar Boolean vector $\Phi_i^\downarrow\left(\alpha_0^\downarrow, \ldots, \alpha_i^\downarrow\right)$. Accordingly, a univariate T-function f is a mapping

$$(2.2) \qquad (\chi_0; \chi_1; \chi_2; \ldots) \overset{f}{\mapsto} (\psi_0(\chi_0); \psi_1(\chi_0, \chi_1); \psi_2(\chi_0, \chi_1, \chi_2); \ldots),$$

where $\chi_j \in \{0, 1\}$, and each $\psi_j(\chi_0, \ldots, \chi_j)$ is a Boolean function in Boolean variables $\chi_0, \ldots, \chi_j$. T-functions may be viewed as mappings from non-negative integers to non-negative integers: e.g., a univariate T-function f sends a number with the base-2 expansion

$$\chi_0 + \chi_1 \cdot 2 + \chi_2 \cdot 2^2 + \cdots$$

to the number with the base-2 expansion

$$\psi_0(\chi_0) + \psi_1(\chi_0, \chi_1) \cdot 2 + \psi_2(\chi_0, \chi_1, \chi_2) \cdot 2^2 + \cdots$$

Further in the paper we refer to these Boolean functions $\psi_0, \psi_1, \psi_2, \ldots$ as *coordinate functions* of a T-function f. If we restrict T-functions to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as *T-functions on k-bit words*: We usually associate the set of all k-bit words to the set $\{0, 1, \ldots, 2^k - 1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

The determinative property of T-functions (which might be used to state equivalent definition of a T-function) is *compatibility* with all congruences modulo powers of 2: Given a (univariate) T-function f,

$$(2.3) \qquad \text{if } a \equiv b \pmod{2^s} \text{ then } f(a) \equiv f(b) \pmod{2^s}.$$

Vice versa, every compatible map is a T-function.

Important examples of T-functions are basic machine instructions:

- integer arithmetic operations (addition, multiplication,...);
- bitwise logical operations ($\vee$, $\oplus$, $\wedge$, $\neg$);
- some their compositions (masking, shifts towards high order bits, reduction modulo 2^k).

Since obviously a composition of T-functions is a T-function (for instance, *any polynomial with integer coefficients is a T-function*), the T-functions are natural functions that can be evaluated by digital computers.

2.2. **2-adic numbers and 2-adic Calculus.** As it follows directly from the definition, any T-function is well-defined on the set $\mathbb{Z}_2$ of all infinite binary sequences $\ldots \delta_2(x)\delta_1(x)\delta_0(x) = x$, where $\delta_j(x) \in \{0,1\}$, $j = 0, 1, 2, \ldots$. Arithmetic operations (addition and multiplication) with these sequences could be defined via standard "school-textbook" algorithms of addition and multiplication of natural numbers represented by base-2 expansions. Each term of a sequence that corresponds to the sum (respectively, to the product) of two given sequences could 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. The ring $\mathbb{Z}_2$ is called the ring of 2-*adic integers*. The ring $\mathbb{Z}_2$ contains a subring $\mathbb{Z}$ of all rational integers: For instance, $\ldots 111 = -1$, since

$$
\begin{array}{r}
\ldots 1111 \\
+ \ \ldots 0001 \\
\hline
\ldots 0000
\end{array}
$$

Moreover, the ring $\mathbb{Z}_2$ contains all rational numbers that can be represented by irreducible fractions with odd denominators. For instance, the following calculations show that $\ldots 01010101 \times \ldots 00011 = \ldots 111$, i.e., that $\ldots 01010101 = -1/3$ since $\ldots 00011 = 3$ and $\ldots 111 = -1$:

$$
\begin{array}{r}
\times \ \ldots 010101 \\
\ldots 000011 \\
\hline
\ldots 010101 \\
+ \ \ldots 10101 \\
\hline
\ldots 111111
\end{array}
$$

Sequences with only finite number of 1s correspond to non-negative rational integers in their base-2 expansions, sequences with only finite number of 0s correspond to negative rational integers, while eventually periodic sequences (that is, sequences that become periodic starting with a certain place) correspond to rational numbers represented by irreducible fractions with odd denominators: For instance, $3 = \ldots 00011$, $-3 = \ldots 11101$, $1/3 = \ldots 10101011$, $-1/3 = \ldots 1010101$. So the j-th term $\delta_j(u)$ of the corresponding sequence $u \in \mathbb{Z}_2$ is merely the j-th digit of the base-2 expansion of u whenever u is a non-negative rational integer, $u \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$.

What is important, the ring $\mathbb{Z}_2$ is a metric space with respect to the metric (distance) $d_2(u, v)$ defined by the following rule: $d_2(u, v) = \|u - v\|_2 = 1/2^n$, 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 $d_2(3, 1/3) = 1/8$. The function $d_2(u, 0) = \|u\|_2$ is the *2-adic absolute value* of the 2-adic integer u, and $\mathrm{ord}_2\, u = -\log_2 \|u\|_2$ is the 2-adic valuation of u. Note that for $u \in \mathbb{N}_0$ the valuation $\mathrm{ord}_2\, u$ is merely the exponent of the highest power of 2 that divides u (thus, loosely speaking, $\mathrm{ord}_2\, 0 = \infty$, so $\|0\|_2 = 0$).

Now we can represent every 2-adic integer $x = \ldots \delta_2(x)\delta_1(x)\delta_0(x)$ (where $\delta_i(x) \in \{0, 1\}$, $i = 0, 1, 2, \ldots$) as the series

$$(2.4) \qquad\qquad x = \sum_{i=0}^{\infty} \delta_i(x) \cdot 2^i; \quad (\text{where } \delta_i(x) \in \{0, 1\}, i = 0, 1, 2, \ldots).$$

The series in the right-hand side are called *canonical 2-adic expansion* of the 2-adic integer x; the series converges to x with respect to the 2-adic metric.

Although T-functions are maps from 2-adic integers to 2-adic integers, we also introduce here 2-adic numbers whic are not necessarily 2-adic integers. Denote $\mathbb{Q}_2$ the set of all series of the form $u = \sum_{i=-k}^{\infty} \alpha_i \cdot 2^i$ for all $k = 0, 1, 2, \ldots$ and all $\alpha_{-k}, \alpha_{-k+1}, \ldots \in \{0, 1, \}$. In a way similar to that we have defined addition and multiplication on $\mathbb{Z}_2$, we define these operations on $\mathbb{Q}_2$; the set $\mathbb{Q}_2$ with respect to the so defined addition and multiplication is a *field of 2-adic numbers*, whereas $\mathbb{Z}_2$ is a ring of integers of this field. The absolute value $\|\cdot\|_2$ can be expanded to the whole field $\mathbb{Q}_2$ (by setting $\|u\|_2 = 2^{-\ell}$ where ℓ is the smallest of $j = -k, -k+1, \ldots$ such that $\alpha_j \neq 0$); so $\mathbb{Q}_2$ is a metric space, and the 2-adic absolute value $\|\cdot\|_2$ satisfy all usual axioms. In particular, given $a, b, c \in \mathbb{Q}_2$,

(1) $\|a \cdot b\|_2 = \|a\|_2 \cdot \|b\|_2$,
(2) $\|a - c\|_2 \leq \|a - b\|_2 + \|b - c\|_2$ (the *triangle inequality*).

It worth noting here that for the 2-adic metric the triangle inequality actually holds in a stronger form:

$$\|a - c\|_2 \leq \max\{\|a - b\|_2, \|b - c\|_2\} \text{ (the } strong \text{ triangle inequality)},$$

for all $a, b, c, \in \mathbb{Q}_2$. Now metric on the n-th Cartesian power $\mathbb{Q}_2^n$ of $\mathbb{Q}_2$ can be defined in the following way: $\|(a_1, \ldots, a_n) - (b_1, \ldots, b_n)\|_2 = \max\{\|a_i - b_i\|_2 : i = 1, 2, \ldots, n\}$ for every $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{Q}_2^n$.

Once the metric is defined, one defines notions of convergent sequences, limits, continuous functions on the metric space, and derivatives if the space is a commutative ring. For instance, with respect to the 2-adic metric the following sequence tends to -1:

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

Derivations of a function $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$, which is defined on and valuated in the space $\mathbb{Z}_2$ of 2-adic integers, may be defined in a standard way as in classical (e.g., real) Calculus just by replacing real absolute value $|\cdot|$ by the 2-adic absolute value $\|\cdot\|_2$, as follows:

Definition 1 (2-adic differentiability)**.** *The function f is said to be differentiable at the point $x \in \mathbb{Z}_2$ (and the 2-adic number $f'(x) \in \mathbb{Q}_2$ is said to be its derivative at the point x) if and only if for arbitrary $M \in \mathbb{N} = \{1, 2, \ldots\}$ and sufficiently small (w.r.t. the 2-adic absolute value) h the following inequality holds:*

$$\left\| \frac{f(x + h) - f(x)}{h} - f'(x) \right\|_2 \leq \frac{1}{2^M}$$

Reduction modulo 2^n of a 2-adic integer v, i.e., setting all terms 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 precision $1/2^n$: This approximation is an n-digit positive rational integer $v \wedge (2^n - 1)$; the latter will be denoted also as $v \bmod 2^n$.

Actually *a processor works with approximations of 2-adic integers with respect to 2-adic metric*: When an overflow happens, i.e., when a number that must be written into an n-bit register consists of more than n significant bits, the processor just writes only n low order bits of the number into the register thus reducing the number modulo 2^n. Thus, precision of the approximation is defined by the bitlength of the processor.

2.3. **2-adic continuity of T-functions.** What is most important within the scope of the paper is that all T-functions are *continuous* functions of 2-adic variables since *all T-functions satisfy Lipschitz condition with a constant 1 with respect to the 2-adic metric*, and vice versa.

