# Stream Cipher Design based on Jumping Finite State Machines

Cees J.A. Jansen*
Banksys NV, Brussels, Belgium
cja@iae.nl

August 11, 2005

**Abstract**

This paper presents a new way of constructing binary cascade clock-controlled LFSR sequence generators as building blocks for stream ciphers. In these constructions the bottleneck of multiple clocking shift registers is removed, resulting in so called jump-controlled sequence generators, that operate in a single clock pulse and are most efficient to implement. The constructions make use of special properties of irreducible polynomials over finite fields. This paper also aims at giving insight into the mathematical theory behind the constructions. To this end, theory is developed and many of the rich set of properties of irreducible polynomials over $GF(2)$, such as periods, jump indices and the number and cardinalities of various classes of polynomials are presented.

**Keywords:** LFSR, finite state machine, sequence generation, clock-control, irreducible polynomial, transition matrix, jump index, dual polynomial.

## 1 Introduction

Today stream ciphers are widely used in areas where the combination of security, performance and implementation complexity is of importance. One such area is wireless communications (GSM, 3GPP, Bluetooth, IEEE802.11), where a low gate count in hardware or DSP platform implementation requirements prevail. Another area is highspeed link encryption where encryption rates of tens of gigabits per second are quite common. Although many streamcipher algorithms have been broken, a number of secure stream ciphers still exist and new initiatives like the European ECRYPT STVL stream cipher project, [5] are proposed.

In stream cipher cryptography a well known construction for generating complex sequences is based on cascading clock controlled feedback shift registers. With this method (see e.g. [13]) subsequent linear FSRs are clocked, i.e. stepped through their

*J.v. Riebeeckstraat 10, 5684 EJ Best, The Netherlands

state space, by a previous LFSR output one or more times before using the corresponding output bit. Due to the multiple clocking feature, this construction generally results in a decreased rate of sequence generation, rendering it less attractive for high speed implementations. The more general problem of finding an efficient way to let an autonomous linear finite state machine make one big step, i.e. moving to a state more than one step further, without having to traverse consecutive intermediate states, motivated the research of which the results are presented here in detail. Several parts of these results were presented earlier at RECSI VII, [9], and at SASC 2004, [10], but this paper is an extended version containing proofs of theorems. A paper from the author describing some extensions to general finite fields appeared in [11]. Stream cipher proposals based on the theory of this paper, were submitted in April 2005 to the ECRYPT stream cipher call [18, 15].

In Section 2 some basic notation and theory is introduced. Section 3 discusses a new way of effectively multiple clocking binary Linear Finite State Machines, which makes use of a property of the associated irreducible characteristic polynomial denoted by the name Jump Index. Also, an additional involution operation on polynomials is introduced, which characterizes the natural multiple clocking (or jumping) behaviour of LFSMs. Additional conditions for LFSMs with clock-controlled jumps are given in Section 4. In Section 5 sets of binary irreducible polynomials are defined, containing sets of 1, 2, 3 and 6 polynomials which are related by alternate application of the two different operators. The existence conditions of these sets and the cardinalities of the classes of sets for given degrees are presented. Section 6 discusses the generalisation of the theory developed in the previous sections to composite polynomials. Finally, we conclude in Section 7.

# 2 Linear Feedback Shift Register Basics

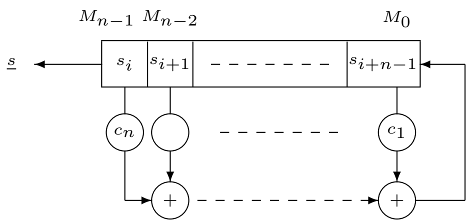


Figure 1: The Linear Feedback Shift Register

Linear feedback shift registers are widely used in sequence generators for cryptographic purposes. They implement in a very natural way a linear recurrence relation between the individual sequence symbols generated. A figure of an LFSR over $GF(q)$ is shown in Figure 1. The sequence $\underline{s} = (\ldots, s_i, s_{i+1}, \ldots)$ satisfies the linear recurrence relation (1) of order $n$.

$$s_{j+n} = \sum_{i=1}^{n} c_i s_{j+n-i} \quad \Longleftrightarrow \quad \sum_{i=0}^{n} c_i s_{j+n-i} = 0, \quad \text{with } c_0 = -1 \tag{1}$$

The feedback coefficients $c_i$ are usually written as a so called Feedback Polynomial (sometimes called Connection Polynomial), $F(x)$, of degree equal to the length of the recursion $n$, as given by (2).

