

Binomial Characterization of Cryptographic Sequences

Sara D. Cardell[1(✉)] and Amparo Fúster-Sabater[2]

[1] Instituto de Matemática, Estatística e Computação Científica, UNICAMP, R. Sérgio Buarque de Holanda, 651, Campinas, SP 13083-859, Brazil
sdcardell@ime.unicamp.br

[2] Instituto de Tecnologías Físicas y de la Información, C.S.I.C., Serrano 144, 28006 Madrid, Spain
amparo@iec.csic.es

Abstract. The generalized self-shrinking generator is a sequence generator that produces binary sequences with good cryptographic properties. On the other hand, the binomial sequences are a well-defined class of sequences that can be obtained considering infinite successions of binomial coefficients modulo 2. In this work, we see that the generalized sequences can be computed as a finite binary sum of binomial sequences. Moreover, the cryptographic parameters of the generalized sequences can be studied in terms of the binomial sequences.

Keywords: Generalized generator · Binomial sequence · Binomial characterization · Decimation · Cryptography

1 Introduction

Protection of confidential information uses an encryption function called *cipher* to convert the original message or *plaintext* into the ciphered message or *ciphertext*. In symmetric cryptography, there is a single piece of secret information called *key* that is shared by both communicating parties.

Inside the symmetric cryptography, stream ciphers are the simplest and fastest among all the encryption procedures so they are in widespread use and can be found in different technological applications e.g. the encryption system E0 in Bluetooth network specifications [6], the SNOW 3G Generator [12] in wireless communication of high-speed data with 4G/LTE (Long-Term Evolution) technology or the algorithm RC4 in Microsoft Word and Excel spreadsheet [17]. The conjunction of simplicity and speed in a single process preserves the leading part of the stream ciphers in any cryptographic application.

The main concern in stream cipher design is to generate from a short and truly random key a long and pseudorandom sequence called *keystream* sequence. For encryption, the sender performs the bitwise XOR (exclusive-OR) operation among the bits of the plaintext and the keystream sequence. The result is the ciphertext that is sent to the receiver. For decryption, the receiver generates the

© Springer Nature Switzerland AG 2019
S. Misra et al. (Eds.): ICCSA 2019, LNCS 11619, pp. 803–816, 2019.
https://doi.org/10.1007/978-3-030-24289-3_59

same keystream sequence, performs the same bitwise XOR operation between the received ciphertext and the keystream sequence and recovers the original message. Recall that both encryption and decryption procedures use the same XOR logic operation, that is a simple and balanced operation.

Most keystream generators are based on maximal-length Linear Feedback Shift Registers (LFSRs) [10] whose output sequences, the so-called PN-sequences, are combined in a nonlinear way to produce pseudorandom sequences for cryptographic application. Nonlinear filters, combinational generators, clock-controlled generators or irregularly decimated generators are some of the most popular keystream generators. See [9,15,16] for a comprehensive introduction to this topic.

Inside the family of irregularly decimated generators, we can enumerate: (a) the *shrinking generator* [5] that involves two LFSRs, (b) the *self-shrinking generator* [14] involving only one LFSR and (c) the most representative element of this family, the *generalized self-shrinking generator* or family of generators [11], that includes the self-shrinking generator as one of its members. Irregularly decimated generators produce sequences that exhibit good cryptographic properties: long periods, excellent run distribution and self-correlation, balancedness [7], simplicity of implementation, etc. The underlying idea of this type of generators is the irregular decimation of a PN-sequence according to the bits of another. The decimation result is a sequence that will be used as keystream sequence in the encryption/decryption procedure. This work focuses on the generalized self-shrinking generators and their output sequences the so-called *generalized self-shrunken sequences* (GSS sequences) or simply generalized sequences.

On the other hand, the binomial sequences are a family of binary sequences whose terms are binomial numbers reduced modulo 2. More precisely, the binomial sequences correspond to the diagonals of the Sierpinski's triangle modulo 2. In this way, the binomial sequences exhibit many attractive properties that can be very useful in the analysis and generation of keystream sequences. In this work, it is shown the close relationship between generalized sequences and the class of binomial sequences, in the sense that these binomial sequences can be used to analyse the cryptographic properties of those generalized sequences.

The work is organized as follows. Fundamental and basic concepts used throughout the work are introduced in Sect. 2. Next in Sect. 3, the characteristics of the binomial sequences are discussed in detail. The representation and computation of generalized sequences in terms of binomial sequences is the subject of Sect. 4. Finally, conclusions in Sect. 5 end the paper.

2 Preliminaries

In this section, we present some basic concepts about sequences that we need to know before introducing the main results.

2.1 Binary Sequences

Let $\mathbb{F}_2$ be the Galois field of two elements. We say $\{a_n\} = \{a_0, a_1, a_2 \ldots\}$ is a binary sequence if its terms $a_n \in \mathbb{F}_2$, for $n = 0, 1, 2, \ldots$. The sequence $\{a_n\}$ is periodic if and only if there exists an integer T such that $a_{n+T} = a_n$, for all $n \geq 0$.

