Chapter 2
Keystream Generators Based on Irregular Decimation

In this chapter, we study the definition and the principal characteristics of the main keystream generators based on irregular decimation: the shrinking generator, the self-shrinking generator, the modified self-shrinking generator and the generalized self-shrinking generator.

First of all, we need to recall the concept of decimation. Let $\{v_i\}$, $i = 0, 1, 2, \ldots$, be a linear recursive sequence over a finite field. The decimation of this sequence by distance d is a new sequence $\{v_{d \cdot i}\}$, $i = 0, 1, 2, \ldots$, obtained by taking every dth term of $\{v_i\}$ (see [22]).

Example 2.1 Consider the LFSR of length 3 with characteristic polynomial $p(x) = 1 + x + x^3$. If we consider the initial state $\{1\ 0\ 0\}$, the PN-sequence generated is the following:

$$\{a_i\} = \{1\ 0\ 0\ 1\ 0\ 1\ 1\ \ldots\}.$$

Since $p(x)$ is primitive, $\{a_i\}$ has maximum-period equal to 7. Now, if we denote by $\{b_i\}$ the sequence obtained decimating $\{a_i\}$ by distance 2:

$$\begin{array}{ccccccc} b_0 & b_4 & b_2 & b_5 & b_3 & b_6 & \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \ldots \end{array}$$

this sequence has the form $\{b_i\} = \{a_{2i}\} = \{1\ 0\ 0\ 1\ 0\ 1\ 1\ \ldots\}$. Notice that $\{b_i\}$ is the same PN-sequence $\{a_i\}$. This is due to the fact that the period of the PN-sequence and the distance of decimation are relatively primes, that is, $\gcd(7, 2) = 1$ [41]. ■

S. Díaz Cardell, A. Fúster-Sabater, *Cryptography with Shrinking Generators*,
SpringerBriefs in Mathematics, https://doi.org/10.1007/978-3-030-12850-0_2

2.1 Shrinking Generator

In this section we present the main characteristics of the first generator based on irregular decimation, the shrinking generator.

2.1.1 *Definition and Basic Features*

The **shrinking generator** (SG) was introduced by Coppersmith, Krawczyk and Mansour in [15]. This generator was very attractive in that moment, due to its conceptual simplicity, since it combines two binary maximum-length LFSRs in a simple way. The output sequence of the generator is produced by shrinking the output sequence of one LFSR under the control of the other. In other words, the PN-sequence $\{a_i\}$, $i = 0, 1, 2, \dots,$ produced by one of the registers, denoted by R_1, decimates the PN-sequence $\{b_i\}$, $i = 0, 1, 2, \dots$, produced by the other register, denoted by R_2. Let L_1 and L_2, with $\gcd(L_1, L_2) = 1$, be the number of stages (or length) of R_1 and R_2 and $p_1(x), p_2(x) \in \mathbb{F}_2[x]$ their characteristic polynomials, respectively. We consider these polynomials to be primitive, to assure the output sequences are maximum-period or PN-sequences. We will denote by $\{s_j\}$, $j = 0, 1, 2, \dots$, the output sequence of the generator and we will call it the **shrunken sequence**. The decimation rule is very simple:

$$\begin{cases} \text{If } a_i = 1, \text{ then } s_j = b_i. \\ \text{If } a_i = 0, \text{ then } b_i \text{ is discarded,} \end{cases}$$

that is, the output bit of R_2 is taken if the current bit of R_1 is 1, otherwise it is discarded.

The key of the generator is the initial states of both registers and the characteristic polynomials, which are recommended to be part of the key.

When $\gcd(L_1, L_2) = 1$, the period of the shrunken sequence is

$$T = 2^{L_1-1}\left(2^{L_2} - 1\right),$$

and its linear complexity, denoted by LC, satisfies $L_2 2^{L_1-2} < LC \leq L_2 2^{L_1-1}$. Furthermore, the shrunken sequence is balanced and has other good cryptographic properties [15]. Therefore, this scheme is supposed to be suitable for practical implementation in encryption procedures.

Let us see an illustrative example of this generator.

Example 2.2 Consider R_1 the LFSR with characteristic polynomial $p_1(x) = 1 + x + x^2$ and initial state $\{1\ 0\}$. The PN-sequence generated by R_1, in this case, is $\{a_i\} = \{1\ 0\ 1\ \dots\}$. Consider also R_2 the LFSR with characteristic polynomial $p_2(x) = 1 + x + x^3$ and initial state $\{1\ 0\ 0\}$. The PN-sequence produced is $\{b_i\} =$

{1 0 0 1 0 1 1 . . .}. Then, the shrunken sequence can be computed in the following way:

$$\begin{aligned}
\{a_i\} &: 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ \ldots \\
\{b_i\} &: 1\ \cancel{0}\ 0\ 1\ \cancel{0}\ 1\ 1\ \cancel{1}\ 0\ 0\ \cancel{1}\ 0\ 1\ \cancel{1}\ 1\ 0\ \cancel{0}\ 1\ 0\ \cancel{1}\ 1\ \ldots \\
\{s_j\} &: \mathbf{1\quad 0\,1\quad 1\,1\quad 0\,0\quad 0\,1\quad 1\,0\quad 1\,0\quad 1}\ \ldots
\end{aligned}$$

The shrunken sequence $\{s_j\}$ has period 14 and, thanks to the Berlekamp–Massey algorithm [63], it is not difficult to check that its characteristic polynomial is $p(x)^2 = \left(1 + x^2 + x^3\right)^2$, consequently its linear complexity equals 6. ■

Despite its simplicity, there are currently no known attacks better than exhaustive search of the initial states of the registers, when the characteristic polynomials are secret.

It is worth noticing that there may be multiple initial states that produce the same keystream sequence (equivalent keys). For example, let us consider the registers used in Example 2.2. If we consider initial states {0 1} and {0 1 1}, respectively, we obtain the following shrunken sequence:

$$\begin{aligned}
\{a_i\} &: 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ \ldots \\
\{b_i\} &: \cancel{0}\ 1\ 1\ \cancel{1}\ 0\ 0\ \cancel{1}\ 0\ 1\ \cancel{1}\ 1\ 0\ \cancel{0}\ 1\ 0\ \cancel{1}\ 1\ 1\ \cancel{0}\ 0\ 1\ \ldots \\
\{s_j\} &: \quad \mathbf{1\,1\quad 0\,0\quad 0\,1\quad 1\,0\quad 1\,0\quad 1\,1\quad 0\,1}\ \ldots
\end{aligned}$$

On the other hand, if we consider initial states {1 1} and {1 1 1}, respectively, we obtain the following shrunken sequence:

$$\begin{aligned}
\{a_i\} &: 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ \ldots \\
\{b_i\} &: 1\ 1\ \cancel{1}\ 0\ 0\ \cancel{1}\ 0\ 1\ \cancel{1}\ 1\ 0\ \cancel{0}\ 1\ 0\ \cancel{1}\ 1\ 1\ \cancel{0}\ 0\ 1\ \cancel{0}\ \ldots \\
\{s_j\} &: \mathbf{1\,1\quad 0\,0\quad 0\,1\quad 1\,0\quad 1\,0\quad 1\,1\quad 0\,1}\quad \ldots
\end{aligned}$$

which is the same as before. Due to leading 0s in the first two PN-sequences, both keys generate the same shrunken sequence. For this reason, we always consider initial states that start with 1. Thus, the effective key size is smaller than the key space.

