mathematics

MDPI

Article

Representations of Generalized Self-Shrunken Sequences

Sara D. Cardell [1], Joan-Josep Climent [2], Amparo Fúster-Sabater [3,*] and Verónica Requena [2]

1 Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas 13083-859, Sao Paulo, Brazil; scardell@unicamp.br
2 Departament de Matemàtiques, Universitat d'Alacant, E-03690 Alacant, Spain; jcliment@ua.es (J.-J.C.); vrequena@ua.es (V.R.)
3 Instituto de Tecnologías Físicas y de la Información, C.S.I.C., E-28006 Madrid, Spain
* Correspondence: amparo@iec.csic.es

Received: 26 May 2020; Accepted: 15 June 2020; Published: 19 June 2020

Abstract: Output sequences of the cryptographic pseudo-random number generator, known as the generalized self-shrinking generator, are obtained self-decimating Pseudo-Noise (PN)-sequences with shifted versions of themselves. In this paper, we present three different representations of this family of sequences. Two of them, the p and G-representations, are based on the parameters p and G corresponding to shifts and binary vectors, respectively, used to compute the shifted versions of the original PN-sequence. In addition, such sequences can be also computed as the binary sum of diagonals of the Sierpinski's triangle. This is called the B-representation. Characteristics and generalities of the three representations are analyzed in detail. Under such representations, we determine some properties of these cryptographic sequences. Furthermore, these sequences form a family that has a group structure with the bit-wise XOR operation.

Keywords: generalized self-shrinking generator; PN-sequence; binomial sequence; additive group; coset

1. Introduction

Most of the devices that form part of the Internet-of-Things (IoT) require cryptographic security features to prevent users from data losses and the risks related to an improper use of passwords. Putting into effect cryptographic security is complicated. Most of the security systems are based on true random numbers, but their generation is really a difficult task [1,2]. Many popular random "noise" algorithms, for example, algorithms that are part of IoT devices, end up to be imperfect, showing glitches that make them predictable and vulnerable. Some weaknesses are never (publicly) found out, creating a false sense of security. The devices in which flaws are detected are those with the most flagrant errors and those most popular, for example, algorithms A5 in GSM communications cryptanalyzed in [3,4], the generator RC4 for encrypting Internet traffic cryptanalyzed in [5] or the J3Gen generator for low-cost passive RFID tags cryptanalyzed in [6]. To sum up, it is hard to build a true random number generator that can provide a strong cryptographic foundation for system security, especially for IoT devices (see [7,8]).

Pseudo-Random Number Generators (PRNGs) are reproducible and deterministic algorithms [9,10] used to generate random number sequences for cryptographic applications, such as key and nonces generation, digital signatures, and IoT security. These applications require various statistical properties, such as low autocorrelation, large period and linear complexity, rich dimensional distribution of the output sequence, and uniformity of distribution for large quantities of generated numbers (see ([11], Chapter 2) for more details).

Binary sequences produced by maximal-length Linear Feedback Shift Registers (LFSRs), called Pseudo-Noise (PN)-sequences [12], have been widely used in many diverse applications such as digital

broadcasting, mobile wireless communications, e-commerce or cryptography (stream ciphers) [13,14]. In order to ensure practical cryptographic stability, it is necessary to destroy the linearity inherent to PN-sequences via different non-linear procedures.

LFSRs play an important role in the design of cryptographic PRNGs [15,16]. Among the most popular families of cryptographic sequence generators based on PN-sequences we can enumerate: non-linear filters with only one LFSR, combination generators that involve several LFSRs, clock-controlled registers where one LFSR controls the clock of the others or irregular decimation-based generators [11]. We focus our attention on this latter family.

Generally speaking, the regular decimation [17] of a sequence $\{a_i\}_{i\geq 0}$ by distance d is a new sequence obtained by taking every d-th term of $\{a_i\}_{i\geq 0}$, that is, $\{a_{d\cdot i}\}_{i\geq 0}$. Nevertheless, it is the irregular decimation of PN-sequences [18], which can be considered as a powerful PRNG, producing sequences with good cryptographic properties, such as long periods, good distribution of zeros and ones along the sequence, large linear complexity, and two-valued autocorrelation properties.

In the literature, there are three well-known irregularly decimated generators: the **shrinking generator** [19], made up of two LFSRs with different lengths, the **self-shrinking generator** [20], based on the self-decimation of one single PN-sequence, and the **generalized self-shrinking generator (GSSG)** [21], which produces a family of sequences that includes the sequence produced by the self-shrinking generator [22]. Moreover, the modified self-shrinking generator [23] and the t-modified self-shrinking generator [24] are also members of such a family. These generators are fast, easy to implement and they generate good cryptographic sequences. Therefore, they seem adequate for lightweight cryptography and, in general, low-cost applications. In [25], the authors studied the randomness of the family of sequences generated by the GSSG by means of several complete and powerful batteries of statistical tests and graphical tools. In fact, they provided a useful vision of the behavior of such sequences and proved their suitability for cryptographic applications. In [24], the relationship among the generalized self-shrinking generator and the t-modified self-shrinking generator is deeply analyzed. Furthermore, in [26], the authors studied the relationship between that generator and the modified self-shrinking generator. In [27], other authors presented an extension of the self-shrinking generator to the Galois field of p^n elements with p a prime integer, that is, the p-ary Generalized Self-Shrinking Generator (p-GSSG). Furthermore, they proved that the sequences generated by this new generator have large periods and good statistical properties.

At any rate, there exist other ways to built irregularly decimated generators, for example, irregularly decimated generators based on Feedback with Carry Shift Registers (FCSRs) instead of the traditional LFSRs [28,29]. These variants of the previous generators unify in a unique structure the non-linearity inherent to the FCSRs with the irregular decimation technique. An FCSR is the arithmetic or with carry analog of an LFSR. The main difference is the fact that the elementary additions are not modulo 2 additions but with the propagation of carries. FCSRs have been used in the design of stream ciphers [30], generating pseudo-random numbers [31], and can be efficiently implemented in parallel architectures [32].

In modern algebra, group theory is the study of groups, which are sets of elements with an operation that satisfies certain axioms. The basic structure of groups can be found in many mathematical phenomena such as symmetry and certain types of transformations. Group theory has applications in robotics, computer vision/graphics and medical image analysis, physics, chemistry, computer science, and even puzzles like Rubik's cube can be represented using group theory [33–37]. As we show in this paper, group theory also has applications in cryptography, since the set of output sequences of the generalized self-shrinking generator has the structure of an additive group and some of the properties of this family of sequences can be deduced as a consequence of this fact.

In this work, we study in detail three different representations of the sequences produced by the GSSG: the G-representation (introduced in [21]), the new p-representation and the B-representation (introduced in [38]). As far as we know, there are no other known representations for this kind of generators in the literature. In addition, we introduce a new way to compute the B-representation. Such a representation relates the output sequences of our generator with shifted versions of the diagonals of

the binary Sierpinski's triangle, named binomial sequences. In terms of this representation, the structural properties of some binary sequences are easily analyzed. In brief, we give a binomial expression of these sequences, providing a relation among binomial coefficients, binary sequences and group theory.

2. Fundamentals and Basic Notation

In this section, we introduce some of the main concepts related to our work: the generalized self-shrinking generator and the binomial sequences.

2.1. PN-Sequences and GSSG

Traditionally, LFSRs implement linear recurring sequences [12]. LFSRs are electronic devices in which the information units are elements of binary field $\mathbb{F}_2$. They are made up of r interconnected memory cells (stages) that shift their contents to their next stages and a linear feedback to the empty stage. The register is shown in Figure 1.

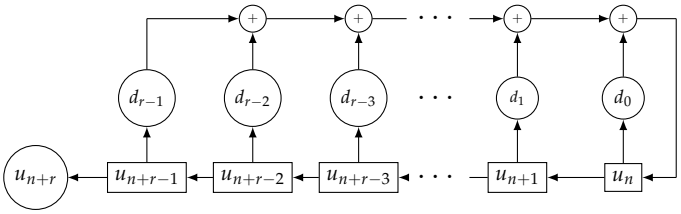

Figure 1. Linear Feedback Shift Registers (LFSR) of length r.

Generates the linear recurring sequence $\{u_n\}_{n\geq 0}$ (or denoted by $\{u_n\}$) given by

$$u_{n+r} = d_{r-1}u_{n+r-1} + d_{r-2}u_{n+r-2} + d_{r-3}u_{n+r-3} + \cdots + d_1u_{n+1} + d_0u_n, \quad n \geq 0.$$

If the monic polynomial

$$p(x) = x^r + d_{r-1}x^{r-1} + d_{r-2}x^{r-2} + d_{r-3}x^{r-3} + \cdots + d_1x + d_0 \in \mathbb{F}_2[x]$$

is a primitive polynomial, then the LFSR is called a **maximal-length LFSR** [12] and generates a **PN-sequence** (Pseudo Noise sequence) with maximum **period** $T = 2^r - 1$ with 2^{r-1} ones and $2^{r-1} - 1$ zeros. This polynomial is known as the **characteristic polynomial** of the recurring sequence.

A common metric of the security of a sequence for its possible cryptographic application is the **linear complexity** [39–41], denoted by LC. Roughly speaking, the parameter LC determines the portion of sequence we need in order to recover the whole sequence. In fact, LC is the length of the shortest LFSR that generates such a sequence ([42], Chapter 5). Making use of the concept of recurrence, we can say that the LC of a sequence is the lowest order of its linear recurrence relationship. In cryptography, linear complexity clearly must take a large value, for example, half of the period: $LC \simeq T/2$. Nowadays, values of T in the range $T \geq 2^{128}$ seem to be enough for cryptographic purposes (see specifications of the candidates in the call of NIST for lightweight cryptography primitives [43]).

Consider a PN-sequence $\{u_i\}_{i\geq 0}$ obtained from a maximal-length LFSR with L stages, an L-dimensional binary vector $\mathcal{G} = [g_0, g_1, g_2, ..., g_{L-1}] \in \mathbb{F}_2^L$ and let $\{v_i\}_{i\geq 0}$ be the sequence defined as:

$$v_i = g_0u_i + g_1u_{i-1} + g_2u_{i-2} + \cdots + g_{L-1}u_{i-L+1} \quad \text{for } i \geq 0. \tag{1}$$

Next, we define a decimation rule to generate a new sequence $\{s_j\}_{j\geq 0}$ as follows:

$$\begin{cases} \text{If } u_i = 1, & \text{then } s_j = v_i, \\ \text{If } u_i = 0, & \text{then } v_i \text{ is discarded.} \end{cases} \tag{2}$$

The sequence $\{s_j\}_{i\geq 0}$, denoted by $S(\mathcal{G})$, is called the **generalized self-shrunken sequence**, GSS-sequence or simply **generalized sequence** associated with $\mathcal{G}$, see [21]; and the sequence generator is called the **generalized self-shrinking generator** (GSSG).

Notice that when $\mathcal{G}$ runs over $\mathbb{F}_2^L \setminus \{\mathbf{0}\}$ we obtain all the shifted versions of $\{u_i\}_{i\geq 0}$ (see Theorem 2). The set of sequences $\mathcal{S} = \{S(\mathcal{G}) \mid \mathcal{G} \in \mathbb{F}_2^L\}$ is called the **family of generalized sequences** based on the PN-sequence $\{u_i\}_{i\geq 0}$. This family $\mathcal{S}$ with the addition modulo 2, that is, with the bit-wise XOR operation, is an additive group [21]. In particular, the neutral element is the sequence $S([0,0,\ldots,0]) = \{0\,0\,0\,0\,0\ldots\}$ and the opposite of any sequence $S(\mathcal{G})$ is the sequence itself. Moreover, the period of every generalized sequence is a divisor of 2^{L-1} (the number of ones in the PN-sequence) and every sequence of this family is balanced except for the sequence identically of 1 and the null sequence ([21], Theorem 1).

Example 1. *Consider the primitive polynomial* $p(x) = x^3 + x^2 + 1$ *and the PN-sequence* $\{u_i\}_{i\geq 0} = \{1\,1\,1\,0\,1\,0\,0\}$ *generated by* $p(x)$ *with initial state* $\{1\,1\,1\}$. *As illustration of the decimation rule given in (2) consider, for instance,* $\mathcal{G} = [0,0,1]$ *and the corresponding sequence* $\{v_i\}_{i\geq 0} = \{0\,0\,1\,1\,1\,0\,1\}$. *We apply the decimation rule as follows:*

$$\begin{array}{lccccccc} \{u_i\}: & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ \{v_i\}: & 0 & 0 & 1 & \not{1} & 1 & \not{0} & \not{1} \\ \{s_j\}: & \mathbf{0} & \mathbf{0} & \mathbf{1} & & \mathbf{1} & & \end{array}$$

The corresponding generalized sequence is $S([0,0,1]) = \{0\,0\,1\,1\}$.