Indeed, it is obvious that the function $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfy the condition $\|f(u) - f(v)\|_2 \leq \|u - v\|_2$ for all $u, v \in \mathbb{Z}_2$ if and only if f is compatible, since the inequality $\|a - b\|_2 \leq 1/2^k$ is just equivalent to the congruence $a \equiv b \pmod{2^k}$. A similar property holds for n-variate T-functions (we just use the metric $\|\cdot\|_2$ on the n-Cartesian power $\mathbb{Z}_2^n$). So we conclude:

$$T\text{-}functions = compatible\ functions = 1\text{-}Lipschitz\ functions$$

This implies in particular that given a T-function $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and $n \in \mathbb{N}$, the map $f \bmod 2^n \colon z \mapsto f(z) \bmod 2^n$ is a well-defined transformation of the residue ring $\mathbb{Z}/2^n\mathbb{Z} = \{0, 1, \ldots, 2^n - 1\}$; actually the reduced map $f \bmod 2^n$ is a T-function on n-bit words.

The observation we just have made indicates why the the 2-adic analysis can be used in a study of T-functions. For instance, one can prove that the following functions satisfy Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

- subtraction: $(u, v) \mapsto u - v$;
- exponentiation: $(u, v) \mapsto (1 + 2u)^v$;
- raising to negative powers, $u \mapsto (1 + 2u)^{-n}$;
- division: $(u, v) \mapsto \frac{u}{1 + 2v}$.

We now consider derivations of T-functions. We first note that as a T-function is mere a 1-Lipschitz function w.r.t. 2-adic metric, once the derivative exists, *the derivative must be a 2-adic integer*. That is, for the case of T-functions we can re-state Definition 1 in the following equivalent form:

Definition 2 (differentiability of T-functions)**.** *A T-function $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be differentiable at the point $x \in \mathbb{Z}_2$ (and the 2-adic number $f'(x) \in \mathbb{Z}_2$ is said to be its derivative at the point x) if and only if for*

arbitrary $M \in \mathbb{N} = \{1, 2, \ldots\}$ *and sufficiently small* (w.r.t. the 2-adic absolute value) $h \in \mathbb{Z}_2$ *the following congruence holds:*

$$f(x + h) \equiv f(x) + f'(x) \cdot h \pmod{2^{\operatorname{ord}_2 h + M}}$$

Example 1 (differentiability of $\wedge$). *The function* $f(x) = x \wedge c$ *is differentiable at every* $x \in \mathbb{Z}_2$ *for any* $c \in \mathbb{Z}$, *and*

$$f'(x) = \begin{cases} 0, & \text{if } c \geq 0; \\ 1, & \text{if } c < 0. \end{cases}$$

Proof. Indeed, take n greater than the bitlength of $|c|$ (that is, $n \geq \log_2 |c| + 1$); then for all $s \in \mathbb{Z}_2$:

$$f(x + 2^n s) = \begin{cases} f(x) & , \text{if } c \geq 0, \\ f(x) + 2^n s & , \text{if } c < 0, \end{cases}$$

$\square$

In the same manner we can fill the rest of the table of derivations of logical T-functions:

Example 2 (derivations of other logical T-functions). *Let* $c \in \mathbb{Z}$, *then for every* $x \in \mathbb{Z}_2$

$$(2.5) \qquad (\neg x)' = -1; \qquad (x \oplus c)' = \begin{cases} 1, & \text{if } c \geq 0; \\ -1, & \text{if } c < 0. \end{cases} \qquad (x \vee c)' = \begin{cases} 1, & \text{if } c \geq 0; \\ 0, & \text{if } c < 0. \end{cases}$$

Note that rules of derivations (e.g., chain rule) do not depend on metric; thus they are the same both in a classical and in a 2-adic cases, so applying the rules one can find derivatives of T-functions that are used in stream ciphers:

Example 3 (derivative of the Klimov-Shamir T-function).

$$(x + (x^2 \vee 5))' = 1 + 2x$$

Now with the use of Definition 2 we define the notion of *uniform differentiability* of a T-function in the same way as in classical Calculus:

Definition 3 (uniform differentiability). *A T-function* $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *is called uniformly differentiable* (or, equidifferentiable) *iff for every sufficiently large* $M \in \mathbb{N}$ *there exists* $K \in \mathbb{N}$ *such that once* $|h|_2 \leqslant \frac{1}{2^K}$ (*that is, once* $h \equiv 0 \pmod{2^K}$), *the congruence*

$$f(x + h) \equiv f(x) + f'(x) \cdot h \pmod{2^{\operatorname{ord}_2 h + M}}$$

holds for all $x \in \mathbb{Z}_2$. *Given* M, *the minimum* $K = K(M)$ *with this property is denoted via* $N_M(f)$.

For instance, it can be easily verified that Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is uniformly differentiable and $N_M(f) = M$.

Now we introduce another notion related to differentiability that has no direct analogs in classical Calculus.

Definition 4 (differentiability modulo 2^M). *Given* $M \in \mathbb{N}$, *a T-function* $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *is said to be differentiable modulo* 2^M *at the point* $x \in \mathbb{Z}_2$ (*and the 2-adic integer* $f'_M(x) \in \mathbb{Z}_2$ *is said to be its derivative modulo* 2^M *at the point* x) *if and only if for a sufficiently small* (w.r.t. the 2-adic absolute value) $h \in \mathbb{Z}_2$ *the following congruence holds:*

$$f(x + h) \equiv f(x) + f'(x) \cdot h \pmod{2^{\operatorname{ord}_2 h + M}}.$$

Definition 5 (uniform differentiability modulo 2^M). *Given* $M \in \mathbb{Z}$, *a T-function* $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *is called uniformly differentiable modulo* 2^M *iff there exists* $K \in \mathbb{N}$ *such that once* $|h|_2 \leqslant \frac{1}{2^K}$ (*that is, once* $h \equiv 0$ (mod 2^K)), *the congruence*

$$f(x + h) \equiv f(x) + f'(x) \cdot h \pmod{2^{\operatorname{ord}_2 h + M}}$$

holds for all $x \in \mathbb{Z}_2$. *The minimum* $K = K(M)$ *with this property is denoted via* $N_M(f)$.

Note that the notion of derivative modulo 2^M is somewhat like saying 'a derivative with a precision of M digits after the point' in classical Calculus; however, the latter in real Calculus is meaningless, whereas in 2-adic Calculus the phrase has a precise mathematical meaning.

From Definition 4 it readily follows that the derivative modulo 2^M is defined up to a summand which is 0 modulo 2^M; that is, if a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is uniformly differentiable modulo 2^M then its derivative modulo 2^M is a map from $\mathbb{Z}_2$ into the residue ring $\mathbb{Z}/2^M\mathbb{Z}$. Furthermost, it can be proved (see [3]) that a derivative modulo 2^m is a periodic function with a period of length $2^{N_M(f)}$. Thus we state

Proposition 1 (derivatives modulo 2^M). *If a T-function f is uniformly differentiable modulo 2^M, then its derivative modulo 2^M is a periodic function with a period of length $2^{N_M(f)}$; so the derivative can be considered as a map from the residue ring $\mathbb{Z}/2^{N_M(f)}\mathbb{Z}$ to the residue ring $\mathbb{Z}/2^M\mathbb{Z}$.*

Rules of derivation modulo 2^M are of a similar form to that of the classical case; however, they are congruences modulo 2^M rather than equalities.

Example 4. *The T-function $f(x) = x \oplus (-1/3)$ is uniformly differentiable modulo 2^M if and only if $M = 1$; its derivative modulo 2 is 1, and $N_2(f) = 1$. If $M > 1$ then f is differentiable modulo 2^M at no point.*

From Definition 4 it immediately follows that

- if a T-function is differentiable modulo 2^{M+1} then it is uniformly differentiable modulo 2^M;
- a T-function is uniformly differentiable iff it is uniformly differentiable modulo 2^M for all $M \in \mathbb{N}$.

Thus, we have the following hierarchy of classes of uniform differentiability:

$$\mathfrak{D}_1 \supset \mathfrak{D}_2 \supset \mathfrak{D}_3 \supset \cdots \supset \mathfrak{D}_\infty,$$

where $\mathfrak{D}_i$ is the class of all T-functions that are uniformly differentiable modulo 2^i, $i = 1, 2, 3, \ldots$, and $\mathfrak{D}_\infty$ is a class of all uniformly differentiable T-functions. It turns out that *the T-functions of most interest to cryptography, the ones that are invertible, all lie in $\mathfrak{D}_1$; that is, they all are uniformly differentiable modulo 2.*

2.4. **Differentiability, invertibility and single cycle property.** Given $n \in \mathbb{N}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be *bijective modulo 2^n* iff it is invertible on n-bit words; that is, iff the reduced map $f \bmod 2^n\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is a permutation on the residue ring $\mathbb{Z}/2^n\mathbb{Z}$. Similarly, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be *transitive modulo 2^n* iff it is a single cycle on n-bit words; that is, iff the reduced map $f \bmod 2^n\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is a permutation on the residue ring $\mathbb{Z}/2^n\mathbb{Z}$ with the only cycle (hence, with the cycle of length 2^n).

Definition 6. *We say that a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective iff it is bijective modulo 2^n for all $n \in \mathbb{N}$; we say that f is transitive iff f is transitive modulo 2^n for all $n \in \mathbb{N}$.*

Actually the above definition is a theorem that is proved in the p-adic ergodic theory: transitive T-functions are exactly 1-Lipschitz ergodic transformations on $\mathbb{Z}_2$, whereas bijective T-functions are measure-preserving isometries of $\mathbb{Z}_2$ (see [3]). For not to overload the paper we are not going to give a deeper look into the p-adic ergodic theory; within the scope of the paper the above definition is sufficient. The point is that for some T-functions bijectivity (resp., transitivity) modulo 2^n for *some* $n \in \mathbb{N}$ implies their bijectivity (resp., transitivity); that is, under certain conditions, if a T-function is invertible (resp., has a single cycle property) on n-bit words for *some* $n \in \mathbb{N}$, then it is bijective (resp, transitive) invertible (resp., has a single cycle property) on n-bit words for *all* $n \in \mathbb{N}$. For proofs of rest claims of the section readers are referred to monograph [3].