$$\text{Feedback Polynomial} \qquad F(x) := \sum_{i=0}^{n} c_i x^i \tag{2}$$

The $n^{\text{th}}$ order linear recursion is commonly represented by its Characteristic Polynomial, $C(x)$, also of degree $n$, as given by (3).

$$\text{Characteristic Polynomial} \qquad C(x) := \sum_{i=0}^{n} c_i x^{n-i} \tag{3}$$

Polynomials $F$ and $C$ are each others reciprocals, i.e. the roots of $F(x)$ are the reciprocals of the roots of $C(x)$. This relation is commonly expressed as $C(x) = x^n F(x^{-1})$ or vice versa. Some authors take $-c_i$ as feedback coefficients, whence $c_0 = 1$ resulting in a monic characteristic polynomial, see e.g. [4, pg. 26]. It is customary to consider only the monic version of the Feedback Polynomial, i.e. $c_n^{-1} F(x)$.

In general the order $n$ of the recursion need not be minimal, meaning that there may be another recursion of order less than $n$, which the generated sequence satisfies. The minimal order recursion of a sequence gives rise to the so called Minimal Polynomial $M(x)$ of $\underline{s}$. This minimal polynomial is unique and divides the characteristic polynomial $C(x)$ (see e.g. [12, pp. 418–423,102]). The roots of $C(x)$ form solutions of the recursion equation.

Another way to look at the LFSR is to consider it as a Linear Finite State Machine. In this case the state of the LFSM is represented by a vector $\underline{\sigma}^t = (\sigma_{n-1}^t, \sigma_{n-2}^t, \ldots, \sigma_0^t)$, where $\sigma_i^t$ denotes the content of memory cell $M_i$ after $t$ transitions. As the finite state machine is linear, transitions from one state to the next can be described by a multiplication of the state vector with a transition matrix $\boldsymbol{T}$, i.e. $\underline{\sigma}^{t+1} = \underline{\sigma}^t \boldsymbol{T}$, for $t \geq 0$. The transition matrix is given by (4) for the LFSR of Figure 1.

$$\boldsymbol{T} = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_n \\ 1 & 0 & \cdots & 0 & c_{n-1} \\ 0 & 1 & \cdots & 0 & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_1 \end{pmatrix} \tag{4}$$

It can be seen that the matrix is equal to the so called companion matrix (see e.g. [12, pp. 67–68,102]) of the polynomial $x^n - c_1 x^{n-1} - \cdots - c_{n-1} x - c_n = C(x)$. The characteristic polynomial of $\boldsymbol{T}$ in the linear algebra sense, i.e. $\det(x\boldsymbol{I} - \boldsymbol{T})$, precisely equals this polynomial and, hence, $C(\boldsymbol{T}) = 0$. So the companion matrix plays the role of a root of $C$ and, consequently, can be used to form solutions of the recursion equation. Several authors use slightly different definitions of a companion matrix, depending on the use of column or row vector representation and the shift direction of the LFSR as can be seen in [7, pg. 35] and [17, pg. 132]. In Section 3 we will have a closer look at companion matrices of polynomials.

From the foregoing it can be concluded that multiple clocking of an LFSR in fact comes down to multiplying the state vector with some power of the transition matrix. A new transition matrix can be constructed by raising the original matrix to some power and rewiring the LFSR accordingly. Strictly speaking this results in a LFSM which need not be a shift register. Also, switching between the two transition matrices, as is needed for cascade clock control is easily achieved by means of a switch for every memory cell. This method is used in many stream cipher implementations, for instance in the Jansen-Roelse Synchronous Stream Cipher [6], which is used for streaming data protection. However, there exists a more efficient way to implement the conditional multiple clocking of LFSRs as will be shown in the next section.

# 3 Jumping: a natural way of multiple clocking

In the remainder of this paper we will focus on the binary case, although many results obtained in this paper have been generalized in a rather straightforward manner to $GF(q)$, see [11]