From now on, we consider two registers R_1 and R_2, with primitive characteristic polynomials $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, lengths L_1 and L_2 and $\gcd(L_1, L_2) = 1$, respectively. Besides, the PN-sequences generated by both registers are denoted by $\{a_i\}$ and $\{b_i\}$ and have periods $T_1 = 2^{L_1} - 1$ and $T_2 = 2^{L_2} - 1$, respectively. We assume without loss of generality that $a_0 = 1$.

2.1.2 Characteristic Polynomial and Interleaved PN-Sequences

In this section, we will see that the shrunken sequence is constructed interleaving one unique PN-sequence and the form of its characteristic polynomial.

Theorem 2.1 ([9]) *The 2^{L_1-1} sequences obtained decimating the shrunken sequence by distance 2^{L_1-1} starting in positions $0, 1, 2, \dots, 2^{L_1-1}-1$, respectively, are PN-sequences with characteristic polynomial*

$$p(x) = \left(x+\alpha^{T_1}\right)\left(x+\alpha^{2T_1}\right)\left(x+\alpha^{4T_1}\right)\cdots\left(x+\alpha^{2^{L_2-1}T_1}\right),$$

where $\alpha \in \mathbb{F}_2^{L_2}$ is a root of the polynomial $p_2(x)$ and $T_1 = 2^{L_1}-1$ is the period of the PN-sequence generated by R_1.

All the interleaved PN-sequences of the shrunken sequence are generated by the same characteristic polynomial, this means that all of them are shifted versions of the same PN-sequence.

It is worth remarking that, since α is a primitive element of the field $\mathbb{F}_2^{L_2}$, $p_2(x)$ needs to be primitive.

Example 2.3 Consider two registers, R_1 and R_2, with characteristic polynomials $p_1(x) = 1+x+x^3$ and $p_2(x) = 1+x+x^4$ and initial states $\{1\ 0\ 0\}$ and $\{1\ 0\ 0\ 0\}$, respectively. Denote by $\{a_i\}$ and $\{b_i\}$ the PN-sequences generated by R_1 and R_2, respectively. The shrunken sequence generated by these registers has period $T = 60$ and is given by

$$\{s_j\} = \{100011111010000110010110110011010100001011100011011101011011\dots\}.$$

If we decimate the shrunken sequence $\{s_j\}$ by distance $2^{L_1-1} = 4$ starting in positions 0, 1, 2 and 3, respectively, we obtain four interleaved PN-sequences:

$$\begin{array}{rcccccccccccccccc}
\{s_{4j}\}: & 1 & 1 & 1 & \langle 0 \rangle & 1 & \boxed{0} & 1 & 1 & 0 & \textcircled{0} & 1 & 0 & 0 & 0 & 1 & \dots \\
\{s_{4j+1}\}: & \textcircled{0} & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & \dots \\
\{s_{4j+2}\}: & \boxed{0} & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & \dots \\
\{s_{4j+3}\}: & \langle 0 \rangle & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \dots
\end{array} \tag{2.1}$$

According to Theorem 2.1, the characteristic polynomial of the interleaved PN-sequences is given by

$$p(x) = \left(x+\alpha^{7}\right)\left(x+\alpha^{14}\right)\left(x+\alpha^{28}\right)\left(x+\alpha^{56}\right) = 1+x^3+x^4,$$

where $\alpha \in \mathbb{F}_{2^4}$ is a root of $p_2(x)$. Therefore, the four interleaved PN-sequences are shifted versions of the same PN-sequence generated by $p(x)$. In expression (2.1), we can check that the bits $\textcircled{0}$, $\boxed{0}$ and $\langle 0 \rangle$ in the PN-sequence $\{s_{4j}\}$ represent the starting points of the sequences $\{s_{4j+i}\}$ $(1 \le i \le 3)$, respectively. ■

Corollary 2.1 ([9, Corollary 1]) *If $L_2 = L_1 + 1$, then the polynomial $p(x)$, given in Theorem 2.1, is the reciprocal polynomial of $p_2(x)$.*

It is worth reminding that the reciprocal polynomial of the polynomial $r(x) = r_0+r_1x+\cdots+r_{l-1}x^{l-1}+r_lx^l$ is of the form $r^*(x) = r_l+r_{l-1}x+\cdots+r_1x^{l-1}+r_0x^l$.

Now, we introduce the form of the characteristic polynomial of the shrunken sequence.

Theorem 2.2 ([28]) *The characteristic polynomial of the shrunken sequence has the form $p(x)^m$, for $2^{L_1-2} < m \leq 2^{L_1-1}$ with $p(x)$ as in Theorem 2.1.*

Notice that $p(x)^{2^{L_1-1}}$ always generates the shrunken sequence, but sometimes this polynomial might not be the characteristic polynomial of lowest degree. For instance, consider again the shrunken sequence generated in Example 2.3. In this case, we computed the polynomial $p(x) = 1+x^3+x^4$. Now, we know that $p(x)^4 = \left(1+x^3+x^4\right)^4$ generates the shrunken sequence and, since $p(x)^3$ does not generate it, we can assume that $p(x)^4$ is its characteristic polynomial.