Let r be a positive integer, and let $d_1, d_2, d_3, \ldots, d_r$ be constant coefficients with $d_i \in \mathbb{F}_2$. A binary sequence $\{a_n\}$ satisfying the relationship

$$a_{n+r} = d_r a_n + d_{r-1} a_{n+1} + \cdots + d_3 a_{n+r-3} + d_2 a_{n+r-2} + d_1 a_{n+r-1}, \quad n \geq 0, \quad (1)$$

is called a (r-th order) linear recurring sequence in $\mathbb{F}_2$. The terms $\{a_0, a_1, \ldots, a_{r-1}\}$ are referred to as the initial values (or initial state) and determine the rest of the sequence uniquely. A relation of the form given by the Eq. (1) is called a (r-th order) linear recurrence relationship.

The monic polynomial

$$p(x) = d_r + d_{r-1} x + \cdots + d_3 x^{r-3} + d_2 x^{r-2} + d_1 x^{r-1} + x^r \in \mathbb{F}_2[x]$$

is called the characteristic polynomial of the linear recurring sequence and $\{a_n\}$ is said to be generated by $p(x)$.

The generation of linear recurring sequences can be implemented on Linear Feedback Shift Registers (LFSRs) [10]. These structures handle information in the form of binary elements and they are based on shifts and linear feedback. In fact, a LFSR is an electronic device with r memory cells (stages), shift to the adjacent stage and linear feedback to the empty stage. If the characteristic polynomial of the linear recurring sequence is primitive [10], then the LFSR is said to be maximal-length and its output sequence has period $T = 2^r - 1$. Such an output sequence is called PN-sequence (pseudonoise sequence).

Linear complexity, LC, is a much used metric of the security of a keystream sequence [16]. Roughly speaking, LC measures the amount of sequence bits needed to reconstruct the rest of the sequence. In a more precise way, LC of a sequence $\{a_n\}$ is defined as the length of the shortest LFSR that generates such a sequence or, equivalently, as the lowest order linear recurrence relationship that generates such a sequence. In cryptographic terms, LC must be as large as possible; the recommended value is approximately half the sequence period, $LC \simeq T/2$.

2.2 The Family of Generalized Sequences

The more representative element in the class of irregularly decimated generators is the generalized self-shrinking generator (or simply generalized generator) [11], a particularization of the shrinking generator [3,5] that includes the sequences generated by: the self-shrinking generator [1,14], the modified self-shrinking generator [2,13] and the t-modified self-shrinking generator [4]. The family of generalized sequences is described as follows:

Definition 1. *Let* $\{a_n\}$ $(n = 0, 1, 2, \dots)$ *be a PN-sequence generated by a maximal-length LFSR with an* L*-degree characteristic polynomial. Let* p *be an integer and* $\{v_n\}$ $(n = 0, 1, 2, \dots)$ *be an* p*-position left shifted version of* $\{a_n\}$ *with* $(p = 0, 1, 2, \dots, 2^L - 2)$*. The decimation rule is very simple:*

1. *If* $a_n = 1$*, then* v_n *is output.*
2. *If* $a_n = 0$*, then* v_n *is discarded and there is no output bit.*

Thus, for each p *an output sequence* $\{s_0\, s_1\, s_2 \dots\}$ *denoted by* $\{S(p)_n\}$ $(n \geq 0)$ *is generated. Such a sequence is called the generalized self-shrunken sequence (GSS-sequence) (or simply generalized sequence) associated with the shift* p*.*

Recall that $\{a_n\}$ remains fixed while $\{v_n\}$ is the sliding sequence or left-shifted version of $\{a_n\}$. When p ranges in the interval $p \in [0, 1, 2, \dots, 2^L - 2]$, then the family of $2^L - 1$ generalized sequences is obtained. For each possible sequence $\{v_n\}$ and after the application of the decimation rule, a new generalized sequence is generated. The GSS-sequence family includes the $2^L - 1$ generalized self-shrunken sequences plus the identically null sequence. Some important facts extracted from [8,11] are enumerated:

1. This family always includes [8] the sequence $\{111111\dots\}$ for $p = 0$ and the sequences $\{101010\dots\}$ and $\{010101\dots\}$ for $p = q, q+1$, respectively, where q is an integer corresponding to the power $\alpha^q \in \mathbb{F}_{2^L}$ satisfying $\alpha^{q+1} = \alpha^q + 1$.
2. All the sequences in this family are balanced except for sequences $\{0000\dots\}$ and $\{1111\dots\}$, [11, Theorem 1].
3. By construction, the family of generalized self-shrinking sequences consists of 2^L sequences of 2^{L-1} bits each of them [11, Section I]. Consequently, the period of each one of these sequences is a factor of 2^{L-1}.
4. The family of generalized self-shrinking sequences has structure of Abelian group whose group operation is the bit-wise addition mod 2, the neutral element is the sequence $\{0000\dots\}$ and the inverse element of each sequence is the own sequence, [11, Theorem 2].
5. The self-shrinking sequence is a member of the GSS-sequence family [11, Section I] with shift $p = 2^{L-1}$.