Proposition 2. *If a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective then it is uniformly differentiable modulo 2 and its derivative modulo 2 is 1 everywhere: $f_2'(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$ (equivalently, for all $x \in \mathbb{Z}/2^{N_1(f)}\mathbb{Z}$).*

Theorem 1. *Let a T-function f be uniformly differentiable modulo 2. Then f is bijective iff f is bijective modulo $2^{N_1(f)}$ and $f_2'(x) \equiv 1 \pmod 2$ everywhere. Equivalently: if and only if f is bijective modulo $2^{N_1(f)+1}$.*

Theorem 2. *Let a T-function f be uniformly differentiable modulo 4. Then f is transitive iff f is transitive modulo $2^{N_2(f)+2}$.*

Example 5. *The Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is transitive.*

Proof. Indeed, f is uniformly differentiable, $N_2(f) = 2$; so it suffices to check whether the residues modulo 16 of $0, f(0), f^2(0) = f(f(0)), \ldots, f^{15}(0)$ are all different. This can readily be verified by direct calculations. $\quad\square$

It worth noting here that all transitive (as well as all bijective) T-functions can be represented in a certain 'explicit' form:

Theorem 3 ([6], also [3, Theorem 4.44]).
- *A T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective if and only if it is of the form $f(x) = c + x + 2g(x)$, where g is an arbitrary T-function, $c \in \{0, 1\}$.*
- *A T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is transitive if and only if it is of the form $f(x) = 1 + x + 2(g(x+1) - g(x))$, where g is an arbitrary T-function.*

2.5. **Properties of coordinate sequences.** Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and a 2-adic integer $x_0 \in \mathbb{Z}_2$, consider i-th coordinate sequence $(\delta_i(f^j(x_0))_{j=0}^\infty$. The sequence satisfies recurrence relation (1.1); that is, the second half of the period of the i-th coordinate sequence is a bitwise negation of the first half; so the shortest period (which is of length 2^{i+1}) of the sequence is completely determined by its first 2^i bits. It turns out that given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (The independence of coordinate sequences). *Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$:*

$$\delta_i(f^j(x_0)) = \zeta_j, \quad \text{for all } j = 0, 1, \ldots, 2^i - 1.$$

The essence of our contribution is that *coordinate sequences of a transitive T-function that is uniformly differentiable modulo 4 are not independent any longer: there are linear relations among them.*

3. Main results: statements

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and the initial state $x_0 \in \mathbb{Z}_2$, for $i = 0, 1, 2, \ldots$ denote $x_i = f^i(x_0)$, $\chi_n^i = \delta_i(f^n(x_0))$, the n-th digit in the canonical 2-adic expansion of the n-th iterate of x_0. That is, the binary sequence $(\chi_n^i)_{i=0}^\infty$ is the n-th coordinate sequence of the recurrence sequence determined by the recurrence law $x_{i+1} = f(x_i)$.

3.1. **Linear relation.** Our first result yields that if a transitive T-function is uniformly differentiable modulo 4 then *two* adjacent coordinate sequences satisfy linear relation of form (1.2):

Theorem 5. *Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f) + 1$ the following congruence holds:*

$$(3.1) \qquad \chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^i + \chi_n^i + \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + y(i) \pmod 2. \qquad (i = 0, 1, 2, \ldots),$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^\infty$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermost, $\gamma(i)$ does not depend on n.

Proof. See Appendix A.1. $\quad\square$

Note that if a T-function is transitive then by Proposition 2 it is uniformly differentiable modulo 2; so conditions of Theorem 5 seem not too restrictive: we only demand that the T-function lies in the second large differentiability class $\mathfrak{D}_2$ whereas it already lies in the largest one (i.e., in $\mathfrak{D}_1$) due to transitivity.

As both polynomial T-functions (the ones represented by polynomials over $\mathbb{Z}_2$) and the Klimov-Shamir T-function (of the form $x + (x^2 \vee C)$, $C \in \mathbb{Z}$) are uniformly differentiable (thus, lie in $\mathfrak{D}_\infty$ and whence in $\mathfrak{D}_2$), our Theorem 5 could be considered as a generalization of results due to Jin-Song Wang and Wen-Feng Qi, [38], and to Molland and Helleseth, [30, 31]. However, the class of transitive T-functions that are uniformly differentiable modulo 4 (thus, the class of T-functions that satisfy our Theorem 5) is much wider: for instance, it contains all T-functions of forms $f(x) = u(x) + 4 \cdot v(x)$ and $f(x) = u(x + 4 \cdot v(x))$, where u is a transitive T-function that is uniformly differentiable modulo 4 and v is an *arbitrary* T-function, see [3, Proposition 9.29]. In particular, this implies that a monster T-function from (1.3) satisfies Theorem 5.

Moreover, given an arbitrary T-function g that is uniformly differentiable modulo 2 (say, given a bijective T-function g), the T-function $f(x) = 1 + x + 2(g(x+1) - g(x))$ is transitive and uniformly differentiable modulo 4; cf. Theorem 3.

These examples serve to demonstrate how large is the class of T-functions that satisfy Theorem 5. More specific examples of the latter functions can be constructed with the use of various techniques of non-Archimedean analysis, see [3]. For instance, exponential functions of the form $f(x) = ax + a^x$, where $a \equiv 1$ (mod 2), are uniformly differentiable and transitive, as well as rational functions of the form $f(x) = \frac{u(x)}{1+4 \cdot v(x)}$, where u is a transitive polynomial and v is arbitrary T-function. We remind that a polynomial over $\mathbb{Z}_2$ is transitive iff it is transitive modulo 8.

3.2. **Quadratic relation.** Our second result yields that if a T-function lies in the third largest differentiability class $\mathfrak{D}_3$ then there exist a quadratic relation among *three* adjacent coordinate sequences:

Theorem 6. *Let the ergodic T-function f be uniformly differentiable modulo 8. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_3(f) + 2$ the following congruence holds:*

$$(3.2) \qquad \chi_n^{i+2^{n-2}} \equiv \chi_{n-2}^i \chi_{n-1}^i + \theta(n)(\chi_{n-2}^i + \chi_{n-1}^i) + \chi_n^i + y_i \pmod 2, \qquad (i = 0, 1, 2, \ldots),$$

where $\theta(n) \in \{0, 1\}$ does not depend on i. Furthermost, the length of the shortest period of the binary sequence $(y_i)_{i=0}^{\infty}$ is a factor of $2^{N_3(f)}$ if $N_3(f) > 1$.

Proof. See Appendix A.2. □

As the Klimov-Shamir T-function $f(x) = x + (x^2 \vee C)$ for $C \in \mathbb{Z}$, is uniformly differentiable, it satisfy Theorem 6 once it is transitive, i.e., once $C \equiv 5 \pmod 8$ or $C \equiv 7 \pmod 8$; thus, Theorem 6 may be considered as a generalization of a result of Yong-Long Luo and Wen-Feng Qui [27] who proved quadratic relation for the Klimov-Shamir T-function.

4. Application to T-function-based stream ciphers

In this section we discuss how relations (3.1) and (3.2) from Theorems 5 and 6 may be used to attack stream ciphers that use T-functions to generate pseudorandom sequences. We do not construct attacks themselves, we only point out some approaches that may result in the attacks. We consider mostly the linear relation; however, one may use the quadratic relation as well, by analogy.

Basically a stream cipher is a pseudorandom generator where the produced binary sequence is used as a keystream, i.e., is XOR-ed with a plaintext to encrypt a message. A pseudorandom generator (PRG) can be thought of as an algorithm that takes at random a short initial binary string, the key, and stretches it to a much longer binary sequence, the keystream, which looks like random. that is, passes a set of reasonable tests in a reasonable time. A stream cipher must withstand various cryptographic attacks.
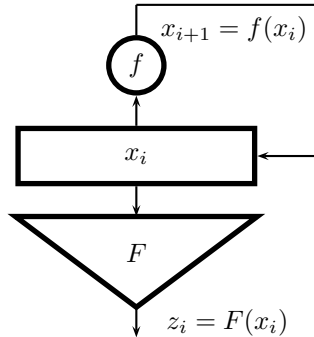

FIGURE 1. Pseudorandom generator

Basically a PRG can be considered as an automaton with no input (see Figure 1) , where initial state $x_0 \in \{0, 1, \ldots, 2^k - 1\}$ is a key, or is produced during the 'warming-up' stage from the key and IV, the initial vector. We assume that the *state transition function f is a T-function on k-bit words*. Moreover, f (as

well as the output function F) may depend on a key, or even may change during the encryption procedure, that is actually the recurrence law is $x_{i+1} = f_i(x_i)$. In the latter case, the corresponding generator is called *counter-dependent* [37]; and we assume that *all* f_i are T-functions on k-bit words. Foremost, they may be multivariate T-functions as well, and not necessarily univariate ones.

Our second basic assumption yields that one knows *sufficiently long segments of two coordinate sequences* $(\chi_{n-1}^i)_{i=0}^\infty$ and $(\chi_n^i)_{i=0}^\infty$ $n \le k-1$, of the state sequence $(x_i)_{i=0}^\infty$. In this Section, we explain *how under these assumptions one can recover low order coordinate sequences* $(\chi_m^i)_{i=0}^\infty$ *for $m < n-1$*. After explaining general method in Subsection 4.1 for the case of univariate transitive T-function, we apply the method to multivariate transitive T-functions (Subsection 4.2) and to counter-dependent generators (Subsection 4.3).

4.1. **General method.**

Assume that the state transition function f does not depend on i, and assume that f is a reduction modulo 2^k of a univariate transitive T-function $\tilde{f}: \mathbb{Z}_2 \to \mathbb{Z}_2$ (i.e., $f = \tilde{f} \bmod 2^k$) which is *uniformly differentiable modulo 4* so that $N_2(\tilde{f}) < n-1 < k-1$. It can be shown (see e.g. the example at the end of 4.2.2) that, given a T-function f which is transitive on k-bit words, transitive T-functions $\tilde{f}: \mathbb{Z}_2 \to \mathbb{Z}_2$ which are uniformly differentiable modulo 4 and such that $f = \tilde{f} \bmod 2^k$ always exist; however, the core of our assumption is that the number $N_2 = N_2(\tilde{f})$ must be sufficiently small: $N_2 < n-1 < k-1$.