In Table 1, we can see the family of all generalized sequences generated by the PN-sequence $\{u_i\}_{i\geq 0}$. *Notice that the* $\{v_i\}_{i\geq 0}$ *sequences are shifted versions of the PN-sequence* $\{u_i\}$ *(which appears at the bottom of the table), a fact that we will prove later in Theorem 2. The bits in bold of each sequence* $\{v_i\}_{i\geq 0}$ *are the bits of the corresponding generalized sequence.*

Table 1. Generalized sequences for $p(x) = x^3 + x^2 + 1$.

$\mathcal{G}$	$\{v_i\}$ Sequence	Generalized Sequences
000	**000**0000	0000
001	**001**1101	0011
010	**011**1010	0110
011	**010**0111	0101
100	**111**0100	1111
101	**110**1001	1100
110	**100**1110	1001
111	**101**0011	1010
	1110100	

Notice that, since the number of ones in a PN-sequence of period $2^L - 1$ is 2^{L-1} (see [12]), the period of the generalized sequences is a divisor of 2^{L-1}. We will see that there are always two sequences of period 1 (the identically 1 and 0 sequences), two sequences of period 2, $\{0\,1\,0\,1\,0\,1\,0\,1\}$ and $\{1\,0\,1\,0\,1\,0\,1\,0\,1\}$, and the remaining sequences have the maximum period 2^{L-1} (although there is no mathematical proof for this last statement).

Relating to the linear complexity, in [39] Blackburn introduced an upper bound for the linear complexity of the self-shrinking generator. A generalization of this bound was introduced in [40] for the linear complexity of generalized sequences, that is, $LC \leq 2^{L-1} - (L-2)$. Furthermore, we know that for all generalized sequences, except for those with period 1 and 2, we have $2^{L-2} \leq LC$ (although there is no proof for this statement either).

2.2. Binomial Sequences

The binomial number $\binom{n}{i}$ represents the coefficient corresponding to x^i in the expansion of the polynomial $(1+x)^n$. For every integer $n \geq 0$, we know that $\binom{n}{0} = 1$ while $\binom{n}{i} = 0$ for $i > n$. Now, binomial sequences are introduced as follows.

Definition 1. *Given a fixed integer $k \geq 0$, the sequence $\left\{b_n^{(k)}\right\}_{n\geq 0}$ given by*

$$b_n^{(k)} = \begin{cases} 0, & \text{if } n < k, \\ \binom{n}{k} \bmod 2, & \text{if } n \geq k, \end{cases}$$

*is named the **k-th binomial sequence**.*

In the sequel, the sequence $\left\{b_n^{(k)}\right\}_{n\geq 0}$ will be simply denoted by $\left\{\binom{n}{k}\right\}$. Table 2 shows the first eight binomial coefficients as well as the first eight binomial sequences with their corresponding periods and linear complexities. To check the form of the first 32 binomial sequences, see reference [38]. Moreover, recall that binomial sequences are just shifted versions of the successive diagonals of the Sierpinski's triangle depicted in Figure 2.

Table 2. The first 8 binomial coefficients, their binomial sequences $\left\{\binom{n}{k}\right\}$, periods and complexities.

Binomial Coeff.	Binomial Sequences $\left\{\binom{n}{k}\right\}$	Period	*LC*
$\binom{n}{0}$	11111111...	1	1
$\binom{n}{1}$	01010101...	2	2
$\binom{n}{2}$	00110011...	4	3
$\binom{n}{3}$	00010001...	4	4
$\binom{n}{4}$	00001111...	8	5
$\binom{n}{5}$	00000101...	8	6
$\binom{n}{6}$	00000011...	8	7
$\binom{n}{7}$	00000001...	8	8

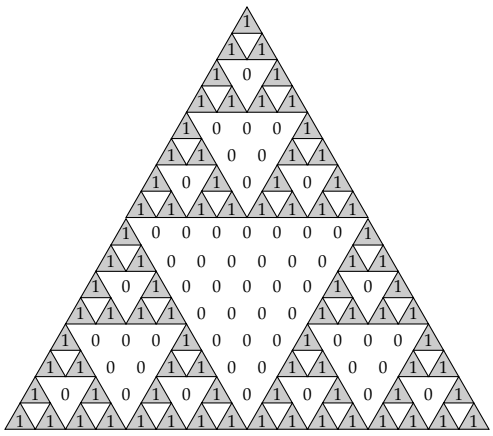

Figure 2. Sierpinski's triangle.

Theorem 1 ([38], Proposition 3, Theorem 13)**.** *The binomial sequence $\left\{\binom{n}{2^r+l}\right\}$ with $0 \leq l < 2^r$ and r being a positive integer has period of value $T = 2^{r+1}$ and linear complexity of value $LC = 2^r + l + 1$.*

Check [38] for more properties of binomial sequences.

3. Representation of Generalized Sequences

In this section, we present three different representations of the generalized self-shrunken sequences. From these representations we can obtain important information about the sequences. For instance,

the binomial representation or B-representation of the generalized sequences allows us to examine the cryptographic parameters of these sequences and obtain their linear complexity; the p-representation and G-representation provide information about the shifted PN-sequences used in the decimation and allow us to define a partition of the family of generalized sequences.

It is worth saying that there exist certain advantages and disadvantages among these representations. On the one hand, the B-representation is more general and can be used for any binary sequence with a period of a power of two. On the other hand, the p-representation and the G-representation are specific representations for generalized sequences and, therefore, do not exist for other generators. However, both representations are related, being possible to get one from the other. In this section, we present some relations between the different representations.

3.1. The G-Representation of a Generalized Self-Shrunken Sequence

It is well known [12] that a PN-sequence $\{u_i\}_{i\geq 0}$ generated by an LFSR with primitive polynomial $p(x)$ of degree L can be represented by the trace map as follows

$$u_i = \mathrm{Tr}(A\alpha^i) = A\alpha^i + A^2\alpha^{2i} + A^4\alpha^{4i} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}i}, \quad i \geq 0, \tag{3}$$

where $A \in \mathbb{F}_{2^L}$ with $A \neq 0$ and α is a root of $p(x)$, that is, a primitive element of $\mathbb{F}_{2^L}$.

From now on, we consider $\{u_i\}_{i\geq 0}$ a PN-sequence obtained from a maximal-length LFSR with characteristic polynomial $p(x)$ of degree L.

Next theorem proves that the sequence $\{v_i\}_{i\geq 0}$ given in (1) is a shifted version of the PN-sequence $\{u_i\}_{i\geq 0}$.

Theorem 2. *Assume that $\{u_i\}_{i\geq 0}$ is a PN-sequence obtained from a maximal-length LFSR with characteristic polynomial $p(x)$ of degree L. If $\mathcal{G} = [g_0, g_1, \ldots, g_{L-1}] \in \mathbb{F}_2^L$ is a nonzero vector, then the sequence $\{v_i\}_{i\geq 0}$ obtained from Expression (1) is a shifted version of $\{u_i\}_{i\geq 0}$. In fact, $\{v_i\}_{i\geq 0} = \left\{u_{i-L+1+\tau(\mathcal{G})}\right\}_{i\geq 0}$, where $\tau(\mathcal{G}) \in \{0, 1, \ldots, 2^L - 2\}$ such that*

$$\alpha^{\tau(\mathcal{G})} = g_0\alpha^{L-1} + g_1\alpha^{L-2} + \cdots + g_{L-2}\alpha + g_{L-1} \in \mathbb{F}_{2^L}$$

with $\alpha \in \mathbb{F}_{2^L}$ being a root of $p(x)$.

Proof. From Expressions (1) and (3), it follows that

$$\begin{aligned}
v_i &= g_0\left(A\alpha^i + A^2\alpha^{2i} + A^4\alpha^{4i} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}i}\right)\\
&\quad + g_1\left(A\alpha^{i-1} + A^2\alpha^{2(i-1)} + A^4\alpha^{4(i-1)} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}(i-1)}\right)\\
&\quad + \cdots\\
&\quad + g_{L-2}\left(A\alpha^{i-L+2} + A^2\alpha^{2(i-L+2)} + A^4\alpha^{4(i-L+2)} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}(i-L+2)}\right)\\
&\quad + g_{L-1}\left(A\alpha^{i-L+1} + A^2\alpha^{2(i-L+1)} + A^4\alpha^{4(i-L+1)} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}(i-L+1)}\right)\\
&= A\left(\alpha^{i-L+1}\left(g_0\alpha^{L-1} + g_1\alpha^{i-2} + \cdots + g_{L-2}\alpha + g_{L-1}\right)\right)\\
&\quad + A^2\left(\alpha^{i-L+1}\left(g_0\alpha^{L-1} + g_1\alpha^{i-2} + \cdots + g_{L-2}\alpha + g_{L-1}\right)\right)^2\\
&\quad + A^4\left(\alpha^{i-L+1}\left(g_0\alpha^{L-1} + g_1\alpha^{i-2} + \cdots + g_{L-2}\alpha + g_{L-1}\right)\right)^4\\
&\quad + \cdots\\
&\quad + A^{2^{L-1}}\left(\alpha^{i-L+1}\left(g_0\alpha^{L-1} + g_1\alpha^{i-2} + \cdots + g_{L-2}\alpha + g_{L-1}\right)\right)^{2^{L-1}}\\
&= A\left(\alpha^{i-L+1}\alpha^{\tau(\mathcal{G})}\right) + A^2\left(\alpha^{i-L+1}\alpha^{\tau(\mathcal{G})}\right)^2 + A^4\left(\alpha^{i-L+1}\alpha^{\tau(\mathcal{G})}\right)^4 + \cdots + A^{2^{L-1}}\left(\alpha^{i-L+1}\alpha^{\tau(\mathcal{G})}\right)^{2^{L-1}}\\
&= A\left(\alpha^{i-L+1+\tau(\mathcal{G})}\right) + A^2\left(\alpha^{i-L+1+\tau(\mathcal{G})}\right)^2 + A^4\left(\alpha^{i-L+1+\tau(\mathcal{G})}\right)^4 + \cdots + A^{2^{L-1}}\left(\alpha^{i-L+1+\tau(\mathcal{G})}\right)^{2^{L-1}}\\
&= u_{i-L+1+\tau(\mathcal{G})}.
\end{aligned}$$

□

Note that if in Expression (1) we consider $\mathcal{G} = [0, 0, 0, \ldots, 0]$, then $\{v_i\}_{i\geq 0}$ is the null sequence.

From now on, we denote by G the decimal representation of the vector $\mathcal{G} = [g_0, g_1, g_2, ..., g_{L-2}, g_{L-1}] \in \mathbb{F}_2^L$, i.e.

$$G = g_0 \cdot 2^{L-1} + g_1 \cdot 2^{L-2} + \cdots + g_{L-2} \cdot 2 + g_{L-1}.$$

Moreover, we will use indistinctly G and $\mathcal{G}$. For example $S(G) = S(\mathcal{G})$ and $\tau(G) = \tau(\mathcal{G})$.

Remark 1. *Since $G = 3$ is the decimal representation of the binary number $[0, 0, 0, \ldots, 0, 1, 1]$, we have that*

$$\alpha^{\tau(3)} = \alpha + 1,$$

that is, $\tau(3) = \mathcal{Z}_\alpha(1)$, where $\mathcal{Z}_\alpha(1)$ denotes the Zech logarithm of 1 with basis α.

Recall that the Zech logarithm of t with a basis of the primitive element α is such that $\alpha^{\mathcal{Z}_\alpha(t)} = \alpha^t + 1$. Check [44] for more properties of this discrete logarithm.

Example 2. *Consider the LFSR in which the characteristic polynomial is $p(x) = x^5 + x^2 + 1$. For the initial state $\{1\ 1\ 1\ 1\ 1\}$, we obtain the PN-sequence*

$$\{1\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,0\}$$

which generates the family of generalized sequences shown in Table 3. The bits in bold in each sequence $\{v_i\}_{i\geq 0}$ correspond to the positions of the ones of the PN-sequence $\{u_i\}_{i\geq 0}$, which appears at the bottom of the table. Furthermore, these bits are the digits of the corresponding $S(\mathcal{G})$ sequence. Thus, in Table 3, the sequence $S(\mathcal{G}) = S([0, 0, 0, 0, 1])$ corresponds to $S(1) = \{1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\}$.

Next, we consider some properties of this representation (G-representation) of the generalized sequences.