Example 1. For an LFSR with characteristic polynomial $p(x) = 1 + x + x^4$ and initial state $\{1\ 1\ 1\ 1\}$, we get the generalized sequences (GSS-sequences) shown in Table 1. The bits in bold in the different sequences $\{v_n\}$ are the digits of the corresponding GSS-sequences associated to their corresponding p. The PN-sequence $\{a_n\}$ with period $T = 2^4 - 1$ is written at the bottom of the table. Note that the sequences corresponding to $p = 2, 8$ are the same but starting at different terms. The same holds for the sequences corresponding to $p = 1, 5, 6, 14$ and $p = 3, 4, 10, 13$. In brief, inside the family of generalized sequences there are shifted versions of the same sequence.

Next a new class of binary sequences that allow one to analyze the GSS-sequences are introduced.

Table 1. GSS-sequences for $p(x) = 1 + x + x^4$

p	$\{v_n\}$ sequences	GSS-sequence
0	**1111**0001**0011**0**1**0	11111111
1	**1110**0010**0**11**0**1**0**1	11100100
2	**1100**0100**1**1**0**1**0**11	11000011
3	**1000**1001**1**10**1**0**1**11	10001101
4	**0001**0011**0**10**1**1**1**1	00011011
5	**0010**0110**1**0**1**11**1**10	00100111
6	**0100**1101**0**1**1**1**1**00	01001110
7	**1001**1010**1**1**1**1**0**0	10010110
8	**0011**0101**1**1**1**0**0**01	00111100
9	**0110**1011**1**1**0**0**1**0	01101001
10	**1101**0111**1**0**0**1**0**0	11011000
11	**1010**1111**0**0**1**0**0**1	10101010
12	**0101**1110**0**0**1**0**1**1	01010101
13	**1011**1100**0**1**0**0**1**0	10110001
14	**0111**1000**1**0**1**1**0**1	01110010
	11110001**0011**0**1**0	

Table 2. Binomial coefficients, binomial sequences, periods and complexities

Binomial coeff.	Binomial sequences	Period	Linear complexity
$\binom{n}{0}$	1 1 1 1 1 1 1 1	$T_0 = 1$	$LC_0 = 1$
$\binom{n}{1}$	0 1 0 1 0 1 0 1	$T_1 = 2$	$LC_1 = 2$
$\binom{n}{2}$	0 0 1 1 0 0 1 1	$T_2 = 4$	$LC_2 = 3$
$\binom{n}{3}$	0 0 0 1 0 0 0 1	$T_3 = 4$	$LC_3 = 4$
$\binom{n}{4}$	0 0 0 0 1 1 1 1	$T_4 = 8$	$LC_4 = 5$
$\binom{n}{5}$	0 0 0 0 0 1 0 1	$T_5 = 8$	$LC_5 = 6$
$\binom{n}{6}$	0 0 0 0 0 0 1 1	$T_6 = 8$	$LC_6 = 7$
$\binom{n}{7}$	0 0 0 0 0 0 0 1	$T_7 = 8$	$LC_7 = 8$

3 Binomial Sequences

The binomial coefficient $\binom{n}{i}$ is the coefficient of the power x^i in the polynomial expansion of $(1 + x)^n$. For every positive integer n, it is a well-known fact that $\binom{n}{0} = 1$ and $\binom{n}{i} = 0$ for $i > n$. Moreover, it is worth noticing that if we arrange these binomial coefficients into rows for successive values of $n = 0, 1, 2, \ldots$, then the generated structure is the Pascal's triangle (see Fig. 1a). The most-left diagonal is the identically 1 sequence, the next diagonal is the sequence of natural numbers $\{1, 2, 3, \ldots\}$, the next one is the sequence of triangular num-

(a) Binomial coefficients arranged as the Pascal's triangle

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$

(b) Sierpinski's triangle

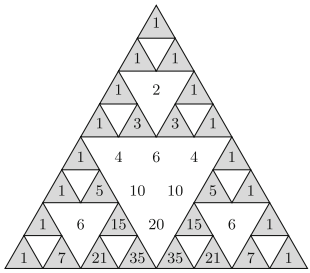

Fig. 1. Pascal's and Sierpinski's triangles

bers $\{1, 3, 6, 10, \ldots\}$, etc. Other interesting sequences (tetrahedral numbers, pentatope numbers, hexagonal numbers, Fibonacci sequence, etc.) can be found over the diagonals of this triangle. On the other hand, if we color the odd numbers of the Pascal's triangle and shade the other ones, we can find the Sierpinski's triangle (see Fig. 1b).