We stress that in most cases the latter assumption is not too restrictive: e.g., for polynomials with integer coefficients we have that $N_2 \le 2$, whereas for the Klimov-Shamir T-function $x + (x^2 \vee 5)$ we have that $N_2 = 2$; and we have $N_2 = 1$ for monster T-function (1.3). Note that although for Klimov-Shamir T-function $x + (x^2 \vee C)$, $C \in \mathbb{Z}$, which is uniformly differentiable if $C \in \mathbb{N}_0$, the number N_2 depends on the length of binary representation of $|C|$, in practice only small C should be used (e.g., $C = 5$) since distribution properties of the Klimov-Shamir T-function are the poorer the more 1-s are in the 2-adic representation of C: For instance, if $C < 0$ then 2-dimensional distribution properties of output sequence of corresponding Klimov-Shamir generator are practically the same as the ones for the transitive T-function $x \mapsto x - 1$, see [35] for a comprehensive study of distribution properties of Klimov-Shamir generators; some information about these can also be found in [3, Section 11.1].

In practice, to construct a T-function $\tilde{f}$ given the T-function f we should do absolutely nothing since actually $\tilde{f}$ is just an expansion of f to the whole space $\mathbb{Z}_2$: for instance, if f is a polynomial with integer coefficients (or Klimov-Shamir T-function $x + (x^2 \vee C)$, or monster T-function (1.3), etc.), then $\tilde{f}$ is just the same polynomial (Klimov-Shamir T-function, monster T-function) considered over a larger domain, $\mathbb{Z}_2$ rather than $\mathbb{Z}/2^k\mathbb{Z}$. Thus, our basic assumption just yields that the transitive T-function f must be uniformly differentiable modulo 4 and $N_2(f)$ must be sufficiently small, at least, smaller than $k-2$; then we can recover coordinate sequences $(\chi_m^i)_{i=0}^\infty$ for $m = n-2, n-3, \ldots, N_2(f)$. Of course, to recover the whole m-th coordinate sequence we just have to recover its first 2^{m-1} terms due to the property (1.1).

We now proceed with all these assumptions in mind.

4.1.1. *The method for a univariate T-function.*

We proceed as follows.

(1) Given first 2^n bits of coordinate sequences $(\chi_{n-1}^i)_{i=0}^\infty$ and $(\chi_n^i)_{i=0}^\infty$, we find the sequence $(y(i))_{i=0}^{2^{n-1}-1}$ by solving equations (3.1) w.r.t. $y(i)$.

(2) As by Theorem 5 the sequence $(y(i)$ does not depend on n, having $(y(i))_{i=0}^{2^{n-1}-1}$ and solving equations (3.1) for $n := n-1$ and $i = 0, 1, 2, \ldots, 2^{n-2}-1$ we find *two* sequences $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$ of solutions $(\chi_{n-2}^i)_{i=0}^{2^{n-2}-1}$: the first sequence $\mathcal{S}_{n-2}^0$ of solutions corresponds to the choice $\chi_{n-2}^0 = 0$, whereas the second one, $\mathcal{S}_{n-2}^1$, corresponds to the choice $\chi_{n-2}^0 = 1$ in equation (3.1). Therefore the two bit sequences $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$ are *mutually complementary*, $\mathcal{S}_{n-2}^0 \oplus \mathcal{S}_{n-2}^1 = (1)_{i=0}^{2^{n-2}-1}$; that is, the sum of the i-th term of the first sequence with the i-th term of the second sequence is always 1 modulo 2, for all $i = 0, 1, 2, \ldots, 2^{n-2}-1$. Now to find full period $\mathcal{S}_{n-2} = (\chi_{n-2}^i)_{i=0}^{2^{n-1}-1}$ of the $(n-2)$-th coordinate sequence $(\chi_{n-2}^i)_{i=0}^\infty$ we use relation (1.1) (which yields that $\chi_{n-2}^{i+2^{n-2}} \equiv \chi_{n-2}^i + 1 \pmod{2}$ in the case under consideration) to continue finite sequences $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$, which actually are two variants of the first half-period of the $(n-2)$-th coordinate sequence $\mathcal{S}_{n-2}$, to full periods, of length 2^{n-1}; we keep the same notation for these two variants of the full period, i.e., $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$. Thus we find *two solutions for the full period of $(n-2)$-th coordinate sequence $\mathcal{S}_{n-2}$, namely, $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$, and the solutions are mutually complementary: $\mathcal{S}_{n-2}^0 \oplus \mathcal{S}_{n-2}^1 = (1)_{i=0}^{2^{n-1}-1}$.*

(3) Next, given the sequence $(y(i))$ and two variants $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$ of the $(n-2)$-th coordinate sequence, we find a pair of mutually complementary sequences $\mathcal{S}_{n-3}^0$ and $\mathcal{S}_{n-3}^1$ for either of $\mathcal{S}_{n-2}^0$ and $\mathcal{S}_{n-2}^1$ by solving equation (3.1) for $n := n - 2$ w.r.t. indeterminate χ_{n-3}^i. However, among these 4 obtained variants of the first half-period of the $(n-2)$-th coordinate sequence there are only *two* different (depending on the value of $\chi_{n-2}^0 \oplus \chi_{n-3}^0$) and they are mutually complementary. Thus, at this step we again obtain *two solutions, $\mathcal{S}_{n-3}^0$ and $\mathcal{S}_{n-3}^1$, for the full period of the $(n-3)$-th coordinate sequence $\mathcal{S}_{n-3}$, and the solutions are mutually complementary: $\mathcal{S}_{n-3}^0 \oplus \mathcal{S}_{n-3}^1 = (1)_{i=0}^{2^{n-2}-1}$.*

(4) Proceed with $n := n - 3$, etc.

Two important remarks should be made:

- As the T-function f is uniformly differentiable modulo 4, at every step j we recover *two* variants of the first half of a period of the $(n-j)$-th coordinate sequence rather than $2^{2^{n-j}}$ variants for a general transitive T-function f, cf. Theorem 4; and the two variants are mutually complementary, so *actually we need to recover only one of these variants*; so at each step j we just solve $2^{n-j} - 1$ linear Boolean equations (3.1), for $i = 1, 2, \ldots, 2^{n-j} - 1$, each of one Boolean indeterminate, χ_{n-j}^i.
- Nowhere in the algorithm we used the T-function f by itself, e.g., its explicit representation in a certain form; *we used only the fact that f is transitive and uniformly differentiable modulo 4.*

4.2. **The case of multivariate T-functions.** We firstly stress that a multivariate transitive T-function that is uniformly differentiable modulo 2 (thus, modulo 4) *does not exist*, see [3, Theorem 4.51]; and secondly, that *all known multivariate transitive T-functions actually are just multivariate representations of univariate transitive T-functions*, see [3, Section 10.4]. We briefly explain now what are the latter representations.

A transitive multivariate T-function is a map of form (2.1) from the n-th Cartesian power $\mathbb{Z}_2^n$ of the space $\mathbb{Z}_2$ to its m-th Cartesian power $\mathbb{Z}_2^m$ where $m = n$. Loosely speaking, we can consider an element of $\mathbb{Z}_2^m$ as a table of m one-side infinite binary rows $x^{(0)}, \ldots, x^{(m-1)}$ (say, stretching from left to right). To this table, we put into the correspondence infinite binary string (that is, a 2-adic integer from $\mathbb{Z}_2$) obtained by reading successively elements of each column of the table, from top to bottom and from left to right. Thus we establish a one-to-one correspondence B between $\mathbb{Z}_2^m$ and $\mathbb{Z}_2$. Now, given a transitive univariate T-function f of form (2.2) and using the correspondence, we construct an m-variate transitive T-function $\mathbf{f} \colon \mathbb{Z}_2^m \to \mathbb{Z}_2^m$: If

$$x = (\chi_0; \chi_1; \chi_2; \ldots) \overset{f}{\mapsto} (\psi_0(\chi_0); \psi_1(\chi_0, \chi_1); \psi_2(\chi_0, \chi_1, \chi_2); \ldots)$$

then $\mathbf{f} = (h^{(0)}, \ldots, h^{(m-1)})$ is defined as follows:

(4.1)

$$
\begin{aligned}
x^{(0)} &= (\chi_0 & ; & \chi_m & ; & \chi_{2m}; & \ldots &) \overset{h^{(0)}}{\mapsto} & (\psi_0(x) & ; & \psi_m(x) & ; & \psi_{2m}(x) & ; \ldots &) \\
x^{(1)} &= (\chi_1 & ; & \chi_{m+1} & ; & \chi_{2m+1}; & \ldots &) \overset{h^{(1)}}{\mapsto} & (\psi_1(x) & ; & \psi_{m+1}(x) & ; & \psi_{2m+1}(x); & \ldots &) \\
& \ldots\ldots & & \ldots & & \ldots & & \ldots & \ldots & & \ldots & & \ldots & \\
x^{(m-1)} &= (\chi_{m-1} & ; & \chi_{2m-1} & ; & \chi_{3m-1}; & \ldots &) \overset{h^{(m-1)}}{\mapsto} & (\psi_{m-1}(x) & ; & \psi_{2m-1}(x) & ; & \psi_{3m-1}(x); & \ldots &)
\end{aligned}
$$

where $x^{(0)}, \ldots, x^{(m-1)}$ are new 2-adic variables, $\psi_j(x) = \psi_j(\chi_0, \ldots, \chi_j)$, $j = 0, 1, 2, \ldots$. We stress that known multivariate transitive T-functions from [18, 14] are based on representations of this sort of univariate transitive T-functions; and that these are multivariate T-functions that are used in the design of ciphers Mir-1 [29], ASC [39], TF-i family [19], and TSC family [15].

To apply our basic approach 4.1.1 to a multivariate T-function $\mathbf{f}$ of this sort, the corresponding univariate T-function f must be uniformly differentiable modulo 4. However, even this is not the case, we can consider a *conjugated* univariate T-function f^w which is uniformly differentiable modulo 4. Indeed, all univariate transitive T-functions are mutually conjugated: *Given a pair of transitive T-functions $u, v \colon \mathbb{Z}_2 \to \mathbb{Z}_2$, there exists a bijective T-function $w \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ such that $u = v^w = w^{-1} \circ v \circ w$*, where $\circ$ stands for composition of functions (see e.g. [13]). Now, if we know the conjugating function w we can apply method 4.1.1.