Theorem 3. *If $G = 2^{L-1}$ then $S(G)$ is the identically 1 sequence.*

Proof. Since $G = 2^{L-1}$ corresponds to the vector $\mathcal{G} = [1, 0, 0, \ldots, 0]$, from Expression (1) we have that $v_i = u_i$, for $i \geq 0$, and according to the decimation rule defined in (2), the output sequence $\{s_j\}_{j\geq 0}$ is the identically 1 sequence. □

Theorem 4. *For $G = 0, 1, \ldots, 2^{L-1} - 1$, the sequences $S(G)$ and $S\left(G + 2^{L-1}\right)$ are complementary sequences, in the sense that $S(G) + S\left(G + 2^{L-1}\right)$ is the identically 1 sequence.*

Proof. Since the L-dimensional vector representations of G and $2^{L-1} + G$ are

$$\mathcal{G} = [0, g_1, g_2, \ldots, g_{L-1}] \quad \text{and} \quad \mathcal{G}' = [1, g_1, g_2, \ldots, g_{L-1}],$$

$\{v_i\}_{i\geq 0}$ and $\{v'_i\}_{i\geq 0}$, defined by $\mathcal{G}$ and $\mathcal{G}'$ respectively, satisfy $v_i = u_i + v'_i$, for $i \geq 0$. Now, from the decimation rule defined in (2), in order to obtain the generalized sequences $S(G)$ and $S\left(G + 2^{L-1}\right)$ we only consider the case when $u_i = 1$. Therefore, $s_j = 1 + s'_j$, which means that the sequences $S(G)$ and $S\left(G + 2^{L-1}\right)$ are complementary. □

One can easily verify that the first 16 generalized sequences in Table 3 are the complementary sequences of the last 16 sequences. This means that if we generate the first 2^{L-1} generalized sequences using the above method, then the remaining sequences are just the complementary sequences of the previous ones. In this way, the computation of generalized sequences is half-reduced.

Table 3. Generalized sequences for $p(x) = x^5 + x^2 + 1$.

G	$\mathcal{G}$	$\{v_i\}$ Sequence	Generalized Sequence
0	00000	**00000**0000**00000**0000000000**00000**00	0000000000000000
1	00001	**11001**1111**10001**1011101010**00010**10	1100110011110000
2	00010	**10011**1111**00011**0111010100**00100**101	1001100110100101
3	00011	**01010**0001**00101**1001111100**01101**11	0101010101010101
4	00100	**00111**1100**01101**1101010000**10010**11	0011100101110010
5	00101	**11110**0011**01110**1010000**10101100**1	1111010110000010
6	00110	**10100**0010**01011**0011111**00110111**0	1010000011010111
7	00111	**01101**1101**01000**0100101**10011111**00	0110110000100111
8	01000	**01111**1000**11011**1010000**10010110**	0111101011000001
9	01001	**10110**0111**11000**1101110**10000100**	1011011000110001
10	01010	**11100**0110**11010**1000010**01011001**	1110001101100100
11	01011	**00101**1001**11110**0011011**01010001**	0010111110010100
12	01100	**01000**0100**10110**0111110**01101101**	0100001110110011
13	01101	**10001**1011**10101**0000100**10110011**1	1000111101000011
14	01110	**11011**1010**10000**1001011**00111110**00	1101101000010110
15	01111	**00010**0101**10011**1110001**10111010**10	0001011011100110
16	10000	**11111**0001**10111**0101000**01001100**	1111111111111111
17	10001	**00110**1110**10100**0010010**11001111**0	0011001100001111
18	10010	**01100**1111**10001**1010100**00100**1	0110011001011010
19	10011	**10101**0000**10010**1100111**10001101**1	1010101010101010
20	10100	**11000**1101**11010**1000100**10110011**	1100011010001101
21	10101	**00001**0010**11001**1111000**11011010**1	0000101001111101
22	10110	**01011**0011**11100**0110111**01000010**	0101111100101000
23	10111	**10010**1100**11111**0001101**11010100**0	1001001111011000
24	11000	**10000**1001**01100**1111100**01101110**	1000010100111110
25	11001	**01001**0110**01111**1000110**11010100**0	0100100111001110
26	11010	**00011**0111**01010**0001001**01100111**	0001110010011011
27	11011	**11010**1000**01001**0110011**11100011**	1101000001101011
28	11100	**10111**0101**00001**0010110**01111000**1	1011110001001100
29	11101	**01110**1010**00010**0101100**11110011**	0111000010111100
30	11110	**00100**1011**00111**1100110**11010100**	0010010111101001
31	11111	**11101**0100**00100**1011001**11100110**	1110100100011001
		111110001**10111**0101000**01001100**	

3.2. The B-Representation of a Generalized Self-Shrunken Sequence

Let E be the shifting operator that acts on the terms of a sequence $\{u_n\}_{n\geq 0}$, that is:

$$E^k u_n = u_{n+k}, \quad \text{for all integer} \quad k \geq 0.$$

Let r be a positive integer. A sequence $\{s_j\}_{j\geq 0}$, of which the period is $T = 2^r$ is, in turn, a particular solution of equation:

$$\left(E^{2^r} + 1\right) z_n = (E+1)^{2^r} z_n = 0, \tag{4}$$

where its characteristic polynomial is $(x+1)^{2^r}$. According to [38,45], the solutions of Equation (4) can be written as:

$$z_n = \binom{n}{0} c_0 + \binom{n}{1} c_1 + \cdots + \binom{n}{T-1} c_{T-1} \quad \text{for } n \geq 0,$$

where the coefficients $c_i \in \mathbb{F}_2$, 1 is the unique root of the polynomial $(x+1)^{2^r}$ with multiplicity 2^r and $\binom{n}{i}$ is a binomial coefficient reduced modulo 2. Thus, $\{z_n\}_{n\geq 0}$ is the bit-wise XOR of T binary sequences $\left\{\binom{n}{i}\right\}$ weighted by T binary coefficients c_i. Hence, all the solutions of the difference equation written in (4) are sums of binomial sequences. In particular, every solution $\{z_n\}_{n\geq 0}$ can be written as:

$$\{z_n\} = \sum_{i=0}^{\nu} c_i \left\{\binom{n}{i}\right\}, \tag{5}$$

with $c_i \in \mathbb{F}_2$, $i = 0, 1, \ldots, \nu$, where ν is the greatest value i for which $c_\nu \neq 0$ while $c_i = 0$ for $\nu < i < T$. Expression (5) is the **binomial representation** (or B-representation) of the sequence $\{z_n\}_{n\geq 0}$.

In terms of this representation, the parameters of the sequence $\{z_n\}_{n\geq 0}$ can be easily analyzed. Indeed, the period of $\{z_n\}_{n\geq 0}$ is the period of the binomial sequence $\left\{\binom{n}{\nu}\right\}$ and the linear complexity of $\{z_n\}_{n\geq 0}$ is the linear complexity of the binomial sequence $\left\{\binom{n}{\nu}\right\}$, that is $LC = \nu + 1$ (see Theorem 1).

As a consequence we can recall the following result.

Theorem 5 ([38], Theorem 2)**.** *Given the binary sequence $\{z_n\}_{n\geq 0}$ with period $T = 2^r$, where r is a positive integer, and linear complexity LC, such sequence can be written as a linear combination of binomial sequences, that is, $\sum_{i=0}^{LC-1} c_i \left\{\binom{n}{i}\right\}$, $c_i \in \mathbb{F}_2$.*

We will use indistinctly the notation $\sum_{i=0}^{LC-1} c_i \left\{\binom{n}{i}\right\}$ or $\left\{\sum_{i=0}^{LC-1} c_i \binom{n}{i}\right\}$ to denote the B-representation of the sequence $\{z_n\}_{n\geq 0}$. Notice that, in the B-representation, the term with the highest index is $\binom{n}{LC-1}$. This means that the last term provides the LC of the sequence. We denote by $\{\mathbf{0}\}$ the B-representation of the null sequence.

Example 3. *Consider the sequence $\{z_n\} = \{1\,1\,1\,0\,0\,1\,0\,0\ldots\}$ with period $T = 8$. This sequence can be also written as a linear combination of the sequences $\left\{\binom{n}{0}\right\} + \left\{\binom{n}{3}\right\} + \left\{\binom{n}{4}\right\} + \left\{\binom{n}{5}\right\}$:*

$$\begin{array}{rll} & \left\{\binom{n}{5}\right\}: & \{0\,0\,0\,0\,0\,1\,0\,1\ldots\} \\ + & \left\{\binom{n}{4}\right\}: & \{0\,0\,0\,0\,1\,1\,1\,1\ldots\} \\ & \left\{\binom{n}{3}\right\}: & \{0\,0\,0\,1\,0\,0\,0\,1\ldots\} \\ & \left\{\binom{n}{0}\right\}: & \{1\,1\,1\,1\,1\,1\,1\,1\ldots\} \\ \hline & \{z_n\}: & \{1\,1\,1\,0\,0\,1\,0\,0\ldots\} \end{array}$$

Since the binomial sequence $\left\{\binom{n}{\nu}\right\}$ (the term with highest index) is $\left\{\binom{n}{5}\right\}$, then the linear complexity of $\{z_n\}$ will be $LC = 6$. In the same way, its period $T = 8$ coincides with the period of the sequence $\left\{\binom{n}{5}\right\}$.

In [38], the authors proposed an algorithm to compute the B-representation of any sequence with a period of the power of two. Here, our aim is to propose another method to compute the B-representation of a generalized sequence. Next, we give a method to obtain this representation from any binary sequence of period a power of two. For this, we need to define a binary matrix called the **binomial matrix**, which is similar to the construction of a binary Hadamard matrix. Consider $H_0 = [1]$ the binomial matrix for $t = 0$, that is, a matrix of size $2^0 \times 2^0$. We construct the binomial matrix for $t = 1$ as follows

$$H_1 = \begin{bmatrix} H_0 & H_0 \\ 0 & H_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

which has size $2^1 \times 2^1$. In general, we obtain the binomial matrix for t as

$$H_t = \begin{bmatrix} H_{t-1} & H_{t-1} \\ 0_{t-1} & H_{t-1} \end{bmatrix}$$

where H_{t-1} is the binomial matrix of size $2^{t-1} \times 2^{t-1}$ and 0_{t-1} is the null matrix of the same size.

Let $\{s_n\}_{n\geq 0}$ be a binary sequence of period $T = 2^t$. Given the binomial matrix H_t of size $2^t \times 2^t$, we construct the binary vector

$$B = [s_0, s_1, \ldots, s_{2^t-1}] \cdot H_t \mod 2. \tag{6}$$

The support of the vector B, denoted by $\mathrm{supp}(B)$, is the set of indices of the nonzero entries of B, considering the first position as the 0 position. Then, we define the B**-representation** of $\{s_n\}_{n\geq 0}$,

denoted by $B(\{s_n\})$, as the sequence given by the addition of the binomial sequences $\left\{\binom{n}{i}\right\}$, for $i \in \text{supp}(B)$, that is

$$B\left([s_0, s_1, \ldots, s_{2^t-1}]\right) = \sum_{i \in \text{supp}(B)} \left\{\binom{n}{i}\right\}. \tag{7}$$

Notice that, as a consequence of Expression (6), we can only compute the B-representation of binary sequences of period $T = 2^t$. In particular, we can always obtain the B-representation of any GSS-sequence since the family of generalized sequences consists of 2^L sequences with periods power of two (see [21]).

The following example helps us to understand this construction.

Example 4. *Consider the binary sequence* $\{s_n\} = \{1\,1\,1\,0\,0\,1\,0\,0\ldots\}$ *given in Example 3 in which the B-representation is* $\left\{\binom{n}{0} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5}\right\}$. *We check it using the method defined previously. The period of the sequence is* 2^3, *so we must construct the binomial matrix for* $t = 3$, *that is*

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

From Expression (6), we have that

$$B = [s_0, s_1, \ldots, s_7] \cdot H_3 = [1\,0\,0\,1\,1\,1\,0\,0]$$

and, therefore, $\text{supp}(B) = \{0, 3, 4, 5\}$. *So, from Expression (7), we have that* $B([s_0, s_1, \ldots, s_7]) = \left\{\binom{n}{0} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5}\right\}$, *as we expected.*

Recall that the columns of the binomial matrix (read from right to left) correspond to the successive diagonals of the Sierpinski's triangle in Figure 2. Thus, the binary vector B in Expression (6) is just the product of $[s_0, s_1, \ldots, s_{2^t-1}]$ by the diagonals of such a triangle.

We know that the generalized sequences have periods of the form 2^r, with $r < L$. Therefore, we can express the generalized sequences as a finite sum of binomial sequences.

The following result is an immediate consequence of Theorems 4 and 3.