Example 2.4 Consider the registers with characteristic polynomials $p_1(x) = 1 + x^2 + x^5$ and $p_2(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^7$, respectively. Consider the shrunken sequence generated by these two registers, which has period $T = 2^4(2^7 - 1) = 2032$. According to Theorem 2.1, the polynomial $p(x)$ can be computed as:

$$\begin{aligned} p(x) = &\left(x+\alpha^{31}\right)\left(x+\alpha^{62}\right)\left(x+\alpha^{124}\right)\left(x+\alpha^{248}\right)\left(x+\alpha^{496}\right) \\ &\left(x+\alpha^{992}\right)\left(x+\alpha^{1984}\right) \\ = &\ 1 + x + x^3 + x^6 + x^7, \end{aligned}$$

where $\alpha \in \mathbb{F}_{2^7}$ is a root of $p_2(x)$. In this case, we know that $p(x)^{16}$ generates the shrunken sequence. However, it is easy to check that $p(x)^{15}$ is the characteristic polynomial. ■

Interestingly, $p(x)$ only depends on $p_2(x)$ and L_1. This means that if we fix a primitive polynomial $p_2(x)$ and we consider any primitive polynomial with degree L_1 we always obtain the same $p(x)$.

2.1.3 Shrunken Sequences and Difference Equations

In this section, we show that the shrunken sequence is a solution of a difference equation.

The characteristic polynomial $p(x)$ (with degree L) of an arbitrary sequence $\{a_i\}$ specifies its linear recurrence relationship. This means that the element a_i can be written as a linear combination of the previous elements:

$$a_i \oplus \sum_{j=1}^{L} c_j a_{i-j} = 0, \quad i \geq L.$$

The linear recursion can be expressed as a linear difference equation:

$$\left[E^L \oplus \sum_{j=1}^{L} c_j E^{L-j} \right] a_i = 0, \quad i \geq 0, \tag{2.2}$$

with E being the one-sided shift operator that acts on the sequence terms:

$$\begin{aligned} Ea_i &= a_{i+1}, \\ E^k a_i &= a_{i+k}. \end{aligned} \tag{2.3}$$

If the characteristic polynomial $p(x)$ is primitive and α is one of its roots, then α,α^2,α^{2^2}, ... , $\alpha^{2^{L-1}}$ are the L different roots of such a polynomial as well as primitive elements of $\mathbb{F}_{2^L}$ [59]. Now, if the characteristic polynomial of an arbitrary sequence $\{s_j\}$ is of the form $p(x)^m$, then its roots will be the same as those of $p(x)$ but each one with multiplicity m. The corresponding difference equation is given by

$$\left[E^L \oplus \sum_{k=1}^{L} E^{L-k} \right]^m s_j = 0,$$

and its solutions are of the form $s_j = \sum_{i=0}^{L-1} \sum_{k=0}^{m-1} \binom{j}{k} A_k^{2^i} \alpha^{2^i j}$, where A_k is an arbitrary element in $\mathbb{F}_{2^L}$. Different choices of A_k give rise to different sequences $\{s_j\}$. A particular choice of A_k provides the shrunken sequence generated by $p(x)^m$.

2.1.4 *Obtaining the Second PN-Sequence from the Shrunken Sequence*

Given the shrunken sequence $\{s_j\}$ generated by two registers, R_1 and R_2, it is possible to compute the PN-sequences generated by both registers. In this section, we explain how to obtain the PN-sequence $\{b_i\}$ produced by R_2.

Proposition 2.1 ([11, Proposition 1]) *Let $\delta \in \{1, 2, 3, \dots, T_2 - 1\}$ be such that $T_1 \delta = 1 \ \ mod \ \ T_2$. If the first PN-interleaved sequence is decimated by distance δ, then the resultant sequence is $\{b_i\}$.*

Example 2.5 Consider again the shrunken sequence obtained in Example 2.3 and consider the interleaved PN-sequences given in expression (2.1). Since $L_1 = 3$ and $L_2 = 4$, the unique value for δ such that $7\delta = 1$ mod 15 is $\delta = 13$. This means that if we decimate the first interleaved sequence $\{s_{4j}\}$ by distance 13, according to

Proposition 2.1, we obtain $\{b_i\}$, the PN-sequence generated by $p_2(x) = 1 + x + x^4$:

$$\begin{array}{r ccccccccccccccc}
 & b_0 & b_7 & b_{14} & b_6 & b_{13} & b_5 & b_{12} & b_4 & b_{11} & b_3 & b_{10} & b_2 & b_9 & b_1 & b_8 \\
 & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\{s_{4j}\}: & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\{s_{4j+1}\}: & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
\{s_{4j+2}\}: & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
\{s_{4j+3}\}: & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}$$

In this case $\{b_i\} = \{1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1 \ldots\}$. ■

The previous proposition leads us to the following two results.

Corollary 2.2 ([11, Corollary 2]) *If the polynomials $p_1(x)$, $p_2(x) \in \mathbb{F}_2[x]$ have degrees L_1 and $L_1 + 1$, respectively, then $\delta = T_2 - 2$.*

In Example 2.5, we had that $L_2 = L_1 + 1 = 4$, then it was not necessary to solve the equation given in Proposition 2.1, it was enough to compute $\delta = T_2 - 2 = 13$.

Theorem 2.3 ([11, Corollary 1]) *If the shrunken sequence is decimated by distance $2^{L_1-1}\delta$, then the obtained sequence is the PN-sequence $\{b_i\}$.*

Example 2.6 Consider again the shrunken sequence obtained in Example 2.2. In this example we had that $L_1 = 2$ and $L_2 = 3$, then according to Corollary 2.2, $\delta = 5$. Now, according to Theorem 2.3, we know that if we decimate the shrunken sequence by distance 10:

$$\begin{array}{cccccccccccccc l}
b_0 & & b_3 & & b_6 & & b_2 & & b_5 & & b_1 & & b_4 & & \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \ldots
\end{array}$$

then we obtain again the PN-sequence generated by the second register, R_2:

$$\{b_i\} = \{1\ 0\ 0\ 1\ 0\ 1\ 1\ \ldots\}.$$

■

2.1.5 Obtaining the First PN-Sequence from the Shrunken Sequence

In this section, we analyse how to recover the PN-sequence $\{a_i\}$ produced by R_1 from the shrunken sequence $\{s_j\}$.