4.2.1. *The method for multivariate T-functions.* Denote $B \colon \mathbb{Z}_2^m \to \mathbb{Z}_2$ the above one-to-one correspondence between $\mathbb{Z}_2^m$ and $\mathbb{Z}_2$; thus, given a transitive m-variate T-function $\mathbf{f} = (h^{(0)}, \ldots, h^{(m-1)}) \colon \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ of form (4.1), the corresponding univariate T-function is $f = \mathbf{f}^{B^{-1}} = B \circ \mathbf{f} \circ B^{-1}$. Now let g be a univariate T-function

for which relations (3.1) holds. As $f = g^w$ for a suitable T-function $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ (we assume that w is known), then the i-th term $\mathbf{x}_i$ of the output sequence $(\mathbf{x}_i)_{i=0}^\infty$ of the generator with the recursion law $\mathbf{x}_{i+1} = \mathbf{f}(\mathbf{x}_i)$, $\mathbf{x}_i = (x_i^{(0)}, \dots, x_i^{(m-1)})$ can be represented as $\mathbf{x}_i = \mathbf{f}^i(\mathbf{x}_0) = B^{-1}(w^{-1}(g^i(w(B(\mathbf{x}_0)))))$. Therefore, as for g linear relations (3.1) hold, we can use them to recover coordinate sequences of the sequence $(\mathbf{x}_i)_{i=0}^\infty$ since

$$w(B(\mathbf{x}_i)) = g^i(w(B(\mathbf{x}_0)).$$

In other words, *rather than trying to recover coordinate sequences of the generator with the recursion law* $\mathbf{x}_{i+1} = \mathbf{f}(\mathbf{x}_i)$ *and with initial state* $\mathbf{x}_0$ *we can study coordinate sequences of the generator with the recursion law* $x_i = g(x_0)$ *with the initial state* $x_0 = w(B(\mathbf{x}_0))$ *and with a bijective output function* $B^{-1} \circ w^{-1}$.

Basically the approach will work if the output function $B^{-1} \circ w^{-1}$ is known. However, the bijective output function $B^{-1} \circ w^{-1}$ can be considered as "known" if w is easy to find and easy to invert; i.e.,

- if it is easy to find the conjugating T-function w given T-functions f and g which are conjugated via w: $f = g^w$ (in particular, w must admit then a "short" representation in some form); and
- if, given w, it is easy to find the inverse T-function w^{-1} such that $w \circ w^{-1}$ is an identity transformation (in particular, this means that w^{-1} admits a "short" representation as well).

Indeed, B is just "concatenation of columns": it maps m strings (2-adic integers) $x^{(0)}, \dots, x^{(m-1)}$ (see the left side of (4.1)) to a single string (a 2-adic integer) $x = (\chi_0; \chi_1; \dots; \chi_{m-1}; \chi_m; \dots; \chi_{2m-1}; \chi_{2m}; \dots)$; so the inverse B^{-1} is just "cutting a single string into columns of height m", which is easy.

Finding w from the equation $f = g^w$ may be an infeasible task: Although, given two single cycle permutations f and g on some finite set, one may find all conjugating permutations w by solving the equation by Cauchy method, direct application of the latter will take exponentially long time since in our case the set is of order 2^{km} (if we consider an m-variate T-function on k-bit words). Also, given a bijective T-function w in some 'short' form, there are a number of algorithms to find the inverse T-function w^{-1}; however, the representation of w^{-1} may be too long and thus the problem of finding w^{-1} will also be infeasible.

On the other side, in many practical cases main ideas of the approach work either directly or after certain adjustment: to illustrate, we apply these to a multivariate T-function from [14] which is used in TSC family of stream ciphers.

4.2.2. *Linear relation in multivariate function of TSC family of ciphers.* We start with a description of a general T-function T used in these ciphers. Given $\mathbf{x} = (x^{(0)}, \dots, x^{(m-1)}) \in \mathbb{Z}_2^m$, denote $\delta_j(\mathbf{x}) = (\delta_j(x^{(0)}), \dots, \delta_j(x^{(m-1)}))$ (the j-th columnar binary vector $(\chi_{jm}, \dots, \chi_{(j+1)m-1})$ in the notation of (4.1))

A special m-variate T-function $\alpha(\mathbf{x})$ on k-bit words (the *odd parameter*) is fixed. For our purposes, we do not need detailed description of $\alpha(\mathbf{x})$, we only note that in our terms $\alpha \colon \mathbb{Z}_2^m \to \mathbb{Z}_2$ is a T-function such that $\delta_j(\alpha(\mathbf{x}))$ does not depend on $\delta_j(\mathbf{x})$ and the Boolean function $\delta_j(\alpha(\mathbf{x}))$ of Boolean variables $\chi_0, \dots, \chi_{im-1}$ is of odd weight; that is $\delta_0(\alpha(\mathbf{x})) = 1$ and algebraic normal form of the Boolean function $\delta_j(\alpha(\mathbf{x}))$ contains a monomial $\chi_0 \cdots \chi_{jm-1}$ (this is equivalent to the definition of odd parameter in [14, 16, 18])

Further, an S-box is fixed. That is, the sequence of permutations $S_0, S_1, S_2, \dots$ on m-bit words is given. Each permutation S_j acts on the j-th column $D_j(\mathbf{x}) = \delta_j(\mathbf{x}) = (\chi_{jm}, \dots, \chi_{(j+1)m-1})$ by substituting it for $S_j(D_j(\mathbf{x}))$. Also, a sequence of odd numbers $\sigma_0, \sigma_1, \sigma_2, \dots$ and a sequence of even numbers $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$ are given. Now the T-function T of TSC family of stream ciphers is defined as follows:

$$\delta_j(T(\mathbf{x})) = \begin{cases} S_j^{\sigma_j}(\delta_j(\mathbf{x})), & \text{if } \delta_j(\alpha(\mathbf{x})) = 1; \\ S_j^{\varepsilon_j}(\delta_j(\mathbf{x})), & \text{if otherwise.} \end{cases}$$

The key point is that if m is small, then, given S_j and a permutation L_j that has the same cycle structure as S_j, one easily finds conjugating permutation R_j by solving the equation $S_j = R_j^{-1} L_j R_j$ by Cauchy method.

In TSC family m is small: For every TSC$-i$ ($i = 1, 2, 3, 4$), the input is arranged into $m = 4$ input words of $k = 32$ (TSC-1, -2, -4) or $k = 40$ (TSC-3) bits. That is, to find conjugating permutations one will solve 32 or 40 equations $S_j = R_j^{-1} L_j R_j$ in the symmetric group on 16 elements. Moreover, in TSC family all permutations S_j are single cycles.

Now put $L_j(z) = (z + 1) \bmod 2^m$, a single cycle permutation that acts on m-bit words by adding 1 modulo 2^m; that is, L_j reads the j-column $(\chi_{im}; \chi_{im+1}; \dots; \chi_{(i+1)m-1})$ as a base-2 expansion of a non-negative integer $z = \chi_j m + \chi_{jm+1} \cdot 2 + \dots + \chi_{(j+1)m-1} 2^{m-1}$, sends z to the least non-negative residue $\overline{z + 1}$ of $z + 1$ modulo 2^m and returns the column $(\delta_0(\overline{z+1}); \delta_1(\overline{z+1}); \dots; \delta_{m-1}(\overline{z+1}))$ consider a T-function

$L\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ defined as follows:

$$\delta_j(L(\mathbf{x})) = \begin{cases} L_j^{\sigma_j}(\delta_j(\mathbf{x})), & \text{if } \delta_j(\alpha(\mathbf{x})) = 1; \\ L_j^{\varepsilon_j}(\delta_j(\mathbf{x})), & \text{if otherwise.} \end{cases}$$

This implies that the T-function T is conjugate to the univariate T-function $t\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ that acts as follows: given the input string $x = (\chi_0; \chi_1; \dots)$, it is considered as concatenation of m-bit words $q_0, q_1, \dots$ $q_j = \chi_{jm}\chi_{im+1}\cdots\chi_{(j+1)m-1}$, the T-function t reads each word q_j as a base-2 expansion of the non-negative number $Q_j = \chi_{jm} + \chi_{jm+1}2 + \cdots + \chi_{(j+1)m-1}2^{m-1}$, returns the m-bit word $t_j(q_j)$ that is a base-2 expansion of the number

$$D_j(t(x)) = t_j(Q_j) = (Q_j + \sigma_j \cdot a_j(Q_0, \dots, Q_{j-1}) + \varepsilon_j \cdot (1 - a_j(Q_0, \dots, Q_{j-1}))) \bmod 2^m,$$

where $a_j(Q_0, \dots, Q_{i-1}) = \delta_j(\alpha(B^{-1}(x)))$, B is the one-to-one correspondence between $\mathbb{Z}_2^m$ and $\mathbb{Z}_2$ from 4.2.1.

It turns out that coordinate sequences of each sequence $(D_j(t^i(x)))_{i=0}^\infty$ of m-bit words satisfy relation (3.1). Note that our claim is that the relation holds *only* within every sequence $(D_j(t^i(x)))_{i=0}^\infty$, and *not* necessarily between the coordinate sequences $(\delta_{jm-1}(t^i(x)))_{i=0}^\infty$ and $(\delta_{jm}(t^i(x)))_{i=0}^\infty$ since they belong to coordinate sequences of different sequences, of $(D_{j-1}(t^i(x)))_{i=0}^\infty$ and $(D_j(t^i(x)))_{i=0}^\infty$, respectively.

To prove the claim it suffices to prove it for coordinate sequences (of sufficiently large order) of a univariate T-function f that is defined as follows. Let $u\colon \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2^k\mathbb{Z}$ is a transitive T-function on k-bit words, let the map $v\colon \mathbb{Z}/2^k\mathbb{Z} \to \{0,1\}$ takes value 1 on the odd number of k-bit words: $\#\{z \in \mathbb{Z}/2^k\mathbb{Z}\colon v(z) = 1\}$ is odd; let σ be odd, and let ε be even. Given $x \in \mathbb{Z}_2$, x admits a unique representation $x = \bar{x} + 2^k\tilde{x}$ for a suitable $\tilde{x} \in \mathbb{Z}_2$. Now put

$$f(x) = u(\bar{x}) + 2^k(\tilde{x} + (\sigma - \varepsilon)v(\bar{x}) + \varepsilon).$$

Firstly, we note that f is uniformly differentiable and that $N_2(f) \le k$. Indeed, given $h = 2^\ell r$ for $\ell \ge k$, one has $f(x + h) = u(\bar{x}) + 2^k(\tilde{x} + 2^{\ell-k}r + (\sigma - \varepsilon)v(\bar{x}) + \varepsilon) = f(x) + 2^\ell r = f(x) + h$.