Let $\boldsymbol{A}$ denote the transition matrix of an autonomous Linear Finite State Machine, not necessarily a shift register, and let $f(x)$ denote its characteristic polynomial, i.e. $f(x) = \det(x\boldsymbol{I} + \boldsymbol{A})$. The principal question we ask ourselves here is if it is possible in general to find a power of the transition matrix, which is equal to a linear combination of the matrix raised to two smaller powers: $\boldsymbol{A}^t = \boldsymbol{A}^{t_1} + \boldsymbol{A}^{t_2}$, with $t_1, t_2 < t$. The simplest useful case is the one where there exists a $J$, such that $\boldsymbol{A}^J = \boldsymbol{A} + \boldsymbol{I}$. If indeed such a power of the transition matrix exists, we clearly achieve the same effect if we multiply the state vector either by $\boldsymbol{A}^J$ or by $\boldsymbol{A} + \boldsymbol{I}$. Moreover, changing $\boldsymbol{A}$ into $\boldsymbol{A} + \boldsymbol{I}$ is generally much simpler than rewiring $\boldsymbol{A}$ into $\boldsymbol{A}^J$ for an arbitrary transition matrix $\boldsymbol{A}$. Also, this modification of the transition matrix is an involution, which makes it easier to assess the relevant properties for a practical implementation, in which the transformation and its inverse are needed. As is well known, if $f(x)$ is irreducible then $\boldsymbol{A}$ can be written as the companion matrix of $f(x)$ by applying a suitable matrix multiplication, $\boldsymbol{A}' = \boldsymbol{M}\boldsymbol{A}\boldsymbol{M}^{-1}$, which is always possible; see e.g. [17, 1]. The matrices $\boldsymbol{A}$ and $\boldsymbol{A}'$ are called *similar* matrices.

Note that powers of the companion matrix can be seen to represent all elements of the finite field. Hence, an equivalent statement of the problem is to find an element $\alpha^J$ in the finite field $GF(2^n)$, with $f$ as defining polynomial and $n = \deg(f)$, such that $\alpha^J = \alpha + 1$, where $\alpha$ is an element of $GF(2^n)$. The latter is a special case of Jacobi's logarithm, [12, pp. 79,542], which is defined for non-zero field elements as $\alpha^m + \alpha^n = \alpha^{m+L(n-m)}$. In the case at hand, we have $n = 1$ and $m = 0$, so that $J = L(1)$. The reader more acquainted with Zech's logarithms [8], defined as $\alpha^{Z(x)} = \alpha^x + 1$, note that $J = Z(1)$.

One can conclude from the foregoing that by changing the transition matrix of the Autonomous LFSM from $\boldsymbol{A}$ into $\boldsymbol{A}+\boldsymbol{I}$, effectively $J$ steps through the state space of the original LFSM are made, regardless of the starting state. This jump of $J$ states gives rise to the following definition.

**Definition 1** *Let $f(x)$ be an irreducible polynomial over $GF(2)$. If $x^J \equiv x+1 \bmod f(x)$, for some integer $J$, then $J$ is called the Jump Index of $f$.*

The Jump Index does not exist for every irreducible polynomial, as this depends on the condition $x^J \equiv x+1 \bmod f(x)$ or equivalently $f(x)|(x^J+x+1)$ for some $J$. In other words: $\alpha^J = \alpha+1$, where $\alpha$ is a root of $f(x)$ and, hence, an element of the splitting field $GF(2^n)$ of $f(x)$.

Obviously, it follows that $J \geq \deg(f)$. For irreducible trinomials of the form $x^n+x+1$ the jump index equals the degree of the trinomial. Also, for primitive polynomials, i.e. irreducible polynomials of maximal order (period) $2^n-1$, where $n$ is the degree of $f$, the jump index always exists. The latter can be seen from the fact that $x$ is a primitive element in this case, so successive powers of $x$ generate all non-zero elements of $GF(2^n)$, including the element $x+1$.

The Jump Index is an important parameter of irreducible polynomials just as the period is, because both values determine whether the irreducible polynomial can be used as characteristic polynomial of a shift-multiple-shift LFSR (in general a step-or-jump LFSM), as will be seen later.

Let $f^{\perp}(x)$ denote the characteristic polynomial of the modified transition matrix, it follows that

$$f^{\perp}(x) = \det(x\boldsymbol{I}+\boldsymbol{A}+\boldsymbol{I}) = \det((x+1)\boldsymbol{I}+\boldsymbol{A}) = f(x+1) \tag{5}$$

We have the following definition.