Assume the first interleaved PN-sequence of $\{s_j\}$ is denoted by $\{v_i\}$. Since the other interleaved sequences are shifted versions of the same PN-sequence, it means they are shifted versions of $\{v_i\}$. Then, we assume they have the form $\left\{v_{d_1+i}\right\}, \left\{v_{d_2+i}\right\}, \ldots, \left\{v_{d_{2^{L_1-1}-1}+i}\right\}$, for some positions $d_i \in \left\{0, 1, 2, \ldots, 2^{L_2-2}\right\}$:

$$\begin{array}{rllllll}
\{v_i\}: & \{v_0 & v_1 & v_2 & \cdots & v_{T_2-1} & \cdots\} \\
\left\{v_{d_1+i}\right\}: & \{v_{d_1} & v_{d_1+1} & v_{d_1+2} & \cdots & v_{d_1+T_2-1} & \cdots\} \\
\left\{v_{d_2+i}\right\}: & \{v_{d_2} & v_{d_2+1} & v_{d_2+2} & \cdots & v_{d_2+T_2-1} & \cdots\} \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \\
\left\{v_{d_{2^{L_1-1}-1}+i}\right\}: & \{v_{d_{2^{L_1-1}-1}} & v_{d_{2^{L_1-1}-1}+1} & v_{d_{2^{L_1-1}-1}+2} & \cdots & v_{d_{2^{L_1-1}-1}+T_2-1} & \cdots\}.
\end{array}$$

In order to illustrate this idea, consider again Example 2.3. We had four interleaved PN-sequences that correspond to:

$$\{s_{4j}\} = \{v_i\}, \quad \{s_{4j+1}\} = \{v_{d_1+i}\}, \quad \{s_{4j+2}\} = \{v_{d_2+i}\} \quad \text{and} \quad \{s_{4j+3}\} = \{v_{d_3+i}\}.$$

In this case, the positions are $d_1 = 9$, $d_2 = 5$ and $d_3 = 3$:

$$\begin{array}{rccccccccccccccc}
 & & & & d_3{=}3 & & d_2{=}5 & & & & d_1{=}9 & & & & & \\
 & & & & \uparrow & & \uparrow & & & & \uparrow & & & & & \\
\{s_{4j}\}: & 1 & 1 & 1 & \langle 0 \rangle & 1 & \boxed{0} & 1 & 1 & 0 & \textcircled{0} & 1 & 0 & 0 & 0 & 1 \\
\{s_{4j+1}\}: & \textcircled{0} & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
\{s_{4j+2}\}: & \boxed{0} & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
\{s_{4j+3}\}: & \langle 0 \rangle & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array} \tag{2.4}$$

Before introducing the next result, it is worth reminding that a maximum-length LFSR of L stages produces a PN-sequence with 2^{L-1} ones in its first period [41].

Example 2.7 Consider the LFSR with characteristic polynomial $p(x) = 1 + x + x^4$ and initial state $\{1\ 1\ 1\ 1\}$. The PN-sequence generated by this register is given by

$$\{1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\ \ldots\}.$$

Notice that this PN-sequence has 2^3 ones in its period, that is, in its first 15 bits. ■

Theorem 2.4 ([11, Proposition 2]) *If* $\{0, i_1, i_2, \ldots, i_{2^{L_1-1}-1}\}$ *is the set of indices of the* 1*s in the PN-sequence* $\{a_i\}$ *in its first period, then* $d_k = \delta \cdot i_k$ *mod* $\left(2^{L_1-1} - 1\right)$, *for* $k = 1, 2, \ldots, 2^{L_1-1} - 1$, *where* δ *has the form given in Proposition 2.1.*

In Example 2.3, we had four interleaved PN-sequences $\{v_i\}$, $\{v_{i+d_1}\}$, $\{v_{i+d_2}\}$ and $\{v_{i+d_3}\}$ and $\delta = 13$. We know that $d_1 = 9$, $d_2 = 5$ and $d_3 = 3$ (see expression (2.4)). Then, according to Theorem 2.4, we can compute the indices $\{0, i_1, i_2, i_3\}$ of the four 1s in the first period of $\{a_i\}$ ($i_0 = 0$, without loss of generality) solving the following system:

$$\begin{cases} 13 \cdot i_1 = 9 \bmod 15 \\ 13 \cdot i_2 = 5 \bmod 15 \\ 13 \cdot i_3 = 3 \bmod 15. \end{cases}$$

Therefore, the set of indices is given by $\{0, 3, 5, 6\}$ and then the PN-sequence produced by R_1 is given by $\{a_i\} = \{1\ 0\ 0\ 1\ 0\ 1\ 1 \ldots\}$.

2.2 Self-Shrinking Generator

The **self-shrinking generator** (SSG) was introduced by Meier and Staffelbach in [67]. They presented a simple structure using only one maximal-length LFSR, whose output sequence $\{a_i\}$ is self-decimated. The key consists of the initial state of the register and the characteristic polynomial is again recommended as part of the key.

Let L be the length and $p(x) \in \mathbb{F}_2[x]$ the characteristic polynomial of the register. We consider again $p(x)$ primitive, to assure the output sequence has maximum-period. We will denote by $\{s_j\}$, $j = 0, 1, 2, \ldots$, the output sequence of the generator and we will call it, the **self-shrunken sequence** (SS-sequence). The decimation rule is very simple,

$$\begin{cases} \text{If } a_{2i} = 1, \text{ then } s_j = a_{2i+1}. \\ \text{If } a_{2i} = 0, \text{ then } a_{2i+1} \text{ is discarded,} \end{cases}$$

that is, pairs of bits are considered: if a pair happens to take the value 10 or 11, this pair is taken to produce the bit 0 or 1, depending on the second bit of the pair. On the other hand, if a pair happens to be 01 or 00, it will be discarded.

Example 2.8 Consider the LFSR of $L = 3$ stages with characteristic polynomial $p_1(x) = 1 + x^2 + x^3$ and initial state $\{1\ 0\ 0\}$. The corresponding PN-sequence is given by $\{1\ 0\ 0\ 1\ 1\ 1\ 0\ \ldots\}$. Now the self-shrunken sequence can be computed in the following way:

$$R : \underbrace{1\ \ \mathbf{0}}_{\mathbf{0}}\ \ 0\ \ 1\ \ \underbrace{1\ \ \mathbf{1}}_{\mathbf{1}}\ \ 0\ \ 1\ \ 0\ \ 0\ \ \underbrace{1\ \ \mathbf{1}}_{\mathbf{1}}\ \ \underbrace{1\ \ \mathbf{0}}_{\mathbf{0}}\ \ \ldots$$

The corresponding self-shrunken sequence is given by $\{s_j\} = \{0\ 1\ 1\ 0\ \ldots\}$. ■

The period T of a self-shrunken sequence [67] produced by a maximal-length LFSR of L stages satisfies

$$T \geq 2^{\lfloor \frac{L}{2} \rfloor}.$$

Due to experimental observations, we claim that the period of the self-shrunken sequences is always $T = 2^{L-1}$, when $L > 3$ and $p(x)$ is primitive. However, no proof has been found yet. We encourage the reader to prove this claim.