The binomial coefficients reduced modulo 2 allow us to introduce the concept of binomial sequence.

Definition 2. *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 known as the ***binary k-th binomial sequence****.*

Table 2 shows the binomial sequences and the values of their periods and linear complexities, denoted by T_k and LC_k, respectively, for the first binomial coefficients $\binom{n}{k}$, $k = 0, 1, \ldots, 7$. In Appendix A, one can find the first 32 binomial sequences. Moreover, we can see the pattern and repetitive structure of such sequences.

Recall that the successive binomial sequences correspond to the successive diagonals of the Sierpinski's triangle (see Fig. 1b) reduced modulo 2.

Next, the relation between binomial sequences and every binary sequence with period a power of 2 appears in the following result.

Theorem 1. *Let $\{z_n\}$ be a binary sequence with period $T = 2^L$, L being a positive integer. Then, every binary sequence $\{z_n\}$ can be written as a linear combination of binomial sequences.*

Proof. Since the period of $\{z_n\}$ is a power of 2, then the next equation holds:

$$(E^{2^L} + 1)z_n = (E + 1)^{2^L} z_n = 0,$$

Table 3. GSS-sequences for $p(x) = 1 + x + x^4$

p	α^p	$\{S(p)\}$	p	α^p	$\{S(p)\}$
0	1	1 1 1 1 1 1 1 1	8	$\alpha^8 = 1 + \alpha^2$	0 0 1 1 1 1 0 0
1	α	1 1 1 0 0 1 0 0	9	$\alpha^9 = \alpha + \alpha^3$	0 1 1 0 1 0 0 1
2	α^2	1 1 0 0 0 0 1 1	10	$\alpha^{10} = 1 + \alpha + \alpha^2$	1 1 0 1 1 0 0 0
3	α^3	1 0 0 0 1 1 0 1	11	$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$	1 0 1 0 1 0 1 0
4	$\alpha^4 = 1 + \alpha$	0 0 0 1 1 0 1 1	12	$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$	0 1 0 1 0 1 0 1
5	$\alpha^5 = \alpha + \alpha^2$	0 0 1 0 0 1 1 1	13	$\alpha^{13} = 1 + \alpha^2 + \alpha^3$	1 0 1 1 0 0 0 1
6	$\alpha^6 = \alpha^2 + \alpha^3$	0 1 0 0 1 1 1 0	14	$\alpha^{14} = 1 + \alpha^3$	0 1 1 1 0 0 1 0
7	$\alpha^7 = 1 + \alpha + \alpha^3$	1 0 0 1 0 1 1 0			

where E is the shifting operator that acts on the terms of a sequence $\{a_n\}$, that is: $E^k a_n = a_{n+k}$ for all integer $k \geq 0$.

The characteristic polynomial of the previous equation is $(x + 1)^m$ with $m = 2^L$, that is $x = 1$ is the unique root of the polynomial $(x + 1)$ but with multiplicity m. Therefore, the binary solutions of this equation are given [9] by the expression:

$$z_n = c_0 \binom{n}{0} + c_1 \binom{n}{1} + \cdots + c_{T-1} \binom{n}{T-1} \quad \text{for } n \geq 0, \tag{2}$$

where the coefficients $c_i \in \mathbb{F}_2$ and $\binom{n}{i}$ are binomial coefficients reduced modulo 2. When n takes successive values $n = 0, 1, 2, \ldots$, then each binomial coefficient modulo 2 defines a different binomial sequence. Thus, the sequence $\{z_n\}$ is just the bit-wise XOR of such binomial sequences weighted by binary coefficients c_i.

Different choices of c_i will produce different sequences $\{z_n\}$ with distinct characteristics and properties, but all of them with period 2^l, $0 \leq l \leq L$.

Since the generalized sequences have periods that are powers of 2, then the previous theorem can be directly applied to the GSS-sequence family. In this way, every generalized sequence can be written as a linear combination of binomial sequences as shown in the Eq. (2).

4 Binomial Characterization of Generalized Sequences

According to Theorem 1, a binary sequence of period power of 2 is the bit-wise XOR of binomial sequences. Therefore, we introduce the following definition.

Definition 3. *The set of binomial sequences necessary to obtain a binary sequence of period power of* 2 *is called the* ***binomial characterization*** *of such a sequence.*

In this section, we analyze the binomial characterization of the different sequences in the class of GSS-sequences. Let $\mathbb{F}_{2^L}$ be an additive group, then we can construct the group isomorphism:

$$\begin{aligned} \phi : (\mathbb{F}_{2^L}, +) &\longrightarrow (\mathcal{S}, +) \\ \alpha^p &\longrightarrow \{S(p)\}, \end{aligned} \tag{3}$$

which defines a relationship between α^p (α being a root of $p(x)$, the LFSR characteristic polynomial) and the generalized sequence $\{S(p)\}$ (see Table 3 for the isomorphism (3) corresponding to the polynomial $p(x) = 1 + x + x^4$).