**Definition 2** *Let $f(x)$ be an irreducible polynomial over $GF(2)$. The dual of $f(x)$, denoted by $f^{\perp}(x)$ is defined as $f(x+1)$.*

We call $f^{\perp}(x)$ the *dual* of $f(x)$ because $(f^{\perp})^{\perp} = f((x+1)+1) = f(x)$, which is an involution transformation on polynomials. Moreover, if $f(x)$ has jump index $J$ then the sums of $\alpha$ and $\alpha^J$ for all roots lie in the base field and are equal to 1. The duality operator clearly preserves the degree of the polynomial. The period (or order) of $f$ is not necessarily preserved, as a simple counter example shows: $f(x) = x^4+x^3+1$ has period 15, but $f^{\perp}(x) = f(x+1) = x^4+x^3+x^2+x+1$ has period 5. Irreducibility is also preserved as stated in the following theorem:

**Theorem 1** *Let $f(x)$ be an irreducible polynomial over $GF(2)$, then the dual of $f(x)$, $f^{\perp}(x) = f(x+1)$ is also irreducible.*

**Proof.** Suppose $f^{\perp} = g \cdot h$. Then $(f^{\perp})^{\perp} = g(x+1)h(x+1) = g^{\perp} \cdot h^{\perp} = f$, which contradicts the fact that $f$ is irreducible. □

Clearly, the dual of a reducible polynomial can be defined analogously. This generalization will be treated in Section 6.

Let $f^*(x)$ denote the reciprocal of $f(x)$, i.e. $f^*(x) = x^n f(x^{-1})$. The reciprocal of the characteristic polynomial plays an important role, e.g. as the connection polynomial of LFSRs as was introduced in the previous section. Taking the reciprocal of a polynomial is also an involution operation, provided the polynomial does not contain $x$ as one of its factors. Therefore, one usually considers polynomials with irreducible factors of degree 2 and higher. This is of particular importance, if one considers the interplay of both operators, as $(x+1)^{\perp} = x$ and $x$ has no reciprocal.

A natural question to ask is how the jump indices of a polynomial, its dual and its reciprocal are related. The answer is given by the next theorem:

**Theorem 2** *Let $f$ be an irreducible polynomial of degree $n \geq 2$ over $GF(2)$ with jump index $J$. The jump indices of $f^{\perp}$ and $f^*$, denoted by $J^{\perp}$ and $J^*$ respectively, have the following relation to $J$:*

$$J^{\perp} = J^{-1} \bmod \operatorname{per}(f) \tag{6}$$

$$J^{*} = 1 - J \bmod \operatorname{per}(f) \tag{7}$$

**Proof.** Let $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ be the roots of $f$, then $\alpha^J = \alpha + 1$. The reciprocal $f^*$ has $\alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-2^{n-1}}$ as its roots, and so $\alpha^{-J^*} = \alpha^{-1} + 1$. Multiplying both sides of the latter equation with $\alpha$ gives $\alpha^{1-J^*} = 1 + \alpha = \alpha^J$, hence accounting for (7).

Similarly, $f^{\perp}$ has roots $\alpha^J, \alpha^{2J}, \ldots, \alpha^{2^{n-1}J}$ and so $(\alpha^J)^{J^{\perp}} = \alpha^J + 1 = \alpha$, implying that $J \cdot J^{\perp} \equiv 1 \bmod \operatorname{per}(f)$. □

A consequence of (6) is that the jump index of the dual polynomial only exists if $J$ is relatively prime with the period of $f$. Conversely, if $f$ has a jump index, but $f^{\perp}$ has not, then $\gcd(J, \operatorname{per}(f)) > 1$. In the case that $\gcd(J, \operatorname{per}(f)) = d > 1$, $\alpha^J$ has order $\operatorname{per}(f)/d$ and so the period of $f^{\perp}$ will also be $\operatorname{per}(f)/d$. Theorem 2 also implies that if $f$ has a jump index, then so has $f^*$.

From (7) un upperbound for the jump index is obtained. Together with $J \geq \deg(f)$ this gives the following result.

$$\deg(f) \leq J \leq 1 + \operatorname{per}(f) - \deg(f). \tag{8}$$

**Example 1** *As an example, let us consider the LFSR shown in Figure 2 of length 7 and characteristic polynomial $x^7+x^6+1$, which is a primitive polynomial of Mersenne-prime period 127. Its reciprocal has characteristic polynomial $x^7+x+1$ with a jump index of 7, equal to its degree. Hence, the jump index of the original polynomial is $127+1-7 = 121$ and the dual polynomial has a jump index of $121^{-1} \bmod 127 = 21$. The dual of the reciprocal is $x^7+x^6+x^5+x^4+x^3+x^2+1$ and has a jump index of $7^{-1} \bmod 127 = 109$. The modified LFSR with this characteristic polynomial is shown in Figure 3.*

The impact on shift-multiple-shift sequence generator design of the theory presented in this section should start to become visible. Apparently, by choosing a very