According to Meier and Staffelbach [67] and Blackburn [5], we can say that the linear complexity satisfies

$$2^{\lfloor \frac{L}{2} \rfloor} < LC \leq 2^{L-1} - (L-2).$$

Again, due to experimental observations, we claim that the lower bound for the linear complexity can be improved to: $LC > 2^{L-2}$. However, no proof has been found so far. Actually, this is also a natural consequence of $T = 2^{L-1}$. We let the reader think about this open problem.

Proposition 2.2 ([33]) *The characteristic polynomial of the self-shrunken sequences has the following form: $p_{LC}(x) = (1+x)^{LC}$, where LC is the linear complexity of such a sequence.*

For instance, consider Example 2.8. We had the self-shrunken sequence $\{s_j\} = \{0\ 1\ 1\ 0\ \ldots\}$ produced by $p(x) = 1 + x^2 + x^3$. It is possible to check that the self-shrunken sequence has period $T = 2^{3-1}$ and its characteristic polynomial is $p_3(x) = (1+x)^3$ (see Berlekamp–Massey algorithm [63]). Consequently, the linear complexity of $\{s_j\}$ is $LC = 3$.

2.3 Modified Self-Shrinking Generator

In [53] Kanso introduced a variant of the self-shrinking generator called the **modified self-shrinking generator** (MSSG). This generator, intended for hardware implementation, uses an extended selection rule based on the XORed value of a pair of bits in the PN-sequence. The resultant sequences are balanced and have good statistical properties.

The decimation rule is very simple and can be described as follows: given three consecutive bits $\{a_{3i}, a_{3i+1}, a_{3i+2}\}$, $i = 0, 1, 2, \ldots$, of a PN-sequence $\{a_i\}$, the output sequence $\{s_j\}$ is computed as

$$\begin{cases} \text{If } a_{3i} + a_{3i+1} = 1 \text{ then } s_j = a_{3i+2}, \\ \text{If } a_{3i} + a_{3i+1} = 0 \text{ then } a_{3i+2} \text{ is discarded.} \end{cases}$$

The output sequence $\{s_j\}$ is known as the **modified self-shrunken sequence** (MSS-sequence).

Example 2.9 Let us consider the LFSR of three stages with characteristic polynomial $q(x) = 1 + x^2 + x^3$ and initial state $\{1\ 1\ 1\}$. The PN-sequence generated by this register is given by $\{1\ 1\ 1\ 0\ 1\ 0\ 0\ \ldots\}$. In this case, the modified self-shrunken sequence can be computed as follows:

$$\begin{array}{l} \{a_i\}\text{:}\ \underbrace{1\,1}_{0}\,\cancel{1}\,\underbrace{0\,1}_{1}\,\textcircled{\textbf{0}}\,\underbrace{0\,1}_{1}\,\textcircled{\textbf{1}}\,\underbrace{1\,0}_{1}\,\textcircled{\textbf{1}}\,\underbrace{0\,0}_{0}\,\cancel{1}\,\underbrace{1\,1}_{0}\,\cancel{0}\,\underbrace{1\,0}_{1}\,\textcircled{\textbf{0}}\ldots \\ \oplus\text{:} \end{array}$$

The sequence $\{s_j\} = \{0\ 1\ 1\ 0\ \ldots\}$ (encircled bits) is the MSS-sequence generated by $q(x)$. ■

Now, we are ready to study the properties of this generator. According to [53], if we consider a maximal-length LFSR of L (odd) stages, then:

1. The period T of the MSS-sequence satisfies

$$2^{\lfloor \frac{L}{3} \rfloor} \leq T \leq 2^{L-1}.$$

2. The linear complexity LC of the MSS-sequence satisfies

$$2^{\lfloor \frac{L}{3} \rfloor - 1} \leq T \leq 2^{L-1} - (L-2).$$

Although the MSS-sequences seem to have lower bounds on the period and linear complexity than those of the SSG, Kanso claimed that these sequences provide a higher level of security against several well-known attacks. Besides, Kanso demonstrated that the MSS-sequences possess better randomness properties than those of the SSG. In next section, we will see that both sequences belong to the family of generalized self-shrunken sequences.

2.4 Generalized Self-Shrinking Generator

In [46] Hu and Xiao introduced a specialization of the shrinking generator and a generalization of the self-shrinking generator. This new generator, known as **generalized self-shrinking generator** (GSSG), produces a family of sequences that has group structure. These sequences are also balanced and have quite good correlation.

2.4.1 Definition and Features

Let $\{a_i\}$, $i = 0, 1, 2, \ldots$, be a PN-sequence produced by an LFSR of L stages. Now, consider the binary vector

$$G = [g_0, g_1, \ldots, g_{L-1}] \in \mathbb{F}_2^L$$

and the sequence $\{v_i\}$, $i = 0, 1, 2, \ldots$, sometimes denoted by $v(G)$, such that

$$v_i = g_0 a_i + g_1 a_{i-1} + \cdots + g_{L-1} a_{i-L+1}.$$

Consider the following decimation rule:

$$\begin{cases} \text{If } a_i = 1, \text{ then } s_j = v_i. \\ \text{If } a_i = 0, \text{ then } v_i \text{ is discarded.} \end{cases}$$

This means that the PN-sequence $\{a_i\}$ decimates the sequence $\{v_i\}$, for each value of G.

We denote the sequence $\{s_j\}$, $j = 0, 1, 2, \ldots$, by $s(v)$ or $s(G)$ and call it **generalized self-shrunken sequence** (GSS-sequence). The family of GSS-sequences $s(a) = \{s(G) \mid G \in \mathbb{F}_2^L\}$ is the family of self-shrunken sequences based on the PN-sequence $\{a_i\}$.

It is worth noticing that the family of sequences

$$\left\{\{v_i\}_{i\geq 0}, \mid v_i = g_0 a_i + g_1 a_{i-1} + \cdots + g_{L-1} a_{i-L+1}, G \in \mathbb{F}_2^L, G \neq 0\right\}$$

includes all the $2^L - 1$ shifts sequences of $\{a_i\}$. Then, the PN-sequence $\{a_i\}$ decimates shift versions of itself.

For simplicity, we refer G as the decimal representation of the vector G.