Theorem 6. *For* $G = 0, 1, \ldots, 2^{L-1} - 1$, *the B-representations of* $S(G)$ *and* $S\left(G + 2^{L-1}\right)$ *are equal except for the term* $\left\{\binom{n}{0}\right\}$. *Furthermore, the B-representation of* $S\left(2^{L-1}\right)$ *is exactly* $\left\{\binom{n}{0}\right\}$.

This means that if we have the B-representations of the first 2^{L-1} generalized sequences, then the B-representations of the remaining 2^{L-1} sequences are the same ones except for the term $\binom{n}{0}$. In this way, the computation of generalized sequences is half-reduced.

Example 5. *Consider again the generalized sequences obtained in Example 2. In Table 4, we can find the B-representation of each one of these generalized sequences. As we saw in Section 3.1, the last* 16 *generalized sequences in Table 3 are the complementary sequences of the first* 16 *sequences and then, from Theorem 6, the B-representation of them is the same except for the term* $\left\{\binom{n}{0}\right\}$. *Furthermore, the B-representation of* $S(16)$ *is* $\left\{\binom{n}{0}\right\}$, *as expected.*

Some other properties of the family of generalized sequences can be deduced from the B-representation. We study these properties in detail in Section 4.

Table 4. Binomial representation for the generalized sequences of $p(x) = x^5 + x^2 + 1$.

G	Generalized Sequence	B-Representation
0	0000000000000000	$\{\mathbf{0}\}$
1	1100110011110000	$\{\binom{n}{0} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}\}$
2	1001100110100101	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}\}$
3	0101010101010101	$\{\binom{n}{1}\}$
4	0011100101110010	$\{\binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}\}$
5	1111010110000010	$\{\binom{n}{0} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}\}$
6	1010000011010111	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}\}$
7	0110110000100111	$\{\binom{n}{1} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}\}$
8	0111101011000001	$\{\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}\}$
9	1011011000110001	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}\}$
10	1110001101100100	$\{\binom{n}{0} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}\}$
11	0010111110010100	$\{\binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}\}$
12	0100001110110011	$\{\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}\}$
13	1000111101000011	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}\}$
14	1101101000010110	$\{\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}\}$
15	0001011011100110	$\{\binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}\}$
16	1111111111111111	$\{\binom{n}{0}\}$
17	0011001100001111	$\{\binom{n}{2} + \binom{n}{10} + \binom{n}{12}\}$
18	0110011001011010	$\{\binom{n}{1} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}\}$
19	1010101010101010	$\{\binom{n}{0} + \binom{n}{1}\}$
20	1100011010001101	$\{\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}\}$
21	0000101001111101	$\{\binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}\}$
22	0101111100101000	$\{\binom{n}{1} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}\}$
23	1001001111011000	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}\}$
24	1000010100111110	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}\}$
25	0100100111001110	$\{\binom{n}{1} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}\}$
26	0001110010011011	$\{\binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}\}$
27	1101000001101011	$\{\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}\}$
28	1011110001001100	$\{\binom{n}{0} + \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}\}$
29	0111000010111100	$\{\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}\}$
30	0010010111101001	$\{\binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}\}$
31	1110100100011001	$\{\binom{n}{0} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}\}$

3.3. The p-Representation of a Generalized Self-Shrunken Sequence

In this subsection, we define a new representation of generalized sequences which gives us information of the shifted sequences employed in the decimation rule defined in (2).

From Theorem 2, we have that the sequence $\{v_i\}_{i\geq 0}$ is a shifted version of the PN-sequence $\{u_i\}_{i\geq 0}$. Therefore, instead of considering the vector $\mathcal{G}$ in Expression (1) to construct $\{v_i\}_{i\geq 0}$, we can simply consider the successive shifted versions of $\{u_i\}_{i\geq 0}$ and apply in each case the decimation rule given in (2).

Let us consider the p-shifted version of the PN-sequence $\{u_i\}_{i\geq 0}$ with $0 \leq p < 2^L - 1$. Applying the decimation rule given in (2), we construct the corresponding generalized sequence, which we denote by $S\{p\}$. This new representation of a generalized sequence is called p-representation.

One of the consequences of the group structure of $\mathcal{S}$ is that the sum of two generalized sequences is another generalized sequence. The following theorem allows us to obtain the p-representation of the resulting generalized sequence from the p-representations of two generalized sequences given.

Theorem 7. *Consider that $\{u_i\}_{i\geq 0}$ is the PN-sequence of an LFSR with primitive characteristic polynomial $p(x)$ of degree L and $\alpha \in \mathbb{F}_{2^L}$ is a root of $p(x)$. Then, the sum of two generalized sequences obtained with shifts d_1 and d_2 is another generalized sequence with shift $d_1 + \mathcal{Z}_\alpha(d_2 - d_1)$, i.e,*

$$S\{d_1\} + S\{d_2\} = S\{d_1 + \mathcal{Z}_\alpha(d_2 - d_1)\},$$

where $\mathcal{Z}_\alpha(\cdot)$ is as before the Zech logarithm with basis α.

Proof. Assume that $S\{d_1\} = \{s_j\}$ and $S\{d_2\} = \{\tilde{s}_j\}$ are two generalized sequences obtained from the PN-sequence $\{u_i\}$.

According to the decimation rule given in (2), if supp $(\{u_i\}) = \{i_0, i_1, \ldots, i_{2^{L-1}-1}\}$, then we have that $s_j = u_{d_1+i_j}$ and $\tilde{s}_j = u_{d_2+i_j}$.

We have seen in Expression (3) that every element of $\{u_i\}$ can be expressed as

$$u_i = A\alpha^i + A^2\alpha^{2i} + A^4\alpha^{4i} + \cdots + A^{2^{L-1}}\alpha^{2^{L-1}i},$$

where $A \in \mathbb{F}_{2^L}$ with $A \neq 0$. Therefore, we have that:

$$\begin{aligned} u_{d_1+i_j} =& A\alpha^{d_1+i_j} + A^2\alpha^{2(d_1+i_j)} + A^4\alpha^{4(d_1+i_j)} + \ldots + A^{2^{L-1}}\alpha^{2^{L-1}(d_1+i_j)} \\ u_{d_2+i_j} =& A\alpha^{d_2+i_j} + A^2\alpha^{2(d_2+i_j)} + A^4\alpha^{4(d_2+i_j)} + \ldots + A^{2^{L-1}}\alpha^{2^{L-1}(d_2+i_j)}. \end{aligned}$$

Bit-wise XORing both sequences $\{s_j\} + \{\tilde{s}_j\} = \{u_{d_1+i_j}\} + \{u_{d_2+i_j}\} = \{u_{d_1+i_j} + u_{d_2+i_j}\}$ we get:

$$\begin{aligned} u_{d_1+i_j} + u_{d_2+i_j} &= A\alpha^{i_j}(\alpha^{d_1} + \alpha^{d_2}) + A^2\alpha^{2i_j}(\alpha^{2d_1} + \alpha^{2d_2}) + \ldots + A^{2^{L-1}}\alpha^{2^{L-1}i_j}(\alpha^{2^{L-1}d_1} + \alpha^{2^{L-1}d_2}) \\ &= A\alpha^{i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1)} + A^2\alpha^{2(i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1))} + \ldots + A^{2^{L-1}}\alpha^{2^{L-1}(i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1)} \\ &= u_{i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1)}. \end{aligned}$$

The sequence $\{u_{i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1)}\}$ is the generalized sequence with shift $d_1 + \mathcal{Z}_\alpha(d_2 - d_1)$, that is,

$$S\{d_1 + \mathcal{Z}_\alpha(d_2 - d_1)\} = \{u_{i_j+d_1+\mathcal{Z}_\alpha(d_2-d_1)}\}.$$

□

Notice that there is not any value $p \in \{0, 1, \ldots, 2^L - 2\}$ that represents the null binary sequence $\{0\,0\,0\,0\ldots\}$. So, we denote with $S\{\infty\}$ the p-representation of this sequence. It is worth noticing that $S\{\infty\} = S(0) = \{\mathbf{0}\}$, where $S(0)$ and $\{\mathbf{0}\}$ are the G-representation and the B-representation of the null sequence, respectively.

We have introduced three different notations for generalized sequences: the G-representation, $S(G)$, introduced in Subsection 3.1; the B-representation, $B(\{s_i\})$ given in Subsection 3.2 and the p-representation, $S\{p\}$, given in this subsection. The next theorem, which is a direct consequence of Theorem 2, provides a relation between the G-representation and the p-representation. We can get a representation from the other as follows.

Theorem 8. *Consider the family of generalized sequences denoted by $\mathcal{S} = \{S(G) : G = 0, 1, \ldots, 2^L - 1\} = \{S\{p\} : p = 0, 1, \ldots, 2^L - 2\} \cup \{S\{\infty\}\}$, then*

$$S\{p\} = S\left((\tau(G) - L + 1) \bmod (2^L - 1)\right)$$

with $\tau(G) \in [0, 2^L - 2]$ such that $\alpha^{\tau(G)} = g_0\alpha^{L-1} + g_1\alpha^{L-2} + \ldots + g_{L-1}$, where $\alpha \in \mathbb{F}_{2^L}$ is a root of the primitive polynomial of the corresponding LFSR. Equivalently, $p = (2^L - L + \tau(G)) \bmod (2^L - 1)$.

Example 6. *Consider again Example 2. Applying Theorem 8 to the family of generalized sequences given in Table 3, we obtain the relation between G-representation and p-representation as depicted in Table 5. For instance, if* $G = 10$ *that is* $\mathcal{G} = [0,1,0,1,0]$*, we have to compute* $\tau(10)$ *such that* $\alpha^{\tau(10)} = \alpha^3 + \alpha$*. According to the results in Table 5,* $\tau(10) = 6$*, therefore, from Theorem 8,* $p = \tau(10) - L + 1 = 6 - 5 + 1 = 2$*. It is easy to check that* $S(10) = S\{2\} = \{1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\}$.

Consider now another example. For $G = 13$*, we have* $\mathcal{G} = [0,1,1,0,1]$*. We need to find* $\tau(13)$ *such that* $\alpha^{\tau(13)} = \alpha^3 + \alpha^2 + 1$*. According to Table 5, the value we are looking for is* $\tau(13) = 8$*. Therefore* $p = \tau(13) - L + 1 = 8 - 5 + 1 = 4$*, as we expected from Table 5.*

Table 5. Generalized sequences for $p(x) = x^5 + x^2 + 1$.

$p = (\tau(G) - L + 1) \mod (2^L - 1)$					
G	p	α^p	$\tau(G)$	$\alpha^{\tau(G)}$	$S\{p\}$
1	27	$\alpha^3 + \alpha + 1$	0	1	1100110011110000
2	28	$\alpha^4 + \alpha^2 + \alpha$	1	α	1001100110100101
3	14	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	18	$\alpha + 1$	0101010101010101
4	29	$\alpha^3 + 1$	2	α^2	0011100101110010
5	1	α	5	$\alpha^2 + 1$	1111010110000010
6	15	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	19	$\alpha^2 + \alpha$	1010000011010111
7	7	$\alpha^4 + \alpha^2$	11	$\alpha^2 + \alpha + 1$	0110110000100111
8	30	$\alpha^4 + \alpha$	3	α^3	0111101011000001
9	25	$\alpha^4 + \alpha^3 + 1$	29	$\alpha^3 + 1$	1011011000110001
10	2	α^2	6	$\alpha^3 + \alpha$	1110001101100100
11	23	$\alpha^3 + \alpha^2 + \alpha + 1$	27	$\alpha^3 + \alpha + 1$	0010111110010100
12	16	$\alpha^4 + \alpha^3 + \alpha + 1$	20	$\alpha^3 + \alpha^2$	0100001110110011
13	4	α^4	8	$\alpha^3 + \alpha^2 + 1$	1000111101000011
14	8	$\alpha^3 + \alpha^2 + 1$	12	$\alpha^3 + \alpha^2 + \alpha$	1101101000010110
15	19	$\alpha^2 + \alpha$	23	$\alpha^3 + \alpha^2 + \alpha + 1$	0001011011100110
16	0	1	4	α^4	1111111111111111
17	6	$\alpha^3 + \alpha$	10	$\alpha^4 + 1$	0011001100001111
18	26	$\alpha^4 + \alpha^2 + \alpha + 1$	30	$\alpha^4 + \alpha$	0110011001011010
19	13	$\alpha^4 + \alpha^3 + \alpha^2$	17	$\alpha^4 + \alpha + 1$	1010101010101010
20	3	α^3	7	$\alpha^4 + \alpha^2$	1100011010001101
21	18	$\alpha + 1$	22	$\alpha^4 + \alpha^2 + 1$	0000101001111101
22	24	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	28	$\alpha^4 + \alpha^2 + \alpha$	0101111100101000
23	22	$\alpha^4 + \alpha^2 + 1$	26	$\alpha^4 + \alpha^2 + \alpha + 1$	1001001111011000
24	17	$\alpha^4 + \alpha + 1$	21	$\alpha^4 + \alpha^3$	1000010100111110
25	21	$\alpha^4 + \alpha^3$	25	$\alpha^4 + \alpha^3 + 1$	0100100111001110
26	5	$\alpha^2 + 1$	9	$\alpha^4 + \alpha^3 + \alpha$	0001110010011011
27	12	$\alpha^3 + \alpha^2 + \alpha$	16	$\alpha^4 + \alpha^3 + \alpha + 1$	1101000001101011
28	9	$\alpha^4 + \alpha^3 + \alpha$	13	$\alpha^4 + \alpha^3 + \alpha^2$	1011110001001100
29	10	$\alpha^4 + 1$	14	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	0111000010111100
30	20	$\alpha^3 + \alpha^2$	24	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0010010111101001
31	11	$\alpha^2 + \alpha + 1$	15	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1110100100011001

Corollary 1. *Consider the family of generalized sequences* $\mathcal{S} = \{S(G) : G = 0,1,\ldots,2^L - 1\} = \{S\{p\} : p = 0,1,\ldots,2^L - 2\} \cup \{S\{\infty\}\}$ *generated by the PN-sequence* $\{u_i\}$ *of period* $2^L - 1$*. If* $G = 2^t$*, with* $t \in [0, L-1]$*, then* $\tau(G) = t$ *and* $p = (t - L + 1) \mod (2^L - 1)$ *or equivalently* $p = (2^L - L + t) \mod (2^L - 1)$.