Secondly, f is transitive. Indeed,

$$f^{2^k}(x) = u^{2^k}(\bar{x}) + 2^k\left(\tilde{x} + (\sigma - \varepsilon)\sum_{j=0}^{2^k-1} v(u^j(\bar{x})) + 2^k\varepsilon\right);$$

however, $s = \sum_{j=0}^{2^k-1} v(u^j(\bar{x}))$ is odd by the definition of v since $u^j(\bar{x})$ runs through all k-bit words as $j = 0, 1, 2, \dots, 2^k - 1$, due to transitivity of u. Thus, f is transitive modulo 2^{k+2} as the map $\tilde{x} \mapsto \tilde{x} + (\sigma - \varepsilon)s + 2^k\varepsilon$ is obviously transitive modulo 4 as $(\sigma - \varepsilon)s + 2^k\varepsilon$ is odd. Finally, f is transitive by Theorem 2 and thus satisfy conditions of Theorem 5. This proves our claim (of course, the transitivity of f might be proved directly rather than by applying Theorem 2).

We stress that we only state that there are linear relations of form (3.1) in the output sequences of generators based on T-functions of the sort of ones used in TSC stream ciphers, and we do *not* claim that these relations affect (or do not affect) the security of the ciphers. The latter is out of scope of the paper; it worth noting here only that the ciphers were successfully attacked, however, using vulnerabilities other than the ones we indicate, see e.g. [33, 40].

It also worth noticing here that the method can not be immediately applied to stream ciphers Mir-1, TF-i and ASC although all of these are based on a multivariate version of Klimov-Shamir T-function $x + (x^2 \vee C)$ for which the relations hold due to the result of Molland and Helleseth mentioned at the beginning of the paper.

4.3. **The case of counter-dependent generators.** A counter-dependent generator is a pseudorandom generator with the recursion law $x_{i+1} = f_i(x_i)$, that is, the state transition (and/or the output) function changes dynamically during processing. Counter-dependent generators were introduced in [37]; in [3, Section 10.3] it is shown that counter-dependent generators can be considered as wreath products of dynamical systems which are ordinary generators, and the corresponding theory is developed. The theory enables one to construct counter-dependent generators of the longest possible period. Generators of this kind were used in ABC stream ciphers, see [10, 9, 12, 11, 8].

Loosely speaking, wreath product of generators is a cascaded composition of generators, see Figure 2. If all f_{y_i} are T-functions on k-bit words, the maximum length of the shortest period of the counter-dependent
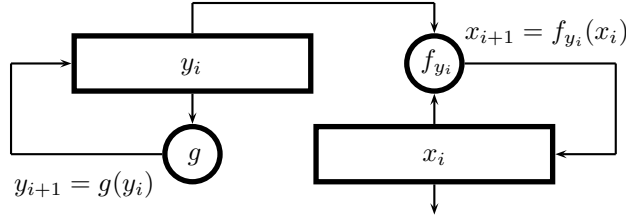
FIGURE 2. Counter-dependent generator, the wreath product of generators

generator from Figure 2 is $p \cdot 2^k$, where p is the length of the shortest period of the generator with the recursion law $y_{i+1} = g(y_i)$. For conditions when the counter-dependent generator achieves the longest possible period see [3, Theorem 10.9; Lemma 10.12]; structure of the corresponding output sequence is presented at Figure 3: the shortest period of this sequence achieves the maximum length, $p \cdot 2^k$, i.e., the period is a finite sequence $(x_i)_{i=0}^{p2^k - 1}$ of length $p \cdot 2^k$ of k-bit words which is a union of p subsequences $(x_{r+pj})_{j=0}^{2^k - 1}$, $r = 0, 1, 2, \ldots, p - 1$, and each subsequence $(x_{r_pj})_{j=0}^{2^k - 1}$ is generated by a transitive T-function w_r: $w_r = f_{y_{r+p+1}} \circ \cdots \circ f_{y_r}$, $w_r(x_{r+(\ell-1)p}) = x_{r+\ell p}$, $\ell = 1, 2, \ldots$. We conclude now that *if all T-functions f_{y_j} are uniformly differentiable modulo 4* then all T-functions w_r are uniformly differentiable modulo 4 and transitive; thus, all T-functions w_r satisfy conditions of Theorem 5. Therefore *coordinate sequences of every subsequence $(x_{r+\ell p})_{\ell=0}^{\infty}$ of output sequence $(x_i)_{i=0}^{\infty}$ satisfy linear relation* (3.1).
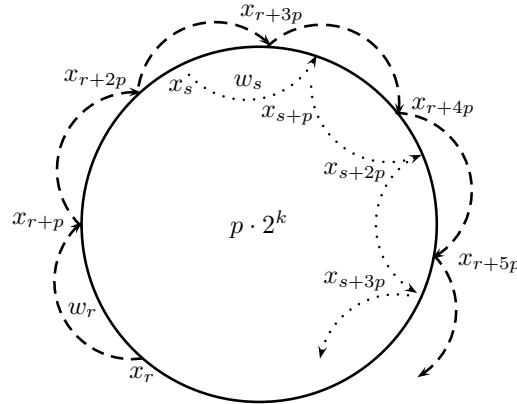

FIGURE 3. Structure of the sequence generated by wreath product.

It is worth noting here that the above result on linear relations in coordinate sequences produced by wreath products of generators can not be applied immediately to ABC stream ciphers since the latter use wreath products of linear feedback shift register with an 'add-xor' generator. However, the latter is based on a transitive T-function of the form $(\ldots ((x \oplus a_1) + a_2) \oplus a_3) + a_4) \oplus \cdots$ which is not uniformly differentiable modulo 4. Of course, this does not serve a proof (or a disproof) that there are no linear relations between coordinate sequences produced by the ABC wreath product.

5. CONCLUSION

In the paper, we prove that a vast body of transitive T-functions exhibit linear and quadratic weaknesses: we found a linear (Theorem 5) and a quadratic (Theorem 6) relation that are satisfied by output sequences generated by univariate transitive T-functions that constitute a very vast class $\mathfrak{D}_2$ (see Subsection 2.3 about the latter class). Earlier relations of this sort were known only for T-functions of two special types: for the Klimov-Shamir T-function $x + (x^2 \vee C)$ and for polynomials with integer coefficients. The class $\mathfrak{D}_2$ is much wider: it contains rational functions, exponential functions as well as their various compositions

with bitwise logical operations. Moreover, we proved that relations of this kind hold in output sequences of corresponding classes of multivariate T-functions as well as in output sequences of T-function-based counter-dependent generators; the latter are generators with a recursion law of the form $x_{i+1} = f_i(x_i)$. Primitives of both types, the multivariate T-function-based ordinary generators and T-function-based counter-dependent generators, are used in stream ciphers, e.g., in ASC, TF-i, TSC, and in ABC. We illustrated our method by finding linear relations for T-function of the sort used in TSC stream ciphers.

References

[1] V. Anashin. Non-Archimedean theory of T-functions. In *Proc. Advanced Study Institute Boolean Functions in Cryptology and Information Security*, volume 18 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 33–57, Amsterdam, 2008. IOS Press.

[2] V. Anashin. Non-Archimedean ergodic theory and pseudorandom generators. *The Computer Journal*, 53(4):370–392, 2010.

[3] V. Anashin and A. Khrennikov. *Applied Algebraic Dynamics*, volume 49 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.

[4] V. S. Anashin. Uniformly distributed sequences of *p*-adic integers. *Mathematical Notes*, 55(2):109–133, 1994.

[5] V. S. Anashin. Uniformly distributed sequences in computer algebra, or how to constuct program generators of random numbers. *J. Math. Sci.*, 89(4):1355–1390, 1998.

[6] V. S. Anashin. Uniformly distributed sequences of *p*-adic integers, II. *Discrete Math. Appl.*, 12(6):527–590, 2002.

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

[8] Vladimir Anashin, Andrey Bogdanov, and Ilya Kizhvatov. ABC: A New Fast Flexible Stream Cipher, Version 3. Technical report, eSTREAM, 2005. Available from `http://www.ecrypt.eu.org/stream/p2ciphers/abc/abc_p2.pdf`.

[9] Vladimir Anashin, Andrey Bogdanov, and Ilya Kizhvatov. ABC: A New Fast Flexible Stream Cipher, Version 2. Technical report, eSTREAM, 2005. Available from `http://crypto.rsuh.ru/papers/abc-spec-v2.pdf`.

[10] Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, and Sandeep Kumar. ABC : A New Fast Flexible Stream cipher. Technical Report 2005/001, eSTREAM, 2005. Available from `http://eprint.iacr.org/`.

[11] Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, and Sandeep Kumar. ABC Is Safe And Sound. *Cryptology ePrint Archive*, 2006. Available from `http://www.ecrypt.eu.org/stream/papersdir/079.pdf`.

[12] Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, and Sandeep Kumar. Security and Implementation Properties of ABC v.2. Technical Report 2006/026, eSTREAM, 2006. Available from `http://www.ecrypt.eu.org/stream/papersdir/2006/026.pdf`.

[13] F. Durand and F. Paccaut. Minimal polynomial dynamics on the set of 3-adic integers. *Bull. London Math. Soc.*, 41(2):302–314, 2009.

[14] J. Hong, D. Lee, Y. Yeom, and D. Han. A new class of single cycle T-functions. In *Fast Software Encryption*, volume 3557 of *Lect. Notes Comp. Sci.*, pages 68–82. Springer-Verlag, 2005.

[15] Jin Hong, Dong Hoon Lee, Yongjin Yeom, and Daewan Han. T-function based stream cipher TSC-3. Technical Report 2005/031, eSTREAM, 2005. Available from `http://www.ecrypt.eu.org/stream/ciphers/tsc3/tsc3.pdf`.