Example 2.10 Consider the PN-sequence

$$\{a_i\} = \{1\ 1\ 1\ 0\ 0\ 1\ 0 \ldots\}$$

generated by the primitive polynomial $p(x) = 1 + x + x^3$. Since $\{a_i\}$ has period equal to 7, then we get 7 generalized self-shrunken sequences based on $\{a_i\}$ plus the identically zero sequence (see Table 2.1). ■

Table 2.1 GSS-sequences generated by $1 + x + x^3$

G			$v(G)$							$s(G)$				LC
0	0	0	$\underline{0}$	$\underline{0}$	$\underline{0}$	0	0	$\underline{0}$	0	**0**	**0**	**0**	**0**	0
0	0	1	$\underline{1}$	$\underline{0}$	$\underline{1}$	1	1	$\underline{0}$	0	**1**	**0**	**1**	**0**	2
0	1	0	$\underline{0}$	$\underline{1}$	$\underline{1}$	1	0	$\underline{0}$	1	**0**	**1**	**1**	**0**	3
0	1	1	$\underline{1}$	$\underline{1}$	$\underline{0}$	0	1	$\underline{0}$	1	**1**	**1**	**0**	**0**	3
1	0	0	$\underline{1}$	$\underline{1}$	$\underline{1}$	0	0	$\underline{1}$	0	**1**	**1**	**1**	**1**	1
1	0	1	$\underline{0}$	$\underline{1}$	$\underline{0}$	1	1	$\underline{1}$	0	**0**	**1**	**0**	**1**	2
1	1	0	$\underline{1}$	$\underline{0}$	$\underline{0}$	1	0	$\underline{1}$	1	**1**	**0**	**0**	**1**	3
1	1	1	$\underline{0}$	$\underline{0}$	$\underline{1}$	0	1	$\underline{1}$	1	**0**	**0**	**1**	**1**	3
			1	**1**	**1**	0	0	**1**	0					

The family $s(a)$ is an L-dimensional linear space on $\mathbb{F}_2$, so it is an Abelian group with neutral element $\{0\ 0\ \ldots\ 0\ 0\}$ [46]. Then, $|s(a)| = 2^L$.

The following results evidence the relation between some values of G and the generated sequences.

Theorem 2.5 ([46, Theorem 1])

1. *$s(G) = \{0\ 0\ 0\ \ldots\}$ if and only if $G = [0, 0, \ldots, 0]$.*
2. *$s(G) = \{1\ 1\ 1\ \ldots\}$ if and only if $G = [1, 0, \ldots, 0]$.*
3. *$s(G)$ is balanced otherwise.*

Theorem 2.6 ([46, Theorem 5])

1. *There are two sequences from $s(G)$ with period equal to 2, which are* $\{1\ 0\ 1\ 0 \ldots\}$ *and* $\{0\ 1\ 0\ 1\ \ldots\}$.
2. *There are two sequences from $s(G)$ with period equal to 1, which are* $\{0\ 0\ 0\ 0 \ldots\}$ *and* $\{1\ 1\ 1\ 1\ \ldots\}$.

This means that the identically 0 sequence, the identically 1 sequence and the sequences that alternate 0 and 1 belong to every family of GSS-sequences. Furthermore, the sequences different from the identically 0 sequence and the identically 1 sequence are balanced.

Theorem 2.7 ([10, Theorem 5]) *The characteristic polynomial of the GSS-sequences generated by a PN-sequence is $p_{LC}(x) = (1 + x)^{LC}$, where LC is the linear complexity of the considered GSS-sequence.*

Example 2.11 Consider the family of GSS-sequences obtained from the LFSR with characteristic polynomial $p(x) = 1 + x + x^3$ in Example 2.10. There are four different sequences (the others are shifted versions of these four) and it is possible to check, via the Berlekamp–Massey algorithm, that their corresponding characteristic polynomials are given by

$$\{0\} : 0\,0\,0\,0 \rightarrow p_0(x) = 1$$

$$\{4\} : 1\ 1\ 1\ 1 \rightarrow p_1(x) = (1 + x)$$

$$\{1, 5\} : 1\ 0\ 1\ 0 \rightarrow p_2(x) = (1 + x)^2$$

$$\{2, 3, 6, 7\} : 0\ 1\ 1\ 0 \rightarrow p_3(x) = (1 + x)^3. \qquad \blacksquare$$

The generalized self-shrinking generator has hardly been studied. For example, there are no works on the period nor the complexity of the sequences. Since any PN-sequence possesses 2^{L-1} ones in its first period [41], it seems evident that the period of the sequences $s(G)$ is a power of 2, that is, 2^t with $t \leq L-1$. Again, due to experimental observations, we can claim that the period of the sequences different from the sequences mentioned in Theorem 2.6 is always 2^{L-1}. Furthermore, the linear complexity of these sequences seems to satisfy:

$$2^{L-2} < LC \leq 2^{L-1} - (L - 2).$$

The upper bound can be obtained adapting the proof given by Blackburn for the self-shrunken sequence in [5] . None of the other bounds has been proven yet. We encourage the reader to think about it.

Given a primitive polynomial $p(x)$ of degree L, the 2^{L-1} GSS-sequences generated are divided into $L-1$ different groups depending on their LC:

- 1 sequence of $LC = 0$, the identically 0 sequence.
- 1 sequence of $LC = 1$, the identically 1 sequence.
- 2 sequences of $LC = 2$, sequences $\{0\ 1\ 0\ 1\ \ldots\}$ and $\{1\ 0\ 1\ 0\ \ldots\}$.
- 2^{i+1} sequences of linear complexity LC_i, with $2^{L-2} < LC_i \leq 2^{L-1} - (L-2)$, for $i = 1, 2, \ldots, L-2$, and $L_1 < L_2 < \cdots < L_{L-2}$.

Example 2.12 In Table 2.2, we can find the 32 GSS-sequences generated by $p(x) = 1 + x^2 + x^3 + x^4 + x^5$. There are:

- 1 sequence with $LC = 0$, the identically 0 sequence.
- 1 sequence with $LC = 1$, the identically 1 sequence.
- 2 sequences with $LC = 2$, sequences $\{0\ 1\ 0\ 1\ \ldots\}$ and $\{1\ 0\ 1\ 0\ \ldots\}$.
- 4 sequences with $LC = 10$.
- 8 sequences with $LC = 12$.
- 16 sequences with $LC = 13$.

■

2.4.2 Generalized Self-Shrunken Sequences and Difference Equations

In this section we present the GSS-sequences as solutions of linear difference equations.