Now, we are going to write the most simple sequences of the generalized sequence family in terms of their binomial characterizations. In fact, we have seen in Subsect. 2.2 that there exists an integer $q \in \{0, 1, \ldots, 2^{L-2}\}$ such that $\alpha^{q+1} = 1 + \alpha^q$. The generalized sequences corresponding to α^q and α^{q+1} are $\{1\,0\,1\,0\,1\,0\,1\,0\ldots\}$ and $\{0\,1\,0\,1\,0\,1\,0\,1\ldots\}$ and their binomial characterizations are $\binom{n}{0} + \binom{n}{1}$ and $\binom{n}{1}$, respectively. In the same way, for α^0 its corresponding generalized sequence is $\{1\,1\,1\,1\,1\,1\,1\,1\ldots\}$ with binomial characterization $\binom{n}{0}$. Coming back to Example 1, we have now that $q = 11$ and consequently

$$\begin{aligned} \phi(\alpha^{11}) = \{S(11)\} = \{1\,0\,1\,0\,1\,0\,1\,0\ldots\} &= \binom{n}{0} + \binom{n}{1} \\ \phi(\alpha^{12}) = \{S(12)\} = \{0\,1\,0\,1\,0\,1\,0\,1\ldots\} &= \binom{n}{1} \\ \phi(\alpha^{0}) = \{S(0)\} = \{1\,1\,1\,1\,1\,1\,1\,1\ldots\} &= \binom{n}{0} \end{aligned}$$

These three basic binomial characterizations allow us to determine the binomial representation for the rest of generalized sequences.

4.1 Partition of the Generalized Sequences

In this section we study the additive subgroups of $(\mathbb{F}_{2^L}, +)$, which will help us to divide the set of generalized sequences associated to a given polynomial into separated groups.

Let us start considering the additive subgroup of $\mathbb{F}_{2^L}$ of order 4 given by:

$$\mathcal{S}_4 = \{0, 1, \alpha^q, \alpha^{q+1}\}.$$

If we denote the zero sequence by $\mathbf{0}$, the corresponding sequences through the isomorphism defined in Eq. (3) are:

$$\phi(\mathcal{S}_4) = \left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\right\}$$

Consider now every subgroup of order 8 that contains $\mathcal{S}_4$. They are of the form

$$\{0, 1, \alpha^q, \alpha^{q+1}, \alpha^{q_1}, \alpha^{q_2}, \alpha^{q_3}, \alpha^{q_4}\},$$

Table 4. Binomial characterization of the GSS-sequences $\{S(p)\}$ of Example 1

p	$\{S(p)\}$	Binomial characterization
0	1 1 1 1 1 1 1 1	$\binom{n}{0}$
1	1 1 1 0 0 1 0 0	$\binom{n}{0}+\binom{n}{3}+\binom{n}{4}+\binom{n}{5}$
2	1 1 0 0 0 0 1 1	$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}$
3	1 0 0 0 1 1 0 1	$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\binom{n}{5}$
4	0 0 0 1 1 0 1 1	$\binom{n}{3}+\binom{n}{4}+\binom{n}{5}$
5	0 0 1 0 0 1 1 1	$\binom{n}{2}+\binom{n}{3}+\binom{n}{5}$
6	0 1 0 0 1 1 1 0	$\binom{n}{1}+\binom{n}{3}+\binom{n}{4}+\binom{n}{5}$
7	1 0 0 1 0 1 1 0	$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{4}$
8	0 0 1 1 1 1 0 0	$\binom{n}{2}+\binom{n}{4}$
9	0 1 1 0 1 0 0 1	$\binom{n}{1}+\binom{n}{2}+\binom{n}{4}$
10	1 1 0 1 1 0 0 0	$\binom{n}{0}+\binom{n}{2}+\binom{n}{3}+\binom{n}{5}$
11	1 0 1 0 1 0 1 0	$\binom{n}{0}+\binom{n}{1}$
12	0 1 0 1 0 1 0 1	$\binom{n}{1}$
13	1 0 1 1 0 0 0 1	$\binom{n}{0}+\binom{n}{1}+\binom{n}{3}+\binom{n}{4}+\binom{n}{5}$
14	0 1 1 1 0 0 1 0	$\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\binom{n}{5}$

such that,

$$\begin{aligned}\alpha^{q_1}+\alpha^{q_2}&=1,\\ \alpha^{q_1}+\alpha^{q_3}&=\alpha^{q},\\ \alpha^{q_1}+\alpha^{q_4}&=\alpha^{q+1}.\end{aligned}$$