Example 7. *Consider again Example 2, where* $L = 5$ *and* $T = 31$*. We can compute the value of p for each* $G = 2^t$*, where* $t = 0,1,2,3,4$*:*

G	$\tau(G) = t$	$p = (t - L + 1) \bmod (2^L - 1)$
1	0	$-4 \bmod 31 = 27$
2	1	$-3 \bmod 31 = 28$
4	2	$-2 \bmod 31 = 29$
8	3	$-1 \bmod 31 = 30$
16	4	$0 \bmod 31 = 0$

This result matches with the expected values for p obtained in Table 5.

It is worth mentioning that the self-shrinking generator is another cryptographic sequence generator based on irregular decimation [20]. In this case, a PN-sequence is self-decimated producing a new sequence with good cryptographic properties. In [22], authors proved that the sequence produced by this generator can also be obtained with the generalized self-shrinking generator and the same characteristic polynomial with shift $p = 2^{L-1}$. As a consequence of this fact and the previous theorem, we can introduce the following result.

Corollary 2. *The sequence $S(G)$ with $\tau(G) = 2^{L-1} + L - 1$ such that $\alpha^{\tau(G)} = g_0\alpha^{L-1} + g_1\alpha^{L-2} + \ldots + g_{L-1}$ is the output sequence generated by the self-shrinking generator with the same LFSR and characteristic polynomial $p(x)$.*

Example 8. *Consider again Example 2. According to the previous corollary, the sequence generated by the self-shrinking generator is $S(G)$ with G such that $\alpha^{\tau(G)} = g_0\alpha^{L-1} + g_1\alpha^{L-2} + \ldots + g_{L-1}$. In this case, $\tau(G) = 20$ and $\alpha^{20} = \alpha^3 + \alpha^2$. Therefore $\mathcal{G} = [0, 1, 1, 0, 0]$ and $G = 12$ which corresponds to the sequence with shift $p = 16$, that is, the output sequence of the self-shrinking generator, as expected.*

The following lemma proves that there exists an element $m \in \{L - 1, L, \ldots, 2^L - 3\}$ such that $\alpha^{m+1} = \alpha^m + 1$. Later, we check that the generalized sequences associated to these values, $S\{m\}$ and $S\{m + 1\}$, are the sequences with period $T = 2$.

Lemma 1. *Let α be a primitive element in $\mathbb{F}_{2^L}$. Then*

$$\alpha^{m+1} = \alpha^m + 1$$

if and only if $m = 2^L - 1 - \mathcal{Z}_\alpha(1)$.

Proof. Assume that $\alpha^{m+1} + \alpha^m = 1$. Then

$$1 = \alpha^{m+1} + \alpha^m = \alpha^m(\alpha + 1) = \alpha^m\,\alpha^{\mathcal{Z}_\alpha(1)} = \alpha^{m+\mathcal{Z}_\alpha(1)},$$

and therefore, $m + \mathcal{Z}_\alpha(1) = 2^L - 1$.

Conversely, assume that $m = 2^L - 1 - \mathcal{Z}_\alpha(1)$. Then

$$\alpha^{m+1} + \alpha^m = \alpha^m(\alpha + 1) = \alpha^{2^L-1-\mathcal{Z}_\alpha(1)}\,\alpha^{\mathcal{Z}_\alpha(1)} = \alpha^{2^L-1} = 1.$$

Therefore, the lemma holds. □

Let $\mathcal{G}_m$ the binary representation of the value of G associated to m, and G_m its decimal representation. Next, we introduce a theorem whose proof helps us to prove Theorem 10.

Theorem 9. *Let m be the integer defined in Lemma 1. Then $|G_m - G_{m+1}| = 2^{L-1}$*

Proof. According to Theorem 8, we can express m and $m + 1$ as:

$$m = \tau(G_m) - L + 1 \quad \text{and} \quad m+1 = \tau(G_{m+1}) - L + 1, \tag{8}$$

where $\tau(G_m)$ and $\tau(G_{m+1})$ satisfy

$$\begin{aligned} \alpha^{\tau(G_m)} &= g_0\alpha^{L-1} + g_1\alpha^{L-2} + \ldots + g_{L-2}\alpha + g_{L-1}, \\ \alpha^{\tau(G_{m+1})} &= g'_0\alpha^{L-1} + g'_1\alpha^{L-2} + \ldots + g'_{L-2}\alpha + g'_{L-1} \end{aligned}$$

with

$$\mathcal{G}_m = [g_0, g_1, \ldots, g_{L-2}, g_{L-1}] \quad \text{and} \quad \mathcal{G}_{m+1} = \left[g'_0, g'_1, \ldots, g'_{L-2}, g'_{L-1}\right].$$

From Lemma 1 and Expression (8) we deduce that:

$$\alpha^{\tau(G_{m+1})} - \alpha^{\tau(G_m)} = \alpha^{L-1}.$$

Therefore,

$$\alpha^{\tau(G_{m+1})} = \alpha^{\tau(G_m)} + \alpha^{L-1} = (g_0+1)\alpha^{L-1} + g_1\alpha^{L-2} + \cdots + g_1\alpha + g_0.$$

As a consequence, the relation between G_m and G_{m+1} is

$$|G_m - G_{m+1}| = 2^{L-1}.$$

□

Theorem 10. *Consider $m \in \{L-1, L, \ldots, 2^L - 3\}$ such that $\alpha^{m+1} = 1 + \alpha^m$, where m is the value given in Lemma 1. The generalized sequences $S\{m\}$ and $S\{m+1\}$ are the sequences of period $T = 2$, that is, the sequences with B-representation $\left\{\binom{n}{1}\right\}$ and $\left\{\binom{n}{0} + \binom{n}{1}\right\}$.*

Proof. Let $\{u_i\}$ be the PN-sequence used in the GSSG. Consider the corresponding shifted versions $\{v_i^{(m)}\} = \{u_{i+m}\}$ and $\{v_i^{(m+1)}\} = \{u_{i+m+1}\}$, where m is as in Lemma 1. According to the proof of Theorem 9, we know that:

$$\mathcal{G}_m = [g_0, g_1, \ldots, g_{L-1}] \quad \text{and} \quad \mathcal{G}_{m+1} = [g_0 + 1, g_1, \ldots, g_{L-1}].$$

Now, from Expression (1):

$$\begin{aligned} v_i^{(m)} &= u_{i+m} = g_0u_i + g_1u_{i-1} + g_2u_{i-2} + \cdots + g_{L-1}u_{i-L+1} \\ v_i^{(m+1)} &= u_{i+m+1} = (g_0+1)u_i + g_1u_{i-1} + g_2u_{i-2} + \cdots + g_{L-1}u_{i-L+1}. \end{aligned}$$

As a consequence, $v_i^{(m)} + v_i^{(m+1)} = u_{i+m} + u_{i+m+1} = u_i$.

Let $\text{supp}(\{u_i\})$ be the set of indices j such that $u_j = 1$. Therefore

$$\begin{cases} v_j^{(m)} = v_j^{(m+1)}, & \text{if } j \notin \text{supp}(\{u_i\}), \quad (9) \\ v_j^{(m)} + v_j^{(m+1)} = 1, & \text{if } j \in \text{supp}(\{u_i\}). \quad (10) \end{cases}$$

Notice that (10) implies that, when $j \in \text{supp}(\{u_i\})$,

$$v_j^{(m)} = 0, v_j^{(m+1)} = 1 \quad \text{or} \quad v_j^{(m)} = 1, v_j^{(m+1)} = 0.$$

As a consequence, the resulting generalized sequences, $S(G_m)$ and $S(G_{m+1})$, are complementary (their sum is the identically 1 sequence).

Assume that $\text{supp}(\{u_i\}) = \left\{i_0, i_1, \ldots, i_{2^{L-1}-1}\right\}$. Let $i_k \in \text{supp}(\{u_i\})$, according to (9), $v_j^{(m)} = v_j^{(m+1)}$ for $j = i_k + 1, i_k + 2, \ldots, i_{k+1} - 1$ (i.e., the integers between i_k and i_{k+1}). Furthermore,

since $\{v_i^{(m+1)}\}$ is also a shifted version of $\{v_i^{(m)}\}$ (shift $p = 1$), we have $v_j^{(m+1)} = v_{j+1}^{(m)}$, for $j \geq 0$. As a result, we obtain the following chain:

$$v_{i_k}^{(m+1)} = v_{i_k+1}^{(m)} = v_{i_k+1}^{(m+1)} = v_{i_k+2}^{(m)} = v_{i_k+2}^{(m+1)} = \cdots = v_{i_{k+1}-1}^{(m+1)} = v_{i_{k+1}}^{(m)}$$

Therefore, $v_{i_k}^{(m+1)} = v_{i_{k+1}}^{(m)}$. This means that $S(G_m)$ is a shifted version of $S(G_{m+1})$, but they are complementary. The only option is that they are the sequences $\{1\,0\,1\,0\,1\,0\,1\,0\,1\ldots\}$ and $\{0\,1\,0\,1\,0\,1\,0\,1\,0\ldots\}$. □

For example, consider Table 5. The sequences $\{1\,0\,1\,0\,1\,0\,1\ \ldots\}$ and $\{0\,1\,0\,1\,0\,1\,0\ \ldots\}$ correspond to shifts $m = 13$ and $m + 1 = 14$ of the PN-sequence $\{u_i\}$. From the isomorphism defined by (11), we have that the generalized sequence $S\{13\}$ is associated with the element $\alpha^t = \alpha^{17} = \alpha^4 + \alpha + 1$, and the generalized sequence $S\{14\}$ is associated with $\alpha^{18} = \alpha + 1$. Therefore, we have $G_{13} = 19$ and $G_{14} = 3$ (see Table 5 again), in which the difference is 2^4 as Theorem 9 indicated.

Theorem 11. *Consider a primitive polynomial $p(x)$ of degree L and let m be the positive integer defined in 1, i.e., $\alpha^{m+1} = \alpha^m + 1$, with α a root of $p(x)$. Then, given β a root of $p^*(x)$, where $p^*(x)$ is the reciprocal polynomial of $p(x)$, we have that $\beta^{m^*+1} = \beta^{m^*} + 1$, with $m^* = 2^L - 2 - m$.*

Proof. We know that $\beta = \alpha^{-1}$ is a root of $p^*(x)$. Then

$$\alpha^{m+1} = \beta^{-m-1} = \beta^{2^L-m-2}$$

and $\alpha^m + 1 = \beta^{-n} + 1 = \beta^{2^L-1-m} + 1$. As a consequence, we have that $\beta^{2^L-2-m} = \beta^{2^L-1-m} + 1$ and

$$\beta^{2^L-1-m} = \beta^{2^L-2-m} + 1.$$

□

In Table 6, we study the values of m, such that $\alpha^{m+1} = \alpha^m + 1$, for every primitive polynomial of degree 5. Consider, for instance, $p(x) = x^5 + x^2 + 1$. For this polynomial $m = 13$. The corresponding value m^* for the reciprocal polynomial $p(x) = x^5 + x^3 + 1$ is computed as $m^* = 2^5 - 2 - 13 = 17$.