According to Theorem 2.7 and other results seen in the previous section, we know that the characteristic polynomial of the GSS-sequence generated by a maximal-length LSFR is of the form:

$$p_t(x) = (1+x)^t, \quad t \leq 2^{L-1} - (L-2).$$

This implies a linear recurrence relationship of the form:

$$(E+1)^t s_j = 0, \tag{2.5}$$

with E being the one-sided shift introduced in expression (2.3). Expression (2.5) represents a linear binary constant coefficient difference equation whose characteristic polynomial $p_t(x)$ has a unique root $\lambda = 1$ with multiplicity t. The solutions of

Table 2.2 GSS-sequences generated by $p(x) = 1 + x^2 + x^3 + x^4 + x^5$

G	$s(G)$																LC
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	1	1	1	1	0	1	0	0	0	0	1	12
2	1	0	0	1	1	1	1	0	0	0	0	1	1	0	0	1	13
3	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	13
4	0	0	1	1	1	1	0	1	0	1	1	0	1	0	0	0	10
5	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	12
6	1	0	1	0	0	0	1	1	0	1	1	1	0	0	0	1	13
7	1	1	1	0	1	1	0	0	1	1	0	1	0	0	0	0	13
8	0	1	1	1	1	0	1	1	0	0	0	1	0	0	1	0	13
9	0	0	1	1	0	1	0	0	1	0	1	1	0	0	1	1	13
10	1	1	1	0	0	1	0	1	0	0	0	0	1	0	1	1	12
11	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	2
12	0	1	0	0	0	1	1	0	0	1	1	1	1	0	1	0	13
13	0	0	0	0	1	0	0	1	1	1	0	1	1	0	1	1	13
14	1	1	0	1	1	0	0	0	0	1	1	0	0	0	1	1	12
15	1	0	0	1	0	1	1	1	1	1	0	0	0	0	1	0	10
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	0	1	1	0	0	0	0	0	1	0	1	1	1	1	0	12
18	0	1	1	0	0	0	0	1	1	1	1	0	0	1	1	0	13
19	0	0	1	0	1	1	1	0	0	1	0	0	0	1	1	1	13
20	1	1	0	0	0	0	1	0	1	0	0	1	0	1	1	1	10
21	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	0	12
22	0	1	0	1	1	1	0	0	1	0	0	0	1	1	1	0	13
23	0	0	0	1	0	0	1	1	0	0	1	0	1	1	1	1	13
24	1	0	0	0	0	1	0	0	1	1	1	0	1	1	0	1	13
25	1	1	0	0	1	0	1	1	0	1	0	0	1	1	0	0	13
26	0	0	0	1	1	0	1	0	1	1	1	1	0	1	0	0	12
27	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	2
28	1	0	1	1	1	0	0	1	1	0	0	0	0	1	0	1	13
29	1	1	1	1	0	1	1	0	0	0	1	0	0	1	0	0	13
30	0	0	1	0	0	1	1	1	1	0	0	1	1	1	0	0	12
31	0	1	1	0	1	0	0	0	0	0	1	1	1	1	0	1	10

this equation are binary sequences $\{s_j\}$ whose generic term is given by

$$s_j = \binom{j}{0}c_0 + \binom{j}{1}c_1 + \cdots + \binom{j}{t-1}c_{t-1},$$

with $c_j \in \mathbb{F}_2$ and $\binom{j}{i}$ as binomial coefficients modulo 2, for $i = 0, 1, \ldots, t-1$ [59]. In fact, each binomial coefficient defines a succession of binary values with constant period T_j. Table 2.3 depicts the first binomial coefficients with their corresponding

Table 2.3 Binomial coefficients reduced modulo 2, binary sequences and periods

Bino. coeff.	Binary sequences	T_j
$\binom{j}{0}$	11111111	$T_0 = 1$
$\binom{j}{1}$	01010101	$T_1 = 2$
$\binom{j}{2}$	00110011	$T_2 = 4$
$\binom{j}{3}$	00010001	$T_3 = 4$
$\binom{j}{4}$	00001111	$T_4 = 8$
$\binom{j}{5}$	00000101	$T_5 = 8$
$\binom{j}{6}$	00000011	$T_6 = 8$
$\binom{j}{7}$	00000001	$T_7 = 8$

binary sequences and periods. The 2^t possible choices of c_i, $i = 0, 1, \dots, t-1$, provide the different binary sequences $\{s_j\}$ that satisfy expression (2.5). Particular choices of c_i give rise to the generalized self-shrunken sequences generated by an LFSR of L stages (including the SS-sequence and the MSS-sequence). Interestingly, all the solutions of expression (2.5) are the bit-wise sum of the basic sequences coming from the binomial coefficients (see Table 2.3) and weighted by c_i, $i = 0, 1, \dots, t-1$.

2.4.3 Relationship with the Modified Self-Shrinking Generator

In this section, we see how the MSS-sequence generated by a primitive polynomial $q(x)$ of degree L can be obtained as one of the GSS-sequences generated by another primitive polynomial of the same degree.

Theorem 2.8 ([10, Theorems 1–2]) *The MSS-sequence obtained by self-decimating a PN-sequence with characteristic polynomial $q(x)$ of degree L, with L odd, can be computed as one of the GSS-sequences using another primitive polynomial $p(x)$ of degree L given by*

$$p(x) = \left(x + \alpha^3\right)\left(x + \alpha^6\right)\left(x + \alpha^{12}\right)\cdots\left(x + \alpha^{3\cdot 2^{L-1}}\right),$$

where $\alpha \in \mathbb{F}_{2^L}$ is a root of $q(x)$.

Notice that the self-shrunken sequence is also a generalized self-shrunken sequence [107]. When the PN-sequence $\{v_i\}$ is shifted 2^{L-1} bits regarding the PN-sequence $\{a_i\}$, then the generated sequence is the self-shrunken sequence.

Example 2.13 Given the LSFR with characteristic polynomial $q(x) = 1 + x^2 + x^5$ and the initial state {1 1 1 1}, we can obtain the following MSS-sequence:

$$\{1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ \ldots\}.$$

According to Theorem 2.8, this sequence can be also obtained using the GSSG with primitive polynomial

$$p(x) = \left(x+\alpha^3\right)\left(x+\alpha^6\right)\left(x+\alpha^{12}\right)\left(x+\alpha^{24}\right)\left(x+\alpha^{48}\right) = 1+x^2+x^3+x^4+x^5,$$

where $\alpha \in \mathbb{F}_{2^5}$ is a root of $q(x)$. In Table 2.2 we can find the 32 GSS-sequences generated by $p(x)$ using the different values of G. For $G = 5$ ($G = [1\ 0\ 1\ 0\ 0]$), the generated GSS-sequence is a shifted version of the MSS-sequence generated by $q(x)$.