Clearly, the binomial characterization of the corresponding sequences will have a common part $\Delta=\sum_{i=2}^{2^{L-1}-(L-2)}a_i\binom{n}{i}$, with $a_i\in\mathbb{F}_2$ and they will have the form:

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

Example 2. Consider again the Example 1. In Table 4, we can see the binomial characterization of each GSS-sequence produced by $p(x)=1+x+x^4$. For instance, consider the four sequences:

$$\left\{\binom{n}{4}+\binom{n}{2},\binom{n}{4}+\binom{n}{2}+\binom{n}{0},\binom{n}{4}+\binom{n}{2}+\binom{n}{1},\binom{n}{4}+\binom{n}{2}+\binom{n}{0}+\binom{n}{1}\right\}$$

Their common part is $\Delta=\binom{n}{4}+\binom{n}{2}$ and they correspond to $\alpha^8,\alpha^2,\alpha^9$ and α^7, respectively. In this case, $q=11$ and the corresponding additive subgroup is:

$$\{0,1,\alpha^{11},\alpha^{12},\alpha^8,\alpha^2,\alpha^9,\alpha^7\}$$

As a consequence of what we have seen before, we can divide the set of GSS-sequences into sets of four elements each of them sharing the same common part. Therefore, given a primitive polynomial of degree L, we can generate 2^L GSS-sequences that can be divided into 2^{L-2} groups (including the trivial group $\left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0}+\binom{n}{1}\right\}$).

In addition, it is possible to determine the linear complexity and period of the different generalized sequences in terms of their binomial characterizations.

The linear complexity of a generalized sequence is given by the expression:

$$LC = k + 1,$$

where k is the greatest integer of the sequence $\binom{n}{k}$ in the binomial characterization of the generalized sequence.

The period of a generalized sequence is the period of the binomial sequence $\binom{n}{k}$ where k is the greatest integer in the binomial characterization of the generalized sequence. In Example 1, for sequences in green we have $LC = 5$ and $T = 8$.

For the class of generalized sequences associated to a characteristic polynomial $p(x)$, it can be checked that there are $L-2$ different linear complexities LC_i among the generalized sequences of the same family (apart from the trivial ones $0, 1, 2$) satisfying:

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

with $LC_i > 2^{L-2}$ [11]. Indeed, there are $2^{L-(i+2)}$ groups (containing four sequences each of them) with linear complexity LC_i. Let us consider the primitive polynomial $p(x) = 1 + x + x^6$ of degree 6. Such a polynomial generates 64 GSS-sequences divided into 16 groups of 4 sequences each group:

- ▷ 8 groups with $LC_1 = 28$
- ▷ 4 groups with $LC_2 = 27$
- ▷ 2 groups with $LC_3 = 26$
- ▷ 1 group with $LC_4 = 25$
- ▷ The group $\left\{\mathbf{0}, \binom{n}{0}, \binom{n}{1}, \binom{n}{0}+\binom{n}{1}\right\}$

4.2 Obtaining Generalized Sequences from Different Groups

It is obvious that if we have a generalized sequence, then we can obtain the other 3 sequences in the same group XOR-ing it with the sequences $\binom{n}{0}$, $\binom{n}{1}$ and $\binom{n}{0}+\binom{n}{1}$, respectively. However, can we obtain a generalized sequence from sequences contained in other groups? Due to the additive group structure, the answer is yes.

Consider the 64 generalized sequences generated with $p(x) = 1 + x + x^6$, see Appendix B. Four different linear complexities LC_i, $i = 1, 2, 3, 4$, appear:

$$LC_1 = 28, \quad LC_2 = 27, \quad LC_3 = 26 \quad \text{and} \quad LC_4 = 25.$$

Table 5. Binomial sequences $\binom{n}{LC_i-1}$ in the previous groups

	$\binom{n}{27}$	$\binom{n}{26}$	$\binom{n}{25}$	$\binom{n}{24}$
A_1	✔	✔	✔	✔
A_2	✔			✔
A_3	✔	✔		✔
A_4	✔		✔	✔
A_5	✔		✔	
A_6	✔	✔		
A_7	✔			
A_8	✔	✔	✔	

	$\binom{n}{27}$	$\binom{n}{26}$	$\binom{n}{25}$	$\binom{n}{24}$
B_1		✔	✔	
B_2		✔		
B_3		✔		✔
B_4		✔	✔	✔
C_1			✔	
C_2			✔	✔
D_1				✔

These sequences can be divided into 16 groups of 4 sequences each of them distributed as follows:

$$A_j = \{\text{Subgroup of sequences with } LC = 28\}, \text{ for } j = 1, 2, \ldots, 8$$
$$B_j = \{\text{Subgroup of sequences with } LC = 27\}, \text{ for } j = 1, 2, \ldots, 4$$
$$C_j = \{\text{Subgroup of sequences with } LC = 26\}, \text{ for } j = 1, 2$$
$$D_j = \{\text{Subgroup of sequences with } LC = 25\}, \text{ for } j = 1$$

plus the four trivial sequences.