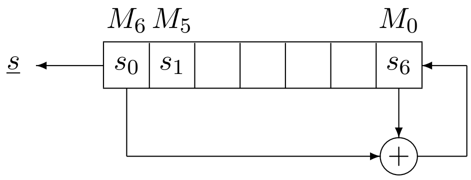


Figure 2: LFSR of length 7 and characteristic polynomial $x^7 + x^6 + 1$

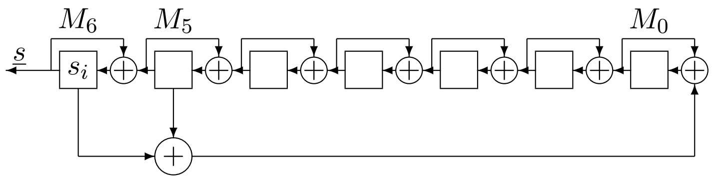


Figure 3: Dual of the Reciprocal: characteristic polynomial $x^7+x^6+x^5+x^4+x^3+x^2+1$

specific number of multiple shifts, the transition matrix of the LFSR raised to this number will be identical to the transition matrix except for the entries on the main diagonal, which are inverted (ones XORed). Equivalently, by adding ones to the entries on the main diagonal of the transition matrix a number of multiple shifts is obtained, equal to the jump index of the characteristic polynomial of that matrix.

The modification of the transition matrix as described here, is of very low complexity, adding only one XOR gate for every cell in the LFSR. Moreover, the number of shifts in a jump of the register, caused by this modification is at least as high as the register length, but can be substantially higher in general. Hence, for many application areas, the method described in this section is much more attractive than the method of rewiring.

Although the general idea is described in this section, many detailed questions concerning e.g. existence conditions of jump indices of polynomials with non-maximal periods are left unanswered here. The intricate consequences of the non-commuting operators $\perp$ and $*$ on sets of dual and reciprocal polynomials is discussed in Section 5. First we will look at clock-controlled LFSR's in more detail.

# 4 LFSR's with clock-controlled jumps

A typical clock-controlled binary sequence generator is shown in Figure 4. The first LFSR generates a binary sequence $\underline{s}_1$ of period $p_1$, which is some divisor of $2^{L_1} - 1$ in the case of an irreducible feedback, where $L_1$ is the length of the LFSR. This sequence, comprising $N_0$ zeroes and $N_1$ ones, is used to clock the second LFSR, i.e. let the second LFSR step through its state space, depending on the bits of the driving sequence by stepping it $c_0$ or $c_1$ times if the output bit is a 0 or a 1 respectively. The total number $N_s$ of steps made by the second LFSR in one period of the first LFSR satisfies $N_s = N_0c_0 + N_1c_1$. Assume that the second LFSR has irreducible feedback.

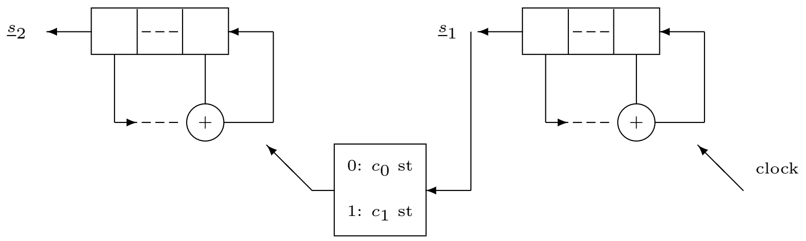


Figure 4: Clock controlled LFSR sequence generator

In order for the output sequence $\underline{s}_2$ of the second LFSR to have a maximal period of $p_1 p_2$ a necessary condition is that $\gcd(N_s, p_2) = 1$. This condition is not sufficient, see [3, Thm 3, pg. 19].

In many situations it is advantageous [19, Ch. 5] to use maximum-length LFSR's, i.e. LFSR's of length $L$ having period $p = 2^L - 1$. In this case the numbers of zeroes and ones, given by $N_0 = \frac{p-1}{2}$ and $N_1 = \frac{p+1}{2}$, have a disparity of 1, caused by the fact that the all-zero state does not occur. The total number of steps is now given by $N_s = c_0 p + (c_1 - c_0)2^{L-1}$. Consequently, if the second LFSR has a period $p_2$ equal to $p$ (or one of its divisors), then the necessary condition for maximum $\underline{s}_2$ period becomes