The self-shrunken sequence generated by $p(x) = 1 + x^2 + x^3 + x^4 + x^5$ is also a GSS-sequence. For instance, consider the initial state $\{1\ 1\ 1\ 1\ 1\}$, we generate the following SS-sequence:

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

which is exactly the GSS-sequence corresponding to $G = 3$ ($G = [0\ 0\ 0\ 1\ 1]$) (see Table 2.2). ■

Now, in order to know which GSS-sequence is the MSS-sequence, we need to recall the definition of Zech logarithm. Zech logarithms are named after Julius Zech who published in 1849 a table of this type logarithms (which he called *addition logarithms*) for doing arithmetic in $\mathbb{Z}_p$. These logarithms are also called as Jacobi logarithms after C.G.J. Jacobi who used them for number theoretic investigations [48].

Definition 2.1 Let $\mathbb{F}_q$ be the Galois field of q elements and $\alpha \in \mathbb{F}_q$ a primitive element. The **Zech logarithm** with basis α is the application $\mathcal{Z}_\alpha : \mathbb{Z}_q \to \mathbb{Z}_q^* \cup \{\infty\}$, such that each element $t \in \mathbb{Z}_q$ corresponds to $\mathcal{Z}_\alpha(t)$, attaining $1 + \alpha^t = \alpha^{\mathcal{Z}_\alpha(t)}$.

Now we are ready to compute the value of G that produces a MSS-sequence as a GSS-sequence.

Theorem 2.9 ([10, Theorem 3]) *The MSS-sequence generated from a PN-sequence with primitive characteristic polynomial $q(x)$ is also a GSS-sequence obtained from a PN-sequence generated by a primitive polynomial $p(x)$ (see Theorem 2.8) that decimates a shifted version of itself with shift* $(D-2)3^{-1} \bmod (2^L - 1)$, *where $D = \mathcal{Z}_\alpha(1)$, $\alpha \in \mathbb{F}_{2^L}$ is a root of $p(x)$ and L is the degree of $p(x)$ and $q(x)$.*

Assume $\{a_i\}$ is a PN-sequence generated by a primitive polynomial and assume $\{b_i\} = \{a_{i+(D-2)3^{-1}}\}$ is the shifted version of $\{a_i\}$ that is decimated by $\{a_i\}$ in order to obtain the MSS-sequence (see Theorem 2.9). According to the definition of GSSG, to find the value of $G = [g_0, g_1, \ldots, g_{L-1}]$ that generates $\{b_i\}$ from $\{a_i\}$, we have to know L bits of $\{a_i\}$ and $2L-1$ bits of $\{b_i\}$ to solve the following system:

$$\begin{cases} a_0 = b_0 g_0 + b_{2^L-2} g_1 + b_{2^L-3} g_2 + \cdots + b_{2^L-L} g_{L-1} \\ a_1 = b_1 g_0 + b_0 g_1 + b_{2^L-2} g_2 + \cdots + b_{2^L-(L-1)} g_{L-1} \\ \qquad \vdots \\ a_{L-1} = b_{L-1} g_0 + b_{L-2} g_1 + b_{L-3} g_2 + \cdots + b_0 g_{L-1}. \end{cases} \tag{2.6}$$

The exact necessary bits of each sequence are $\{a_i\}_{i=0}^{L-1}$ and $\{b_i\}_{i=0}^{L-1} \cup \{b_i\}_{i=2^L-L}^{2^L-2}$, respectively.

Let us see a clarifying example.

Example 2.14 Consider the MSS-sequence generated in Example 2.13:

$$\{s_j\} = \{1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ \underline{\mathbf{0}}\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ \ldots\}. \tag{2.7}$$

According to Theorem 2.8, $\{s_j\}$ can be generated as a GSS-sequence using the primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^5$. Given the PN-sequence $\{a_i\}$ generated by $p(x)$, we consider the PN-sequence $\{b_i\} = \{a_{i+k}\}$ which is a shifted version of $\{a_i\}$, with shift $k = (\mathscr{L}_\alpha(1) - 2) \cdot 3^{-1} \bmod 31$, α root of $q(x)$. This means that $\{b_i\} = \{a_{i+26}\}$.

Taking the initial state $\{1\ 1\ 1\ 1\ 1\}$, we can generate the PN-sequence

$$\{a_i\} = \{1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ \ldots\}$$

that decimates a shifted version of itself,

$$\{b_i\} = \{\mathbf{0}\ \mathbf{1}\ \mathbf{1}\ \mathbf{1}\ \mathbf{0}\ 0\ \mathbf{0}\ \mathbf{1}\ \mathbf{0}\ 1\ 0\ 1\ \mathbf{1}\ 0\ \mathbf{1}\ 0\ \mathbf{0}\ \mathbf{0}\ 0\ \mathbf{1}\ 1\ 0\ 0\ 1\ \mathbf{0}\ \mathbf{0}\ 1\ 1\ \mathbf{1}\ 1\ 1\},$$

with shift equal to 26. Thus, we obtain the output sequence

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

which is a shifted version of the MSS-sequence $\{s_j\}$ starting at the underlined position (see expression (2.7)).

Now, in order to obtain the value of $G = [g_0, g_1, g_2, g_3, g_4]$, we have to solve the system given in (2.6). In this case we have

$$\{a_i\}_{i=0}^{4} = \{0\ 1\ 1\ 1\ 0\}, \quad \{b_i\}_{i=0}^{4} = \{1\ 1\ 1\ 1\ 1\} \quad \text{and} \quad \{b_i\}_{i=27}^{30} = \{0\ 1\ 0\ 0\}.$$

Table 2.4 GSS-sequences obtained with $G = 5$

Initial state					5th GSS-sequence															
1	1	1	1	1	0	1	1	1	0	0	1	0	$\underline{1}$	1	0	0	1	0	0	1
1	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	0	$\underline{1}$	1	0	0
1	0	1	0	1	$\underline{1}$	1	0	0	1	0	0	1	0	1	1	1	0	0	1	0

Therefore, system (2.6) has the following form:

$$\begin{cases} 0 = g_0 + g_3 \\ 1 = g_0 + g_1 + g_4 \\ 1 = g_0 + g_1 + g_2 \\ 1 = g_0 + g_1 + g_2 + g_3 \\ 0 = g_0 + g_1 + g_2 + g_3 + g_4, \end{cases}$$

whose solution is $G = [0\ 0\ 1\ 0\ 1]$ ($G = 5$). Then, the GSSG with primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^5$ produces the MSS-sequence $\{s_j\}$ for $G = 5$ ($G = [0\ 0\ 1\ 0\ 1]$) for any given initial state. For example, in Table 2.4, we can see that the GSS-sequence produced with $G = 5$ using three different initial states provides shifted versions of the same sequence, the MSS-sequence {1 1 0 0 1 0 0 1 0 1 1 1 0 0 1 0}. ■