Each term $\binom{n}{LC_i-1}$, $i = 1, 2, 3, 4$, appears in the binomial characterization of 8 subgroups, see Table 5. It is possible to check that for every value of LC_i, $i = 1, 2, 3, 4$, there exists a group, whose binomial characterization contains exclusively one of the terms $\binom{n}{LC_i-1}$. In our case, these groups are A_7, B_2, C_1 and D_1. Therefore, if we have four sequences, each of them in one of the previous groups, then we can generate the other 64 generalized sequences.

In general, for a primitive polynomial of degree L, we have 2^L sequences divided into 2^{L-2} groups and $L-2$ 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 binomial characterizations of the generalized sequences. As we observed before, there are $L-2$ groups that contain exclusively one element $\binom{n}{LC_i-1}$, $i = 1, 2, \ldots, L-2$. This means that we only need $L-2$ sequences of the family to generate the other 2^L generalized sequences.

5 Conclusions

The binary sequences considered in this work, the so-called generalized sequences, exhibit good cryptographic properties such as long periods and large linear complexities. This makes this sequences suitable for stream cipher applications. On the other hand, the binomial sequences are basic structures able to construct all the binary sequences whose periods are powers of 2; consequently, they are able to construct all the generalized sequences. In addition, the cryptographic parameters of these sequences can be determined via the binomial sequences.

At the same time, the family of generalized sequences can be analyzed and partitioned in terms of its binomial characterization. Moreover, the binomial sequences allow one to generate the whole generalized family from a minimum number of its elements.

Acknowledgements. Research partially supported by Ministerio de Economía, Industria y Competitividad, Agencia Estatal de Investigación, and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project COPCIS (TIN2017-84844-C2-1-R) and by Comunidad de Madrid (Spain) under project CYNAMON (P2018/TCS-4566), also co-funded by European Union FEDER funds. The first author was supported by CAPES (Brazil).

Appendix A

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	$\binom{n}{0}$
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	$\binom{n}{1}$
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	$\binom{n}{2}$
0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	$\binom{n}{3}$
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	$\binom{n}{4}$
0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	$\binom{n}{5}$
0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	$\binom{n}{6}$
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	$\binom{n}{7}$
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	$\binom{n}{8}$
0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	$\binom{n}{9}$
0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	$\binom{n}{10}$
0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	$\binom{n}{11}$
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	$\binom{n}{12}$
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	$\binom{n}{13}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	$\binom{n}{14}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	$\binom{n}{15}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	$\binom{n}{16}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	$\binom{n}{17}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	$\binom{n}{18}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	$\binom{n}{19}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	$\binom{n}{20}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	$\binom{n}{21}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	$\binom{n}{22}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	$\binom{n}{23}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	$\binom{n}{24}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	$\binom{n}{25}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	$\binom{n}{26}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	$\binom{n}{27}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	$\binom{n}{28}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	$\binom{n}{29}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	$\binom{n}{30}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	$\binom{n}{31}$

Appendix B

GSS-sequences for $p(x) = 1 + x + x^6$

$O = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\}$

$A_1 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{5} + \binom{n}{6} + \binom{n}{8} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{15} + \binom{n}{18} + \binom{n}{20} + \binom{n}{24} + \binom{n}{25} + \binom{n}{26} + \binom{n}{27}$

$A_2 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{4} + \binom{n}{5} + \binom{n}{6} + \binom{n}{9} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{15} + \binom{n}{17} + \binom{n}{19} + \binom{n}{22} + \binom{n}{24} + \binom{n}{27}$

$B_1 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{4} + \binom{n}{8} + \binom{n}{9} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{20} + \binom{n}{22} + \binom{n}{25} + \binom{n}{26}$

$A_3 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{3} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{14} + \binom{n}{15} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{24} + \binom{n}{26} + \binom{n}{27}$

$C_1 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{3} + \binom{n}{7} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{14} + \binom{n}{16} + \binom{n}{17} + \binom{n}{20} + \binom{n}{25}$

$B_2 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{3} + \binom{n}{4} + \binom{n}{7} + \binom{n}{8} + \binom{n}{10} + \binom{n}{11} + \binom{n}{12} + \binom{n}{13} + \binom{n}{14} + \binom{n}{16} + \binom{n}{18} + \binom{n}{19} + \binom{n}{22} + \binom{n}{26}$

$A_4 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \binom{n}{6} + \binom{n}{7} + \binom{n}{10} + \binom{n}{14} + \binom{n}{15} + \binom{n}{16} + \binom{n}{19} + \binom{n}{20} + \binom{n}{22} + \binom{n}{24} + \binom{n}{25} + \binom{n}{27}$

$A_5 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \binom{n}{7} + \binom{n}{8} + \binom{n}{12} + \binom{n}{14} + \binom{n}{15} + \binom{n}{19} + \binom{n}{20} + \binom{n}{25} + \binom{n}{27}$