[16] A. Klimov and A. Shamir. Cryptographic applications of T-functions. In *Selected Areas in Cryptography*, volume 3006, pages 248–261, 2003.

[17] A. Klimov and A. Shamir. A new class of invertible mappings. In B.S.Kaliski Jr.et al., editor, *Cryptographic Hardware and Embedded Systems 2002*, volume 2523 of *Lect. Notes in Comp. Sci*, pages 470–483. Springer-Verlag, 2003.

[18] A. Klimov and A. Shamir. New cryptographic primitives based on multiword T-functions. In *Fast Software Encryption*, 2004.

[19] A. Klimov and A. Shamir. The TF-i family of stream ciphers. Handout distributed at: The State of the Art of Stream Ciphers SASC, 2004.

[20] Alexander Klimov. *Applications of T-functions in Cryptography*. PhD thesis, Weizmann Institute of Science, 2005. Available from `http://www.wisdom.weizmann.ac.il/~ask/`.

[21] Alexander Klimov and Adi Shamir. New applications of T-functions in block ciphers and hash functions. In Henri Gilbert and Helena Handschuh, editors, *Fast Software Encryption*, volume 3557 of *Lecture Notes in Computer Science*, pages 18–31. Springer, 2005.

[22] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate texts in math.* Springer-Verlag, second edition, 1984.

[23] N. Kolokotronis. Cryptographic properties of nonlinear pseudorandom number generators. *Designs, Codes and Cryptography*, 46:353–363, 2008.

[24] L. Kotomina. Fast nonlinear congruential generators. Master's thesis, Russian State University for the Humanities, Moscow, 1999. In Russian.

[25] M. V. Larin. Transitive polynomial transformations of residue class rings. *Discrete Mathematics and Applications*, 12(2):141–154, 2002.

[26] Synaptic Laboratories Limited. The VEST cryptosystem for semiconductors. `http://www.vestciphers.com/en/index.html`.

[27] Yong Long Luo and Wen-Feng Qui. On the algebraic structure of Klimov-Shamir T-function. *Journal on Communications*, 29(10), 2008. In Chinese.

[28] K. Mahler. *p-adic numbers and their functions*. Cambridge Univ. Press, 1981. (2nd edition).

[29] Alexander Maximov. A new stream cipher Mir-1. Technical Report 2005/017, eSTREAM, 2005. Available from http://www.ecrypt.eu.org/stream.

[30] Håvard Molland and Tor Helleseth. A linear weakness in the Klimov-Shamir T-function. In *Proc. 2005 IEEE Int. Symp. on Information Theory*, pages 1106–1110, 2005.

[31] Håvard Molland and Tor Helleseth. Linear properties in T-functions. *IEEE Trans. Inf. Theory*, 52(11):5151–5157, 2006.

[32] Dukjae Moon, Daesung Kwon, Daewan Han, Jooyoung Lee, Gwon Ho Ryu, Dong Wook Lee, Yongjin Yeom, and Seongtaek Chee. T-function based stream cipher TSC-4. Technical Report 2006/024, eSTREAM, 2006. Available from http://www.ecrypt.eu.org/stream/papersdir/2006/024.pdf.

[33] F. Muller and T. Peyrin. Linear cryptanalysis of the TSC family of stream ciphers. In *ASIACRYPT*, volume 3788 of *Lect. Notes. Comp. Sci.*, pages 373–394. Springer, 2005.

[34] Sean O'Neil, Benjamin Gittins, and Howard Landman. VEST. Technical report, eSTREAM, 2006. Available from http://www.ecrypt.eu.org/stream/vestp2.html.

[35] S. V. Rykov. On properties of Klimov-Shamir pseudorandom number generator. *Discrete Math. Appl.*, 2011. In press.

[36] W. H. Schikhof. *Ultrametric calculus*. Cambridge University Press, 1984.

[37] A. Shamir and B. Tsaban. Guaranteeing the diversity of number generators. *Information and Computation*, 171:350–363, 2001.

[38] Jin-Song Wang and Wen-Feng Qi. Linear equation on polynomial single cycle T-function. In Dingyi Pei et al., editor, *Inscrypt 2007*, volume 4990 of *Lect. Notes Comp. Sci.*, pages 256–270, Berlin–Hedelberg, 2008. Springer Verlag.

[39] Kai-Thorsten Wirt. ASC A Stream Cipher with BuiltIn MAC Functionality. In *Proc. World Acad. Sci. Engineering and Technology*, volume 23, 2007.

[40] Haina Zhang and Xiaoyun Wang. Differential cryptanalysis of T-function based stream cipher TSC-4. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC*, volume 4817 of *Lect. Notes Comp. Sci.*, pages 227–238. Springer, 2007.

[41] Wenying Zhang and Chuan-Kun Wu. The algebraic normal form, linear complexity and k-error linear complexity of single-cycle T-function. In G. Gong et al., editor, *SETA 2006*, volume 4086 of *Lect. Notes Comp. Sci.*, pages 391–401, Berlin–Heidelberg, 2006. Springer-Verlag.

Appendix A. Proofs of Theorems 5 and 6

During the proofs, we will need the following

Lemma 1. *Let f be a transitive T-function, and let f be uniformly differentiable modulo 4, then*

$$\left(f^{2^{N_2(f)}}(z)\right)'_2 \equiv \prod_{j=0}^{2^{N_2(f)}-1} f'_2(f^j(z)) \equiv 1 \pmod 4,$$

for every $z \in \mathbb{Z}_2$.

Proof of Lemma 1. The left-side congruence immediately follows from the chain rule; the right-side congruence is proved in [3], see the end of the proof of Theorem 4.55 there. It is worth noticing that we actually prove both congruences while proving Theorem 6, see Step 5 in the proof of the latter. □

A.1. **Proof of Theorem 5.** From the transitivity of the T-function f (see Definition 6) it follows that $f^{2^{n-1}}(x) \equiv x \pmod{2^{n-1}}$; that is

$$(A.1) \qquad\qquad f^{2^{n-1}}(x) = x + 2^{n-1}\varphi(x)$$

for a suitable map $\varphi \colon \mathbb{Z}_2 \to \mathbb{Z}_2$. As f is uniformly differentiable modulo 4, from (A.1) we deduce that

$$(A.2) \qquad f^{i+2^{n-1}}(x) = f^i(f^{2^{n-1}}(x)) = f^i(x + 2^{n-1}\varphi(x)) \equiv f^i(x) + 2^{n-1}\varphi(x)(f^i(x))'_2 \pmod{2^{n+1}}$$

once $n \geq N_2(f) + 1$.

Further, $\varphi(x) \equiv \alpha(x) + 2\beta(x) \pmod 4$ where $\alpha \colon \mathbb{Z}_2 \to \mathbb{F}_2 = \{0,1\}$. We claim that $\alpha(x) = 1$ for all $x \in \mathbb{Z}_2$. Indeed, if otherwise, then (A.1) implies that

$$f^{2^{n-1}}(x) = x + 2^n\beta(x) \equiv x \pmod{2^n},$$

in a contradiction to the transitivity of f as necessarily $f^{2^{n-1}}(x) \not\equiv x \pmod{2^n}$ whenever f is transitive, see Definition 6. Thus, given $x \in \mathbb{Z}_2$,

$$(A.3) \qquad\qquad \varphi(x) \equiv 1 + 2\beta \pmod 4,$$

for a suitable $\beta = \beta(x) \in \mathbb{Z}_2$.

As f is bijective, $f'_2(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$, see Proposition 2. This in view of (A.2) and (A.3) implies that if we denote $(f^i(x))'_2 \equiv 1 + 2\gamma \pmod 4$ for a suitable $\gamma = \gamma(i;x) \in \{0,1\}$, then

$$(A.4) \ \ f^{i+2^{n-1}}(x) \equiv f^i(x) + 2^{n-1}(1+2\beta)(1+2\gamma) \pmod{2^{n+1}} \equiv f^i(x) + 2^{n-1} + 2^n(\beta+\gamma) \pmod{2^{n+1}}.$$

Remind that $\chi_j^\ell = \delta_j(f^\ell(x)) \in \{0,1\}$ $(j,\ell = 0,1,2,\ldots)$ according to our notation. With the notation, given $x = x_0 \in \mathbb{Z}_2$, the transitivity of f implies that

$$(A.5) \quad f^{2^{n-1}}(\chi_0^0 + \chi_1^0 \cdot 2 + \cdots) \equiv \chi_0^{2^{n-1}} + \chi_1^{2^{n-1}} \cdot 2 + \cdots + \chi_{n-1}^{2^{n-1}} \cdot 2^{n-1} + \chi_n^{2^{n-1}} \cdot 2^n \equiv$$
$$\chi_0^{2^{n-1}} + \chi_1^{2^{n-1}} \cdot 2 + \cdots + \chi_{n-2}^{2^{n-1}} \cdot 2^{n-2} + (\chi_{n-1}^0 \oplus 1) \cdot 2^{n-1} + \chi_n^{2^{n-1}} \cdot 2^n \quad (\text{mod } 2^{n+1}),$$

where $\oplus$ stands for addition modulo 2. On the other hand,

$$f^{2^{n-1}}(\chi_0^0 + \chi_1^0 \cdot 2 + \cdots) \equiv \chi_0^0 + \chi_1^0 \cdot 2 + \cdots + \chi_n^0 \cdot 2^n + 2^{n-1} + 2^n \beta \quad (\text{mod } 2^{n+1})$$

in view of (A.1) and (A.3). Comparing both congruences, we conclude that $\chi_n^{2^{n-1}} \equiv \chi_{n-1}^0 + \chi_n^0 + \beta \pmod 2$; finally,

$$(A.6) \qquad\qquad \beta \equiv \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} \pmod 2.$$

Now from (A.4), (A.5), (A.6) we obtain:

$$\chi_0^{i+2^{n-1}} + \chi_1^{i+2^{n-1}} \cdot 2 + \cdots + \chi_{n-1}^{i+2^{n-1}} \cdot 2^{n-1} + \chi_n^{i+2^{n-1}} \cdot 2^n \equiv$$
$$\chi_0^i + \chi_1^i \cdot 2 + \cdots + \chi_n^i \cdot 2^n + 2^{n-1} + (\chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + \gamma)2^n \quad (\text{mod } 2^{n+1});$$

henceforth,

$$(A.7) \qquad\qquad \chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^i + \chi_n^i + \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + \gamma \pmod 2.$$

Note that the term χ_{n-1}^i occurs in the right side due to the carry.