Table 6. Primitive polynomials of degree 5 and m such that $1 + \alpha^m = \alpha^{m+1}$.

p(x)	*m*
$x^5 + x^+1$	13
$x^5 + x^3 + 1$	17
$x^5 + x^4 + x^3 + x + 1$	18
$x^5 + x^4 + x^2 + x + 1$	12
$x^5 + x^4 + x^3 + x^2 + 1$	11
$x^5 + x^3 + x^2 + x + 1$	19

Remark 2. *Given the value of m for a primitive polynomial $p(x)$, we can find the value of m^* for $p^*(x)$ without computing any logarithm.*

4. Partitions of the Family of Generalized Sequences

In this section, we study the family of generalized sequences as a partition of cosets of the quotient set given by $\mathcal{S}$ and a subgroup of generalized sequences. This partition will help us in the analysis of the structure of the family of generalized sequences and their cryptographic properties. Their different representations, presented in the previous section, will facilitate us in this study.

4.1. Additive Group Structure

We know that the family $\mathcal{S}$ of generalized sequences with the bit-wise XOR operation $+$ is an Abelian additive group of order 2^L. Therefore, we can see it as an $\mathbb{F}_2$-vector space of dimension L. Furthermore, the additive group structure of $(\mathcal{S},+)$ and Theorem 7 allows us to define the following group isomorphism,

$$\begin{array}{rccc} \phi: & (\mathbb{F}_{2^L},+) & \longrightarrow & (\mathcal{S},+) \\ & 0 & \mapsto & S\{\infty\} \\ & \alpha^p & \mapsto & S\{p\} \end{array} \tag{11}$$

where $S\{p\}$ denotes the p-representation.

Suppose that $\mathcal{S}$ comes from an LFSR of L stages and define $\mathcal{K}$ the set of the generalized sequences with periods 1 and 2; that is

$$\mathcal{K} = \{\{0\,0\,0\,0\,\ldots\},\{1\,1\,1\,1\,\ldots\},\{0\,1\,0\,1\,\ldots\},\{1\,0\,1\,0\,\ldots\}\} = \{S\{\infty\},S\{0\},S\{m\},S\{m+1\}\},$$

where m is given in Lemma 1. We have that $(\mathcal{K},+)$ is a subgroup of $\mathcal{S}$ of order 4; therefore, $\mathcal{K}$ can be considered as a vector subspace of $\mathcal{S}$ of dimension 2.

4.1.1. Subsets of $\mathcal{S}$ of Order 2^2

From the groups $\mathcal{S}$ and $\mathcal{K}$, we can define the quotient group $\mathcal{S}/\mathcal{K} = \{s+\mathcal{K} \mid s \in \mathcal{S}\}$, in which the order $|\mathcal{S}/\mathcal{K}|$ is, by the Lagrange's Theorem (see ([46], Section 6.8)),

$$|\mathcal{S}/\mathcal{K}| = \frac{|\mathcal{S}|}{|\mathcal{K}|} = 2^{L-2}.$$

For each $s \in \mathcal{S}$, the set $s+\mathcal{K}$ is called **cosets of** $\mathcal{S}$ **modulo** $\mathcal{K}$ and s is known as the **representative** of the coset.

Due to the properties of the cosets of a group ([47], Section 5.2) we know that any two cosets are either disjoint or identical, the union of the cosets is the own group and any subgroup is the coset defined by the neutral element. Although derived from a subgroup, cosets are not usually themselves subgroups of $\mathcal{S}$, only subsets. So, we have a partition of the set of generalized sequences $\mathcal{S}$ into 2^{L-2} cosets of size 4, denoted by $\mathcal{S}_4^{(i)}$; that is,

$$\mathcal{S} = \bigcup_{i=1}^{2^{L-2}} \mathcal{S}_4^{(i)}. \tag{12}$$

In the following example, we construct the quotient group of a family of generalized sequences and their cosets, using the p-representations.

Example 9. *Consider the set of GSS-sequences $\mathcal{S}$ given in Table 5 and the null sequence $S\{\infty\}$. We have that $\mathcal{K} = \{S\{\infty\},S\{0\},S\{13\},S\{14\}\}$ and, as $|\mathcal{S}| = 32$, the 8 cosets of $\mathcal{S}$ are $\mathcal{K}$ and*

$$\begin{aligned} S\{5\}+\mathcal{K} &= \{S\{5\},S\{2\},S\{21\},S\{25\}\}, \\ S\{6\}+\mathcal{K} &= \{S\{6\},S\{27\},S\{26\},S\{28\}\}, \\ S\{18\}+\mathcal{K} &= \{S\{18\},S\{1\},S\{24\},S\{15\}\}, \\ S\{19\}+\mathcal{K} &= \{S\{19\},S\{11\},S\{16\},S\{9\}\}, \\ S\{20\}+\mathcal{K} &= \{S\{20\},S\{8\},S\{10\},S\{4\}\}, \\ S\{23\}+\mathcal{K} &= \{S\{23\},S\{12\},S\{30\},S\{17\}\}, \\ S\{29\}+\mathcal{K} &= \{S\{29\},S\{3\},S\{7\},S\{22\}\}. \end{aligned}$$

From the group isomorphism between $\mathbb{F}_{2^L}$ and $\mathcal{S}$ given in (11) and by Theorem 10, we know that

$$\mathbb{K} = \left\{0, 1, \alpha^m, \alpha^{m+1}\right\} = \left\{0, 1, \alpha^m, \alpha^{\mathcal{Z}_\alpha(m)}\right\}$$

is isomorphic to $\mathcal{K}$; therefore, the cosets of $\mathbb{F}_{2^L}$ modulo $\mathbb{K}$ can be written as $\alpha^p + \mathbb{K}$, where $\phi(\alpha^p) = S\{p\} = s \in \mathcal{S}$ is the representative of the coset. Furthermore, each coset will be isomorphic to

$$\alpha^p + \mathbb{K} = \left\{\alpha^p, \alpha^p + 1, \alpha^p + \alpha^m, \alpha^p + \alpha^{\mathcal{Z}_\alpha(m)}\right\}$$

Example 10. *Consider Example 9 again. We know that, in this case, $m = 13$. Therefore, the cosets of $\mathbb{F}_{2^5}$ modulo $\mathbb{K}$ are*

$$\begin{aligned}
\mathbb{K} &= \left\{0, 1, \alpha^{13}, \alpha^{14}\right\},\\
\alpha^5 + \mathbb{K} &= \left\{\alpha^5, \alpha^2, \alpha^{21}, \alpha^{25}\right\},\\
\alpha^6 + \mathbb{K} &= \left\{\alpha^6, \alpha^{27}, \alpha^{26}, \alpha^{28}\right\},\\
\alpha^{18} + \mathbb{K} &= \left\{\alpha^{18}, \alpha, \alpha^{24}, \alpha^{15}\right\},\\
\alpha^{19} + \mathbb{K} &= \left\{\alpha^{19}, \alpha^{11}, \alpha^{16}, \alpha^{9}\right\},\\
\alpha^{20} + \mathbb{K} &= \left\{\alpha^{20}, \alpha^{8}, \alpha^{10}, \alpha^{4}\right\},\\
\alpha^{23} + \mathbb{K} &= \left\{\alpha^{23}, \alpha^{12}, \alpha^{30}, \alpha^{17}\right\},\\
\alpha^{29} + \mathbb{K} &= \left\{\alpha^{29}, \alpha^{3}, \alpha^{7}, \alpha^{22}\right\}.
\end{aligned}$$

Next, we study the B-representation of the cosets of order 4. We focus our attention in this representation because we can obtain the LC of a generalized sequence directly from it (see Theorem 5).

Recalling that we denote by $\{\mathbf{0}\}$ the B-representation of the null sequence, we have that the B-representation of $\phi(\mathcal{K}) = \{S(\infty), S(0), S(m), S(m+1)\}$ is

$$\mathcal{K} = \left\{\{\mathbf{0}\}, \left\{\binom{n}{0}\right\}, \left\{\binom{n}{1}\right\}, \left\{\binom{n}{0} + \binom{n}{1}\right\}\right\}.$$

Therefore, the B-representation of the corresponding sequences of each coset will have the following form

$$\left\{\Delta_s, \Delta_s + \left\{\binom{n}{0}\right\}, \Delta_s + \left\{\binom{n}{1}\right\}, \Delta_s + \left\{\binom{n}{0} + \binom{n}{1}\right\}\right\}$$

where $\Delta_s = \left\{\sum_{i=2}^{2^{L-1}-(L-2)} c_i \binom{n}{i}\right\}$, with $c_i \in \mathbb{F}_2$, denotes the B-representation of the sequence associated to the representative of the coset $s + \mathcal{K}$, denoted by s. From Expression (7), we can obtain Δ_s taking $\{s_n\} = S\{p\} = s$ and the binomial matrix H_{L-1} in Expression (6). Notice that for a sequence with linear complexity equal to LC, we have that $c_{LC-1} = 1$ and $c_i = 0$, for $i \geq LC$ (see Theorem 5). As we know that $LC \leq 2^{L-1} - (L-2)$ for the generalized sequences [40], then we consider the coefficients c_i, for $i = 0, 1, \ldots, 2^{L-1} - (L-2)$, even though the last ones could be zeros.

Example 11. *Consider again the set of generalized sequences $\mathcal{S}$ given in Table 5 and the cosets given in Example 9. In Table 7, we have the B-representation of each generalized sequence. Consider the coset $\alpha^6 + \mathbb{K} = \{\alpha^6, \alpha^{27}, \alpha^{26}, \alpha^{28}\}$. The B-representation of the set of generalized sequences $\{S\{6\}, S\{27\}, S\{26\}, S\{28\}\}$ is given by*

$$\left\{\left\{\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\},\left\{\binom{n}{0}+\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\},\left\{\binom{n}{1}+\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\},\right.$$
$$\left.\left\{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\}\right\},$$

where $\Delta_6=\left\{\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\}$ *is the common term in the four representations.*

We have considered α^6 *as the representative of the coset, but we could choose any element of the coset, since that* $\alpha^6+\mathbb{K}=\alpha^{26}+\mathbb{K}=\alpha^{27}+\mathbb{K}=\alpha^{28}+\mathbb{K}$. *In this example, we consider* α^6 *the representative of the coset, and the B-representation of* $S\{6\}$ *is denoted by* $\Delta_{\alpha^6}=\left\{\binom{n}{2}+\binom{n}{10}+\binom{n}{12}\right\}$.

4.1.2. *Subgroups of* $\mathcal{S}$ *of Order* 2^3

In the previous subsection, we give a partition of the family of generalized sequences using the cosets of $\mathcal{S}$ modulo $\mathcal{K}$ which do not have to be subgroups. In this subsection, we give a partition of $\mathcal{S}$ using subgroups of $\mathcal{S}$ obtained from these cosets and the subgroup $\mathcal{K}$.

We can construct subgroups of $\mathcal{S}$ of order 8, denoted by $\mathcal{S}_8^{(i)}$ for $i=1,2,\ldots,2^{L-2}-1$, from the union of $\mathcal{K}$ and the cosets of $\mathcal{S}$, $s+\mathcal{K}$, for any $s\in\mathcal{S}$.

From the isomorphism given in Expression (11), if we assume that $\phi(\alpha^p)=s$, then these subgroups can be expressed by

$$\mathbb{K}\cup(\alpha^p+\mathbb{K})=\left\{0,1,\alpha^m,\alpha^{m+1},\alpha^p,\alpha^p+1,\alpha^p+\alpha^m,\alpha^p+\alpha^{m+1}\right\}.$$

The *B*-representation of the corresponding sequences of each of the subgroups $\mathcal{S}_8^{(i)}$ for $i=1,2,\ldots,2^{L-2}-1$ will have the following form

$$\left\{\mathbf{0},\left\{\binom{n}{0}\right\},\left\{\binom{n}{1}\right\},\left\{\binom{n}{0}+\binom{n}{1}\right\},\Delta_s,\Delta_s+\left\{\binom{n}{0}\right\},\Delta_s+\left\{\binom{n}{1}\right\},\Delta_s+\left\{\binom{n}{0}+\binom{n}{1}\right\}\right\}$$

where $\Delta_s=\left\{\sum_{i=2}^{2^{L-1}-(L-2)}c_i\binom{n}{i}\right\}$, with $c_i\in\mathbb{F}_2$, is the binomial representation of the representative of the coset $s+\mathcal{S}$.