$B_3 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{6} + \binom{n}{7} + \binom{n}{11} + \binom{n}{13} + \binom{n}{14} + \binom{n}{18} + \binom{n}{19} + \binom{n}{24} + \binom{n}{26}$

$C_2 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{6} + \binom{n}{7} + \binom{n}{8} + \binom{n}{9} + \binom{n}{11} + \binom{n}{13} + \binom{n}{14} + \binom{n}{17} + \binom{n}{20} + \binom{n}{22} + \binom{n}{24} + \binom{n}{25}$

$A_6 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{7} + \binom{n}{9} + \binom{n}{12} + \binom{n}{14} + \binom{n}{15} + \binom{n}{17} + \binom{n}{18} + \binom{n}{22} + \binom{n}{26} + \binom{n}{27}$

$B_4 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \binom{n}{9} + \binom{n}{10} + \binom{n}{12} + \binom{n}{16} + \binom{n}{17} + \binom{n}{18} + \binom{n}{19} + \binom{n}{20} + \binom{n}{24} + \binom{n}{25} + \binom{n}{26}$

$A_7 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{4} + \binom{n}{5} + \binom{n}{8} + \binom{n}{9} + \binom{n}{10} + \binom{n}{11} + \binom{n}{13} + \binom{n}{15} + \binom{n}{16} + \binom{n}{17} + \binom{n}{19} + \binom{n}{27}$

$A_8 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{5} + \binom{n}{10} + \binom{n}{11} + \binom{n}{13} + \binom{n}{15} + \binom{n}{16} + \binom{n}{18} + \binom{n}{20} + \binom{n}{22} + \binom{n}{25} + \binom{n}{26} + \binom{n}{27}$

$D_1 = \{\binom{n}{0}, \binom{n}{1}, \binom{n}{0} + \binom{n}{1}\} + \binom{n}{2} + \binom{n}{6} + \binom{n}{8} + \binom{n}{10} + \binom{n}{12} + \binom{n}{16} + \binom{n}{22} + \binom{n}{24}$

References

1. Cardell, S.D., Fúster-Sabater, A.: Linear models for the self-shrinking generator based on CA. J. Cell. Automata **11**(2–3), 195–211 (2016)
2. Cardell, S.D., Fúster-Sabater, A.: Recovering the MSS-sequence via CA. Procedia Comput. Sci. **80**, 599–606 (2016)
3. Cardell, S.D., Fúster-Sabater, A.: Modelling the shrinking generator in terms of linear CA. Adv. Math. Commun. **10**(4), 797–809 (2016)
4. Cardell, S.D., Fúster-Sabater, A.: The t-modified self-shrinking generator? In: Shi, Y., et al. (eds.) ICCS 2018. LNCS, vol. 10860, pp. 653–663. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93698-7_50
5. Coppersmith, D., Krawczyk, H., Mansour, Y.: The shrinking generator. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 22–39. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_3
6. Fluhrer, S., Lucks, S.: Analysis of the E_0 encryption system. In: Vaudenay, S., Youssef, A.M. (eds.) SAC 2001. LNCS, vol. 2259, pp. 38–48. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45537-X_3
7. Fúster-Sabater, A., García-Mochales, P.: A simple computational model for acceptance/rejection of binary sequence generators. Appl. Math. Model. **31**(8), 1548–1558 (2007)
8. Fúster-Sabater, A., Caballero-Gil, P.: Chaotic modelling of the generalized self-shrinking generator. Appl. Soft Comput. **11**(2), 1876–1880 (2011)
9. Fúster-Sabater, A.: Generation of cryptographic sequences by means of difference equations. Appl. Math. Inf. Sci. **8**(2), 1–10 (2014)
10. Golomb, S.W.: Shift Register-Sequences. Aegean Park Press, Laguna Hill (1982)
11. Hu, Y., Xiao, G.: Generalized self-shrinking generator. IEEE Trans. Inf. Theor. **50**(4), 714–719 (2004)
12. Jenkins, C., Schulte, M., Glossner, J.: Instructions and hardware designs for accelerating SNOW 3G on a software-defined radio platform. Analog Integr. Circ. Sig. Process. **69**(2–3), 207–218 (2011)
13. Kanso, A.: Modified self-shrinking generator. Comput. Electr. Eng. **36**(1), 993–1001 (2010)
14. Meier, W., Staffelbach, O.: The self-shrinking generator. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 205–214. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053436
15. Menezes, A.J., et al.: Handbook of Applied Cryptography. CRC Press, New York (1997)
16. Paar, C., Pelzl, J.: Understanding Cryptography. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-04101-3
17. Paul, G., Maitra, S.: RC4 Stream Cipher and its Variants. CRC Press, Taylor and Francis Group, Boca Raton (2012)