$$\gcd(N_s, p_2) = \gcd(c_1 - c_0, p) = 1. \tag{9}$$

This condition can be generalised in the case of more clocking constants. Consider for example the NESSIE proposal LILI-128 [16], which uses four different clocking constants (1,2,3 and 4), based on two different taps of a driving maximum-length LFSR. Let $c_{00}$, $c_{01}$, $c_{10}$ and $c_{11}$ denote the number of steps if the two taps have values 00, 01, 10 and 11, occurring $N_{00}$, $N_{01}$, $N_{10}$ and $N_{11}$ times in a period $p$ respectively. Because of the maximum-length sequence $N_{01} = N_{10} = N_{11} = \frac{p+1}{4}$ and $N_{00} = p - 3\frac{p+1}{4} = \frac{p-3}{4}$. Hence, $N_s = (c_{01}+c_{10}+c_{11})\frac{p+1}{4}+c_{00}\frac{p-3}{4} = (c_{01}+c_{10}+c_{11}-3c_{00})2^{L-2}+c_{00}p$. The condition for maximum period now becomes $\gcd(c_{11}+c_{10}+c_{01}-3c_{00}, p) = 1$. In LILI-128 this condition does not apply as the LFSR's have different lengths, but the maximum period condition is trivially satisfied by the fact that $p_2 = 2^{89} - 1$, which is a Mersenne prime.

In the special case that jumping LFSR's are used, that either make one step or a jump equivalent to $J$ steps, it is seen that condition (9) can be written as

$$\gcd(J - 1, p) = 1, \tag{10}$$

or also

$$\gcd(J^*, p) = 1, \tag{11}$$

where (11) follows from (10) by application of (7). In other words: the jump index of the feedback polynomial (of the jumping LFSR) must be relatively prime with its period.

# 5 Classes of binary irreducible polynomials

Let $f(x)$ be an irreducible polynomial over $GF(2)$ of degree $n \geq 2$, with period $p$ and jump index $J$. As defined before, $f^*(x)$ and $f^\perp(x)$ denote the reciprocal and the dual of $f(x)$ resp. As can easily be checked the two operators $\perp$ and $*$ do not commute in general. However, straightforward calculation shows that

$$f^{\perp*\perp} = f^{*\perp*}\,, \tag{12}$$

giving rise to sets of at most 6 different polynomials that are obtained by alternated application of the two operators $\perp$ and $*$. An example of such a set is shown in Figure 5 for all 6 binary irreducible polynomials of degree 5.

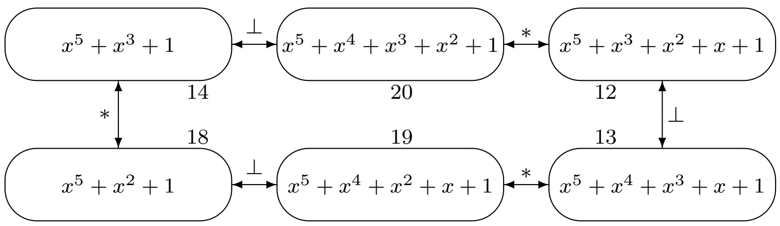


Figure 5: Degree 5 irreducible polynomials over $GF(2)$ forming a set $\mathcal{S}_6$. Also shown are the jump indices.

Interesting cases which arise are the self-dual, self-reciprocal and dual-reciprocal polynomials. A polynomial is self-reciprocal iff $f^* = f$ and is self-dual iff $f^\perp = f$. Analogously, we call a polynomial dual-reciprocal iff $f^* = f^\perp$, implying that $f = f^{*\perp} = f^{\perp*}$. There even exist polynomials which are both self-dual and self-reciprocal. For example $x^2+x+1$ is self-dual and self-reciprocal, $x^4+x^3+x^2+x+1$ is self-reciprocal, $x^4+x+1$ is self-dual and $x^3+x+1$ is dual-reciprocal.

Assume that $f$ is self-reciprocal, but not self-dual. Then it follows from (12) that $(f^{\perp*})^\perp = f^{\perp*}$ and, hence $f^{\perp*}$ is self-dual. Similarly, it follows that if $f$ is self-dual, but not self-reciprocal, then $f^{*\perp}$ is self-reciprocal. As a consequence, for every self-reciprocal irreducible polynomial there exists a self-dual polynomial and vice versa, implying that the number of self-dual irreducible polynomials equals the number of self-reciprocal irreducible polynomials. A further consequence is that there are always three polynomials in such a set formed by application of the dual and reciprocal operators. This case is depicted in Figure 6.