We observe that the subgroups $\mathcal{S}_8^{(i)}$ can also be considered as vector subspaces of dimension three and the union of them provides the group $\mathcal{S}$, that is,

$$\mathcal{S}=\bigcup_{i=1}^{2^{L-2}-1}\mathcal{S}_8^{(i)}. \tag{13}$$

Notice that the Expression (13) is not a disjoint union, since the sequences represented by $\mathbf{0}$, $\left\{\binom{n}{0}\right\}$, $\left\{\binom{n}{1}\right\}$ and $\left\{\binom{n}{0}+\binom{n}{1}\right\}$ are included in each subgroup. On the other hand, Expression (12) is a disjoint union of cosets. Therefore, the considered cosets form a partition of $\mathcal{S}$ while the subgroups of order 8 do not.

Example 12. *Consider again Example 11 and Table 7. We can take the cosets and the appropriate representatives as we can see in Table 7 indicated with different colors. For instance, all the sequences that share* $\Delta_{\alpha^{18}}=\left\{\binom{n}{4}+\binom{n}{5}+\binom{n}{9}+\binom{n}{10}+\binom{n}{11}\right\}$, *are represented in green or the sequences that share* $\Delta_{\alpha^{29}}=\left\{\binom{n}{2}+\binom{n}{4}+\binom{n}{5}+\binom{n}{9}+\binom{n}{11}+\binom{n}{12}\right\}$ *are represented in purple. From the cosets of order* 4 *and the corresponding union with the subgroup* $\mathcal{K}$ *we can obtain the subgroups of order* 8 *with the B-representation as follows*

$$
\begin{aligned}
S_8^{(1)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12} \right\} \\
S_8^{(2)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12} \right\} \\
S_8^{(3)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12} \right\} \\
S_8^{(4)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12} \right\} \\
S_8^{(5)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} \right\} \\
S_8^{(6)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11} \right\} \\
S_8^{(7)} &= \mathcal{K} \cup \left\{ \mathcal{K} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10} \right\}
\end{aligned}
$$

Table 7. Binomial representation of the generalized sequences for $p(x) = x^5 + x^2 + 1$.

p	Generalized Sequences	Binomial Representation
0	1111111111111111	$\binom{n}{0}$
1	1111010110000010	$\binom{n}{0} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}$
2	1110001101100100	$\binom{n}{0} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}$
3	1100011010001101	$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}$
4	1000111101000011	$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}$
5	0001110010011011	$\binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}$
6	0011001100001111	$\binom{n}{2} + \binom{n}{10} + \binom{n}{12}$
7	0110110000100111	$\binom{n}{1} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}$
8	1101101000010110	$\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}$
9	1011110001001100	$\binom{n}{0} + \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}$
10	0111000010111100	$\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}$
11	1110100100011001	$\binom{n}{0} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}$
12	1101000001101011	$\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}$
13	1010101010101010	$\binom{n}{0} + \binom{n}{1}$
14	0101010101010101	$\binom{n}{1}$
15	10100000110101111	$\binom{n}{0} + \binom{n}{1} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}$
16	0100001110110011	$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}$
17	1000010100111110	$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}$
18	0000101001111101	$\binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}$
19	0001011011100110	$\binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12}$
20	0010010111101001	$\binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10}$
21	0100100111001110	$\binom{n}{1} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}$
22	1001001111011000	$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}$
23	0010111110010100	$\binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}$
24	0101111100101000	$\binom{n}{1} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11}$
25	1011011000110001	$\binom{n}{0} + \binom{n}{1} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12}$
26	0110011001011010	$\binom{n}{1} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}$
27	1100110011110000	$\binom{n}{0} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}$
28	1001100110100101	$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{10} + \binom{n}{12}$
29	0011100101110010	$\binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12}$
30	0111101011000001	$\binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11}$

In conclusion, from a primitive polynomial of degree L, we can obtain 2^L generalized sequences which can be divided into 2^{L-2} disjoint subsets, including the trivial group $\mathcal{K} = \left\{ \mathbf{0}, \left\{ \binom{n}{0} \right\}, \left\{ \binom{n}{1} \right\}, \left\{ \binom{n}{0} + \binom{n}{1} \right\} \right\}$ and the cosets of size four constructed by bit-wise XORing a given generalized sequence with $\mathcal{K}$; or into $2^{L-2} - 1$ subgroups of order eight, formed by the union of $\mathcal{K}$ and the cosets of order four.

At this point, a question that arises in a natural way is whether it would be possible to obtain a generalized sequence from other sequences contained in other groups. Due to the additive group structure, the answer is affirmative.

4.2. Study of LC of Generalized Sequences

Linear complexity is a measure of unpredictability of pseudo-random sequences and it is a very important cryptographic property ([48], Section 2.3.5). Our aim in this section is to study the properties of the linear complexity of the family of generalized sequences, derived from their representations.

Cardell and Fúster-Sabater proved in [38] that we can deduce the linear complexity of any binary sequence with a period of the power of two from its B-representation.

Theorem 12 ([38], Corollary 3)**.** *Given a sequence with B-representation* $\sum_{k=1}^{t}\left\{\binom{n}{i_k}\right\}$*, where* $i_1 < i_2 < \cdots < i_t$ *are integer indexes, then the linear complexity of such a sequence is* $i_t + 1$*.*

As a consequence, we can introduce the following result.

Theorem 13. *All the generalized sequences corresponding to a coset* $S_4^{(i)}$ *of order* 4 *have the same LC.*

Proof. This result is immediate using the B-representation in the cosets. The LC of any generalized sequence in a given coset can be determined by the B-representation of the representative, denoted by Δ_s, since the rest of the sequences only differ from Δ_s in the binomial terms $\left\{\left\{\binom{n}{0}\right\},\left\{\binom{n}{1}\right\},\left\{\binom{n}{0}+\binom{n}{1}\right\}\right\}$, which will not affect the value of LC. □

From a high number of computational examples and as a consequence of the structure of the additive group, it is possible to observe that for a family of generalized sequences coming from a PN-sequence with a characteristic polynomial of degree L, we get $L-2$ different linear complexities LC_i satisfying

$$LC_1 > LC_2 > \cdots > LC_{L-3} > LC_{L-2},$$

with $LC_i > 2^{L-2}$, for $i = 1, 2, \ldots, L-2$; apart from the trivial ones, $LC \in \{0, 1, 2\}$, obtained in $\mathcal{K}$. There are $2^{L-(i+2)}$ cosets, each of them with four sequences and each sequence with linear complexity LC_i. The following example shows this fact.

Example 13. *Table 7 shows the family of generalized sequences obtained for the primitive polynomial* $p(x) = x^5 + x^2 + 1$*. We distinguish with different colors the* $2^{5-2} = 8$ *different cosets of* $\mathcal{S}$ *of order* 4*. According to Theorem 12, we can determine the LC of a generalized sequence from its B-representation; and, from Theorem 13 we have that the LC for all the generalized sequences in a coset is the same. In this example, we obtain three different linear complexities*

$$LC_1 = 13, \quad LC_2 = 12, \quad \textit{and} \quad LC_3 = 11,$$

which allows us to classify the cosets of $\mathcal{S}$ *according to their complexities as follows*

$$\begin{aligned} A_i &= \{\textit{ coset of sequences with } LC = 13\}, \textit{ for } i = 1, 2, 3, 4, \\ B_i &= \{\textit{ coset of sequences with } LC = 12\}, \textit{ for } i = 1, 2, \\ C &= \{\textit{ coset of sequences with } LC = 11\}, \end{aligned}$$

and the four trivial sequences of $\mathcal{K}$*, the sequences of which have* $LC = 1$ *and* $LC = 2$*.*

Example 14. *Consider the* 64 *generalized sequences obtained from the primitive polynomial* $p(x) = x^6 + x^5 + 1$*. In Appendix A we show a partition of the group of these generalized sequences* $\mathcal{S}$ *into* $2^{6-2} = 16$ *cosets of order* 4*. Note that we represent in bold the group* $\mathbb{K}$ *and then we add the representative of each coset of* $\mathcal{S}$*. Binomial numbers, marked with different colors, provide the complexities of the sequences in each coset. Recall that the binomial number with the highest index in the B-representation is* $\binom{n}{LC-1}$*.*

Next, we give a classification of the cosets of $\mathcal{S}$ of order 4 according to the value of theirs complexities

$$\begin{aligned} A_i &= \{ \textit{coset of sequences with } LC_1 = 28\}, \textit{ for } i = 1, 2, \ldots, 8, \\ B_i &= \{ \textit{coset of sequences with } LC_2 = 27\}, \textit{ for } i = 1, 2, 3, 4, \\ C_i &= \{ \textit{coset of sequences with } LC_3 = 26\}, \textit{ for } i = 1, 2, \\ D &= \{ \textit{coset of sequences with } LC_4 = 25\}, \end{aligned}$$

and the four trivial sequences of $\mathcal{K}$.

As we can see in Table 8, each term $\binom{n}{LC_i-1}$, $i = 1, 2, 3, 4$ appears in the B-representation of eight cosets. Furthermore, for every value of LC_i, $i = 1, 2, 3, 4$, there exist a coset, the B-representation of which only contains one of the four terms $\binom{n}{LC_i-1}$ but not the others. In this example, these cosets are A_7, B_2, C_1 and D. Therefore, if we have four sequences, each one of them in one of the cosets above, we can obtain the 64 generalized sequences.

Table 8. Binomial coefficients $\binom{n}{LC_i-1}$ in the different subgroups.

	$\binom{n}{27}$	$\binom{n}{26}$	$\binom{n}{25}$	$\binom{n}{24}$
A_1	✔	✔	✔	✔
A_2	✔			✔
A_3	✔	✔		✔
A_4	✔		✔	✔
A_5	✔		✔	
A_6	✔	✔		
A_7	✔			
A_8	✔	✔	✔	
B_1		✔	✔	
B_2		✔		
B_3		✔		✔
B_4		✔	✔	✔
C_1			✔	
C_2			✔	✔
D				✔

In general, given a primitive polynomial of degree L, we generate 2^L generalized sequences which can be divided into 2^{L-2} cosets and with $L-2$ different linear complexities LC_i, $i = 1, 2, \ldots, L-2$. Each term $\binom{n}{LC_i-1}$ appears 2^{L-3} times in the B-representations of the generalized sequences. As we checked previously, there are $L-2$ groups that have one element $\binom{n}{LC_i-1}$, $i = 1, 2, \ldots, L-2$, but not the others. Therefore, we only need $L-2$ sequences to generate the 2^L generalized sequences. We already knew this fact, since that $\mathcal{S}/\mathcal{K}$ is a vector space of dimension 2^{L-2} and thus can be generated by $L-2$ cosets modulo the subspace $\mathcal{K}$ of dimension 2.

5. Conclusions

In this work, we introduce and analyze new ways to represent the generalized sequences, from which we study different properties of the sequences. We introduce the B-representation that allows us to express such sequences by means of binomial sequences, that is, shifted versions of the diagonals of the Sierpinski's triangle. Furthermore, this representation lets us generate binary sequences with controllable parameters such as the period and the linear complexity. We have also defined the G and p-representation, both related between them. From the p-representation we can obtain the shifted version of the corresponding input PN-sequence of the GSSG and vice versa. Using this p-representation, we can define an isomorphism between the family of generalized sequences produced by a primitive

polynomial of degree L and the additive group $\mathbb{F}_{2^L}$. As a consequence, we can create a partition of the sequences into subsets of cardinal 4, known as the cosets. Moreover, the B-representations of the four generalized sequences in each coset exhibit a well defined pattern and similar characteristics. This fact might be exploited in the cryptanalysis of this generator.

We still have different open problems to solve. In Section 4.2, we have analyzed the linear complexity of generalized sequences, but some results are just conjectures. The partition of generalized sequences into cosets of the quotient group $\mathcal{S}/\mathcal{K}$ and the study of the linear complexity of the sequences in each coset have brought new questions to be solved. Furthermore, we want to prove that the period of any generalized sequence obtained from a primitive polynomial of degree L, except from the sequences with period 1 and 2, is always 2^{L-1} and that 2^{L-2} is a lower bound on the linear complexity. Finally, another interesting future line would be to study the generalized shelf-shrinking generator based on FCSRs (or similar structures), analyze their cryptographic properties and adapt all three representations to this new model.

Author Contributions: All authors contributed equally. All authors have read and agreed to the published version of the manuscript.