Now take (and fix) arbitrary $x = x_0 \in \mathbb{Z}_2$. We claim that the function $y(i) = \gamma(i; x)$ is periodic with respect to the variable $i = 0, 1, 2, \ldots$, and that the length of the shortest period of $y(i)$ is a factor of $2^{N_2(f)}$.

Denote $N = N_2(f)$. As $y(\ell) = \delta_1((f^\ell(x))_2')$ by the definition, $y(\ell)$ can not depend on n once $n \geq N+1$; furthermost, we have that $y(i + 2^N) = \delta_1((f^{i+2^N}(x))_2')$. Using sequentially chain rule and Lemma 1 for $z = f^i(x)$ we get:

$$(f^{i+2^N}(x))_2' \equiv \prod_{j=0}^{i+2^N-1} f_2'(f^j(x)) \equiv \prod_{j=0}^{i-1} f_2'(f^j(x)) \prod_{j=0}^{2^N-1} f_2'(f^{j+i}(x)) \equiv \prod_{j=0}^{i-1} f_2'(f^j(x)) \equiv (f^i(x))_2' \quad (\text{mod } 4).$$

Therefore, $y(i + 2^N) = \delta_1((f^{i+2^N}(x))_2') = \delta_1((f^i(x))_2') = y(i)$. This proves our claim and Theorem 5. $\qquad\square$

A.2. **Proof of Theorem 6.** The proof mimics respective steps of the proof of Theorem 5.

<u>Step 1:</u> As $f^{2^{n-2}}(x) = x + 2^{n-2}\varphi(x)$ for a suitable map $\varphi \colon \mathbb{Z}_2 \to \mathbb{Z}_2$, given $n \geq N_3(f) + 2$ we have that

$$(A.8) \qquad\qquad f^{i+2^{n-2}}(x) \equiv f^i(x) + 2^{n-2}\varphi(x)(f^i(x))_3' \pmod{2^{n+1}},$$

cf. (A.1) and (A.2).

<u>Step 2:</u> Denote $\varphi(x) \equiv \alpha + 2\beta + 4\gamma \pmod 8$, for suitable $\alpha, \beta, \gamma \in \{0,1\}$. We prove that $\alpha = 1$ exactly in the same way as in the proof of Theorem 5.

<u>Step 3:</u> We have then that $(f^i(x))_3' = 1 + 2\lambda + 4\eta \pmod 8$, for suitable $\lambda, \eta \in \{0,1\}$. Therefore,

$$(A.9) \quad f^{i+2^{n-2}}(x) = f^i(f^{2^{n-2}}(x)) = f^i(x + 2^{n-2}\varphi(x)) \equiv$$
$$f^i(x) + 2^{n-2} + 2^{n-1}(\beta + \lambda) + 2^n(\beta\lambda + \gamma + \eta) \quad (\text{mod } 2^{n+1}),$$

cf. (A.4).

<u>Step 4:</u> Now we act as in the proof of (A.7). On the one hand,

$$(A.10) \quad f^{2^{n-2}}(\chi_0^0 + \chi_1^0 \cdot 2 + \cdots) \equiv \chi_0^{2^{n-2}} + \chi_1^{2^{n-2}} \cdot 2 + \cdots + \chi_{n-1}^{2^{n-2}} \cdot 2^{n-1} + \chi_n^{2^{n-2}} \cdot 2^n$$
$$\equiv \chi_0^{2^{n-2}} + \chi_1^{2^{n-2}} \cdot 2 + \cdots + (\chi_{n-2}^0 \oplus 1) \cdot 2^{n-2} + \chi_{n-1}^{2^{n-2}} \cdot 2^{n-1} + \chi_n^{2^{n-2}} \cdot 2^n \quad (\text{mod } 2^{n+1}),$$

while on the other hand,

$$f^{2^{n-2}}(\chi_0^0 + \chi_1^0 \cdot 2 + \cdots) \equiv \chi_0^0 + \chi_1^0 \cdot 2 + \cdots + \chi_n^0 \cdot 2^n + 2^{n-2} + 2^{n-1}\beta + 2^n\gamma \quad (\text{mod } 2^{n+1}).$$

From here we deduce that $\chi_{n-1}^{2^{n-2}} = \chi_{n-1}^0 \oplus \chi_{n-2}^0 \oplus \beta$; henceforth

$$(A.11) \qquad\qquad\qquad \beta \equiv \chi_{n-1}^0 + \chi_{n-2}^0 + \chi_{n-1}^{2^{n-2}} \pmod 2,$$

cf. (A.6). Now, combining together (A.9),(A.10), (A.11), we get

$$\chi_0^{i+2^{n-2}} + \chi_1^{i+2^{n-2}} \cdot 2 + \cdots + \chi_{n-1}^{i+2^{n-2}} \cdot 2^{n-1} + \chi_n^{i+2^{n-2}} \cdot 2^n \equiv$$

$$\chi_0^i + \chi_1^i \cdot 2 + \cdots + \chi_n^i \cdot 2^n + 2^{n-2} + 2^{n-1}(\chi_{n-2}^0 + \chi_{n-1}^0 + \chi_{n-1}^{2^{n-2}} + \lambda) + 2^n(\beta\lambda + \gamma + \eta) \pmod{2^{n+1}};$$

so we conclude that

$$\chi_{n-1}^{i+2^{n-2}} \equiv \chi_{n-2}^i + \chi_{n-1}^i + \chi_{n-2}^0 + \chi_{n-1}^0 + \chi_{n-1}^{2^{n-2}} + \lambda \pmod 2$$

and that

$$\chi_n^{i+2^{n-2}} \equiv \chi_{n-2}^i \chi_{n-1}^i + \chi_{n-2}^i(\chi_{n-2}^0 + \chi_{n-1}^0 + \chi_{n-1}^{2^{n-2}} + \lambda) + \chi_{n-1}^i(\chi_{n-2}^0 + \chi_{n-1}^0 + \chi_{n-1}^{2^{n-2}} + \lambda) + \chi_n^i + \beta\lambda + \gamma + \eta \pmod 2.$$

From here we finally obtain that

$$\chi_n^{i+2^{n-2}} \equiv \chi_{n-2}^i \chi_{n-1}^i + \theta(n)(\chi_{n-2}^i + \chi_{n-1}^i) + \chi_n^i + y_i \pmod 2,$$

where $\theta(n) \equiv \chi_{n-2}^0 + \chi_{n-1}^0 + \chi_{n-1}^{2^{n-2}} + \lambda \pmod 2$ and $y_i \equiv \beta\lambda + \gamma + \eta \pmod 2$.

Step 5: Take and fix arbitrary $x \in \mathbb{Z}_2$ and $n \geq N_3(f) + 2$; therefore we fix $\beta, \gamma \in \{0, 1\}$, however, both β and γ depend on n. We claim that the binary sequence $(y_i)_{i=0}^\infty$ is periodic, and that the length of its shortest period is a factor of $2^{N_3(f)}$.

Indeed, by the chain rule

$$(A.12) \qquad\qquad\qquad \left(f^\ell(z)\right)_3' \equiv \prod_{j=0}^{\ell-1} f_3'(f^j(x)) \pmod 8,$$

for arbitrary $z \in \mathbb{Z}_2$ and $\ell = 1, 2, \ldots$. As f is a transitive T-function, $f^{i+2^{N_3(f)}}(x) = f^i(x + 2^{N_3(f)}\Phi(x))$ for a suitable $\Phi \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ (cf. (A.1) and (A.2)); and moreover,

$$f^j(x + 2^{N_3(f)}\Phi(x)) = f^j(x) \bmod 2^{N_3(f)} + 2^{N_3(f)}\widetilde{\Phi}_j(x),$$

where $f^j(x) \bmod 2^{N_3(f)}$ stands for the least non-negative residue of $f^j(x)$ modulo $2^{N_3(f)}$ and $\widetilde{\Phi}_j(x) \in \mathbb{Z}_2$. Now combining the latter equality with (A.12) we see that

$$(A.13) \quad \left(f^{i+2^{N_3(f)}}(x)\right)_3' = \left(f^i(x + 2^{N_3(f)}\Phi(x))\right)_3' \equiv \prod_{j=0}^{i-1} f_2'\left(f^j(x + 2^{N_3(f)}\Phi(x))\right) \equiv$$

$$\prod_{j=0}^{i-1} f_2'\left(f^j(x) \bmod 2^{N_3(f)} + 2^{N_3(f)}\widetilde{\Phi}_j(x)\right) \equiv \prod_{j=0}^{i-1} f_2'\left(f^j(x) \bmod 2^{N_3(f)}\right) \equiv \left(f^i(x)\right)_3' \pmod 8,$$

as $f_2'(x)$ is a periodic function with a period of length $2^{N_3(f)}$, cf. Proposition 1.

Now, as $\lambda = \delta_1((f^i(x))_3')$ and $\eta = \delta_2((f^i(x))_3')$ the functions $\lambda = \lambda(i)$ and $\eta = \eta(i)$ are periodic with respect to the variable $i = 0, 1, 2 \ldots$, and lengths of their shortest periods are factors of $2^{N_3(f)}$. Consequently, the sequence $(y_i)_{i=0}^\infty$ is periodic, and the length of its shortest period is 2^K for some $0 \leq K \leq N_3(f)$. $\qquad\square$

Current address, Tao Shi: The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R.China, And Graduate University of Chinese Academy of Sciences, Beijing 100049, P.R.China
E-mail address, Tao Shi: `shitao@is.iscas.ac.cn`

Current address, Vladimir Anashin: Institute for Information Security, Moscow State University, 119991, Moscow, Russia
E-mail address, Vladimir Anashin: `anashin@iisi.msu.ru; vladimir.anashin@u-picardie.fr`

Current address, Dongdai Lin: The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R.China
E-mail address, Dongdai Lin: `ddlin@is.iscas.ac.cn`