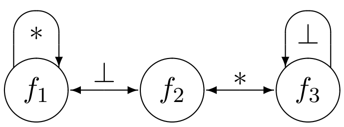


Figure 6: Set $\mathcal{S}_3$ with self-reciprocal $f_1$ and self-dual $f_3$ polynomials

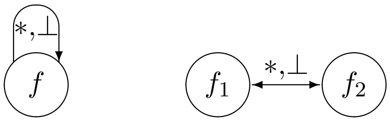


Figure 7: Sets $\mathcal{S}_1$ and $\mathcal{S}_2$

In the case that $f$ is dual-reciprocal, it follows from (12) that there are only two irreducible polynomials in the set formed by application of the two operators, viz. $f$ and $f^* = f^\perp$. Clearly, if a polynomial is both self-dual and self-reciprocal, the set contains only one polynomial. Both situations are shown in Figure 7.

A self-dual polynomial can be applied in situations where the shift-multiple-shift generator's characteristic polynomial must remain the same, regardless whether a shift or a jump is carried out. Dual-reciprocal polynomials result in characteristic polynomials, which are the reciprocals of the originals, when a jump is carried out, thereby effectively generating the reciprocal sequence. Moreover, as will be shown, both types of polynomials have jump indices, which are given by simple expressions, a fact that does not hold in general for arbitrary irreducible polynomials.

It is seen that the two operators $\perp$ and $*$ give rise to classes of polynomials, containing sets of 1, 2, 3 or 6 different, equal degree, irreducible polynomials, denoted by $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_6$ respectively. Table 1 shows the numbers of these sets for degrees from 2 to 32 for $GF(2)$. In this table empty entries represent the value 0, i.e. no such sets exist for that particular degree. The total number of irreducible polynomials is given by (13), see e.g. [12, pp. 91–93].

$$I_q(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}, \quad \text{with } \mu(\cdot) \text{ the Möbius function.} \tag{13}$$

Clearly, if we denote by $S_i(n)$ the number of sets $\mathcal{S}_i$, $i = 1, 2, 3, 6$, we have that $I_2(n) = S_1(n) + 2S_2(n) + 3S_3(n) + 6S_6(n)$.

For the binary case, we will explore the cardinalities of the classes and the necessary existence conditions for the various polynomials in the next subsections. In particular it is shown that $\mathcal{S}_2$ is only non-empty iff $n = \deg(f) \equiv 0 \bmod 3$ and using Berlekamp's counting method the cardinality of this class is determined.

## 5.1 The set $\mathcal{S}_1$

In $GF(2)$ the set $\mathcal{S}_1$ exists only for degree 2. This follows immediately from Theorem 2, by requiring that the relations (6) and (7) both hold for $f(x)$ with $\mathrm{per}(f) = p$:

$$\begin{aligned} J &= 1 - J \bmod p \Longrightarrow 2J^2 = J \bmod p &(14)\\ J &= J^{-1} \bmod p \Longrightarrow 2J^2 = 2 \bmod p &(15) \end{aligned}$$

As $J < p$ it follows that $p = 3$ and $J = 2$. The only irreducible polynomial over $GF(2)$ with these parameters is $x^2 + x + 1$. Moreover, any polynomial $f$ in $\mathcal{S}_1$ must have a jump index, because $f$ is self-dual and hence $\alpha + 1 = \alpha^{2^k}$ for some $k, 0 \leq k < n$, where $n$ is the degree of $f$.

| Degree $n$ | # Irreducible polynomials over $GF(2)$ | Number of Classes | | | |
|---|---|---|---|---|---|
| | | $\mathcal{S}_1$ | $\mathcal{S}_2$ | $\mathcal{S}_3$ | $\mathcal{S}_6$ |
| 2 | 1 | 1 | | | |
| 3 | 2 | | 1 | | |
| 4 | 3 | | | 1 | |
| 5 | 6 | | | | 1 |
| 6 | 9 | | | 1 | 1 |
| 7 | 18 | | | | 3 |
| 8 | 30 | | | 2 | 4 |
| 9 | 56 | | 1 | | 9 |
| 10 | 99 | | | 3 | 15 |
| 11 | 186 | | | | 31 |
| 12 | 335 | | 1 | 5 | 53 |
| 13 | 630 | | | | 105 |
| 14 | 1161 | | | 9 | 189 |
| 15 | 2182 | | 2 | | 363 |
| 16 | 4080 | | | 16 | 672 |
| 17 | 7710 | | | | 1285 |
| 18 | 14532 | | 3 | 28 | 2407 |
| 19 | 27594 | | | | 4599 |
| 20 | 52377 | | | 51 | 8704 |
| 21 | 99858 | | 6 | | 16641 |
| 22 | 190557 | | | 93 | 31713 |
| 23 | 364722 | | | | 60787 |
| 24 | 698870 | | 10 | 170 | 116390 |
| 25 | 1342176 | | | | 223696 |
| 26 | 2580795 | | | 315 | 429975 |
| 27 | 4971008 | | 19 | | 828495 |
| 28 | 9586395 | | | 585 | 1597440 |
| 29 | 18512790 | | | | 3085465 |
| 30 | 35790267 | | 33 | 1091 | 5964499 |
| 31 | 69273666 | | | | 11545611 |
| 32 | 134215680 | | | 2048 | 22368256 |