Funding: This research is partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project COPCIS, reference TIN2017-84844-C2-1-R. It is also supported by Comunidad de Madrid (Spain) under project CYNAMON (P2018/TCS-4566), co-funded by FSE and European Union FEDER funds. The first author is supported by CAPES (Brazil). Finally, the second and fourth author are partially supported by Spanish grant VIGROB-287 of the Universitat d'Alacant.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

LFSR	Linear Feedback Shift Register
PN-sequence	Pseudo-Noise sequence
LC	Linear Complexity
GSSG	Generalized Self-Shrinking Generator
GSS-sequence	Generalized Self-Shrunken Sequence
PRNG	Pseudo-Random Number Generator
FCSR	Feedback with Carry Shift Register

Appendix A

Generalized sequences for $p(x) = x^6 + x^5 + 1$.

$$\mathcal{K} = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\}$$

$$A_1 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{9} + \binom{n}{16} + \binom{n}{19} + \binom{n}{20} + \binom{n}{24} + \binom{n}{25} + \binom{n}{26} + \binom{n}{27}$$

$$A_2 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{4} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{11} + \binom{n}{14} + \binom{n}{17} + \binom{n}{18} + \binom{n}{22} + \binom{n}{23} + \binom{n}{24} + \binom{n}{27}$$

$$B_1 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{4} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11} + \binom{n}{14} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{20} + \binom{n}{22} + \binom{n}{23} + \binom{n}{25} + \binom{n}{26}$$

$$A_3 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{13} + \binom{n}{14} + \binom{n}{15} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{22} + \binom{n}{23} + \binom{n}{24} + \binom{n}{26} + \binom{n}{27}$$

$$C_1 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{3} + \binom{n}{8} + \binom{n}{10} + \binom{n}{13} + \binom{n}{14} + \binom{n}{15} + \binom{n}{17} + \binom{n}{18} + \binom{n}{20} + \binom{n}{22} + \binom{n}{23} + \binom{n}{25}$$

$$B_2 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{3} + \binom{n}{4} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{13} + \binom{n}{15} + \binom{n}{16} + \binom{n}{19} + \binom{n}{26}$$

$$A_4 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{10} + \binom{n}{11} + \binom{n}{13} + \binom{n}{15} + \binom{n}{20} + \binom{n}{24} + \binom{n}{25} + \binom{n}{27}$$

$$A_5 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \binom{n}{7} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{14} + \binom{n}{15} + \binom{n}{16} + \binom{n}{20} + \binom{n}{25} + \binom{n}{27}$$

$$B_3 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{14} + \binom{n}{15} + \binom{n}{19} + \binom{n}{24} + \binom{n}{26}$$

$$C_2 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{6} + \binom{n}{8} + \binom{n}{10} + \binom{n}{12} + \binom{n}{13} + \binom{n}{15} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{20} + \binom{n}{22} + \binom{n}{23} + \binom{n}{24} + \binom{n}{25}$$

$$A_6 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{12} + \binom{n}{13} + \binom{n}{15} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{22} + \binom{n}{23} + \binom{n}{26} + \binom{n}{27}$$

$$B_4 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{20} + \binom{n}{22} + \binom{n}{23} + \binom{n}{24} + \binom{n}{25} + \binom{n}{26}$$

$$A_7 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{7} + \binom{n}{8} + \binom{n}{11} + \binom{n}{12} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{22} + \binom{n}{23} + \binom{n}{27}$$

$$A_8 = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{5} + \binom{n}{7} + \binom{n}{9} + \binom{n}{12} + \binom{n}{14} + \binom{n}{19} + \binom{n}{20} + \binom{n}{25} + \binom{n}{26} + \binom{n}{27}$$

$$D = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\} + \binom{n}{2} + \binom{n}{6} + \binom{n}{12} + \binom{n}{14} + \binom{n}{16} + \binom{n}{24}$$

References

1. Fischer, V. A Closer Look at Security in Random Number Generators Design. In *Constructive Side-Channel Analysis and Secure Design, COSADE 2012*; Schindler, W., Huss, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7275, Lecture Notes in Computer Science, pp. 167–182.
2. Francillon, A.; Castelluccia, C. TinyRNG: A Cryptographic Random Number Generator for Wireless Sensors Network Nodes. In Proceedings of the 2007 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops, Limasso, Cyprus, 16–20 April 2007; pp. 1–7.
3. Biryukov, A.; Shamir, A.; Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. In *Proceedings of Fast Software Encryption 2000*; Goos, G., Hartmanis, J., Van Leeuwen, J., Schneier, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 1978, Lecture Notes in Computer Science, pp. 1–18.
4. Petrovic, S.; Fúster-Sabater, A. Cryptanalysis of the A5/2 Algorithm. *IACR Cryptol. EPrint Arch.* **2000**, *2000*, 52.
5. Paul, G.; Maitra, S. *RC4 Stream Cipher and its Variants*; CRC Press, Taylor and Francis Group: Boca Raton, FL, USA, 2012.
6. Peinado, A.; Munilla, J.; Fúster-Sabater, A. EPCGen2 Pseudorandom Number Generators: Analysis of J3Gen. *Sensors* **2014**, *14*, 6500–6515.
7. Dutta, I.K.; Ghosh, B.; Bayoumi, M. Lightweight Cryptography for Internet of Insecure Things: A Survey. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0475–0481.
8. Philip, M.A.; Vaithiyanathan. A survey on lightweight ciphers for IoT devices. In Proceedings of the 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam, India, 21–23 December 2017; pp. 1–4.
9. Dubrova, E.; Hell, M. Espresso: A stream cipher for 5G wireless communication systems. *Cryptogr. Commun.* **2017**, *9*, 273–289.
10. Orúe López, A.B.; Hernández Encinas, L.; Montoya Vitini, F. Trifork, a new Pseudorandom Number Generator Based on Lagged Fibonacci Maps. *J. Comput. Sci. Eng.* **2010**, *2*, 46–51.
11. Paar, C.; Pelzl, J. *Understanding Cryptography*; Springer: Berlin, Germany, 2010.
12. Golomb, S.W. *Shift Register-Sequences*; Aegean Park Press: Laguna Hill, CA, USA, 1982.
13. Biryukov, A.; Perrin, L. State of the Art in Lightweight Symmetric Cryptography. *IACR Cryptol. EPrint Arch.* **2017**, *2017*, 511.
14. Orúe López, A.B.; Hernández Encinas, L.; Martín Muñoz, A.; Montoya Vitini, F. A Lightweight Pseudorandom Number Generator for Securing the Internet of Things. *IEEE Access* **2017**, *5*, 27800–27806.
15. Hassan, S. ans Bokhari, M.U. Design of Pseudo Random Number Generator using Linear Feedback Shift Register. *Int. J. Eng. Adv. Technol. (IJEAT)* **2019**, *9*, 1956–1965.
16. Rahimov, H.; Babaei, M.; Farhadi, M. Cryptographic PRNG based on combination of LFSR and chaotic logistic map. *Appl. Math.* **2011**, *2*, 1531–1534.
17. Duvall, P.F.; Mortick, J.C. Decimation of Periodic Sequences. *SIAM J. Appl. Math.* **1971**, *21*, 367–372.
18. Díaz Cardell, S.; Fúster-Sabater, A. *Cryptography with Shrinking Generators: Fundamentals and Applications of Keystream Sequence Generators Based on Irregular Decimation*; Springer Briefs in Mathematics; Springer International Publishing: Cham, Switzerland, 2019.
19. Coppersmith, D.; Krawczyk, H.; Mansour, Y. The shrinking generator. In *Advances in Cryptology—CRYPTO '93*; Stinson, D., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; Volume 773, Lecture Notes in Computer Science, pp. 22–39.
20. Meier, W.; Staffelbach, O. The Self-Shrinking Generator. In *Advances in Cryptology—EUROCRYPT 1994*; De Santis, A., Ed.; Springer: Berlin/Heidelberg, Germany, 1995; Volume 950, Lecture Notes in Computer Science, pp. 205–214.
21. Hu, Y.; Xiao, G. Generalized Self-Shrinking Generator. *IEEE Trans. Inf. Theory* **2004**, *50*, 714–719.
22. Zhang, B.; Feng, D. New Guess-and-Determine Attack on the Self-Shrinking Generator. In *Advances in Cryptology —ASIACRYPT 2006*; Lai, X.; Chen, K., Eds.; Springe: Berlin/Heidelberg, Germany, 2006; Volume 4284, Lecture Notes in Computer Science, pp. 54–68.
23. Kanso, A. Modified self-shrinking generator. *Comput. Electr. Eng.* **2010**, *36*, 993–1001.
24. Cardell, S.D.; Fúster-Sabater, A. The *t*-Modified Self-Shrinking Generator. In *Computational Science—ICCS 2018*; Shi, Y., Fu, H., Tian, Y., Krzhizhanovskaya, V.V., Lees, M.H., Dongarra, J., Sloot, P.M.A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; Volume 10860, Lecture Notes in Computer Science, pp. 653–663.

25. Cardell, S.D.; Requena, V.; Fúster-Sabater, A.; Orúe, Amalia, B. Randomness Analysis for the Generalized Self-Shrinking Sequences. *Symmetry* **2020**, *2020*, 1460.
26. Cardell, S.D.; Fúster-Sabater, A. Discrete linear models for the generalized self-shrunken sequences. *Finite Fields Their Appl.* **2017**, *47*, 222–241.
27. Tasheva, A.T.; Tasheva, Z.N.; Petrov, A. Generalization of the Self-Shrinking Generator in the Galois Field $GF(p^n)$. *Adv. Artif. Intell.* **2011**, *2011*, 1–10. doi:10.1155/2011/464971.
28. Dong, L.; Zeng, Y.; Hu, Y. F-GSS: A Novel FCSR-Based Keystream Generator. In Proceedings of the 2009 First International Conference on Information Science and Engineering, Nanjing, China, 26–28 December 2009; pp. 1737–1740.
29. Wang, H.; Wen, Q.; Zhang, J. The Properties of the FCSR-Based Self-Shrinking Sequence. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2013**, *E96.A*, 626–634.
30. Ali, A. Feedback with carry shift registers and (in-depth) security of ciphers based on this primitive. In Proceedings of the 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 9–13 January 2018; pp. 431–438.
31. Goresky, M.; Klapper, A. Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Trans. Inf. Theory* **1997**, *43*, 1342–1345.
32. Stoyanov, B. Self-shrinking bit generation algorithm based on feedback with carry shift register. *Adv. Stud. Theor. Phys.* **2014**, *8*, 1057–1061.
33. Bandelow, C. *Inside Rubik's Cube and Beyond*; Birkhäuser Boston: Cambridge, MA, USA, 1982.
34. Jacobs, P. *Group Theory with Applications in Chemical Physics*; Cambridge University Press: Cambridge, UK, 2005.
35. Liu, Y.; Hel-Or, H.; Kaplan, C.S.; Van Gool, L. Computational Symmetry in Computer Vision and Computer Graphics. *Found. Trends Comput. Graph. Vis.* **2009**, *5*, 1–195. doi:10.1561/0600000008.
36. Lyubarskii, G. *The Application of Group Theory in Physics*; Pergamon, Elsevier, Turkey, 1960.
37. Zhang, J.; Xiong, F.; Kang, J. The Application of Group Theory in Communication Operation Pipeline System. *Math. Probl. Eng.* **2018**, *2018*, 1–10. doi:10.1155/2018/9507823.
38. Cardell, S.D.; Fúster-Sabater, A. Binomial Representation of Cryptographic Binary Sequences and Its Relation to Cellular Automata. *Complexity* **2019**, *2019*, 1–13. doi:10.1155/2019/2108014.
39. Blackburn, S.R. The linear complexity of the self-shrinking generator. *IEEE Trans. Inf. Theory* **1999**, *45*, 2073–2077.
40. Fúster-Sabater, A.; Cardell, S.D. Linear complexity of generalized sequences by comparison of PN-sequences. *RACSAM* **2020**, *2020*. doi:10.1007/s13398-020-00807-5.
41. Key, E.L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators. *IEEE Trans. Inf. Theory* **1976**, *22*, 732–736.
42. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
43. National Institute of Standards and Technology. NIST Lightweight Crypto Standardization Process 2019. Available online: https://csrc.nist.gov/Projects/Lightweight-Cryptography/Round-1-Candidates (accessed on June 2020).
44. Huber, K. Some comments on Zech's logarithms. *IEEE Trans. Inf. Theory* **1990**, *36*, 946–950.
45. Fúster-Sabater, A. Generation of Cryptographic Sequences by means of Difference Equations. *Appl. Math. Inf. Sci.* **2014**, *8*, 475–484.
46. Birkhoff, G.; Mac Lane, S. *A Survey of Modern Algebra*; Macmillan: New York, NY, USA, 1996.
47. Joshi, K.D. *Foundations of discrete mathematics*; Wiley: New York, NY, USA; Wiley Eastern Ltd: New Delhi, India, 1989.
48. Cusick, Thomas W.and Ding, C.; Renvall, A. *Stream Ciphers and Number Theory*; North-Holland Mathematical Library: Amsterdam, Netherlands, 2004.