Table 1: The number of sets $\mathcal{S}_1$,$\mathcal{S}_2$,$\mathcal{S}_3$ and $\mathcal{S}_6$ in the binary case

## 5.2 $\mathcal{S}_3$ and properties of its polynomials

In the beginning of Section 5 it was already shown that a set $\mathcal{S}_3$ consists of three polynomials, one of which is self-reciprocal, and another one which is self-dual. There, we concluded that the number of self-dual polynomials must be equal to the number of self-reciprocal polynomials and, as a consequence, equal to the number of $\mathcal{S}_3$ sets in this class for a certain degree. It is easy to see that self-reciprocal irreducible polynomials cannot exist for odd degrees: the number of non-zero coefficients would necessarily have to be even thus having the value 1 as one of its roots, and hence being divisible by $x + 1$. Therefore, self-reciprocal irreducible polynomials, and consequently also self-dual irreducible polynomials can only exist for even degrees. The following theorem is due to L. Carlitz [2] and gives an expression for the number of self-reciprocal irreducible polynomials over $GF(q)$. Meyn and Götz give a more elegant proof in [14].

**Theorem 3** *The number of monic self-reciprocal irreducible polynomials of degree 2n over GF*$(q)$*,* $I_q^s(n)$*, is given by:*

$$I_q^s(n) = \begin{cases} \frac{1}{2n}(q^n - 1) & n = 2^e,\ q \text{ odd} \\ \frac{1}{2n}\sum_{d|n,\, d \text{ odd}} \mu(d) q^{n/d} & \text{otherwise.} \end{cases} \tag{16}$$

Carlitz' theorem implicitly states that self-reciprocal irreducible polynomials exist over every finite field. In the special case of *GF*(2) we are considering, (16) reduces to:

$$I_2^s(n) = \frac{1}{2n} \sum_{d|n,\, d \text{ odd}} \mu(d) 2^{n/d} \tag{17}$$

This expression also gives the number of self-dual irreducible polynomials over *GF*(2) and, consequently, the number of $\mathcal{S}_3$ sets for all even degrees.

Polynomials that form a set $\mathcal{S}_3$ exhibit certain properties, with regards to their periods and jump indices, which are generally important constraints in the design of sequence generators. We summarize these properties in the following theorem.

**Theorem 4** *Let* $f_1$*,* $f_2$ *and* $f_3$ *be irreducible polynomials of degree* $n > 2$ *over GF*(2) *forming a set* $\mathcal{S}_3$*, such that* $f_1^* = f_1$*,* $f_3^\perp = f_3$ *and* $f_1^\perp = f_2 = f_3^*$*, then the following properties hold:*

- $\mathrm{per}(f_1)|(2^{\frac{n}{2}} + 1)$*, i.e. the period of* $f_1$ *cannot be maximal,*
- $f_1$ *does not have a jump index,*
- *the jump index of* $f_3$ *satisfies* $J(f_3) = 2^{\frac{n}{2}}$*,*
- $\mathrm{per}(f_3) > 2^{\frac{n}{2}} + 1$,
- $\mathrm{per}(f_3)$ *cannot be a prime number.*

**Proof.** Let $\alpha$ be a root of $f_1$ and $\beta$ be a root of $f_3$, both elements of *GF*$(2^n)$.

- Self-reciprocity implies that $\alpha^{-1} = \alpha^{2^k}$, for some $k$, $0 \le k < n$. So $\alpha^{2^k+1} = 1$ and therefore $\mathrm{per}(f_1)|2^k + 1$. As $\mathrm{per}(f_1)$ divides $2^n - 1 = (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}} + 1)$, but does not divide $2^j - 1$ for any $j < n$, it follows that $k = \frac{n}{2}$.

- Suppose $f_1$ has jump index $J$, then $\alpha^J = \alpha + 1$. Self-reciprocity implies that the reciprocal jump index is equal to $J$ and so $\alpha^{-J} = \alpha^{-1} + 1$ or equivalently $(\alpha + 1)^{-1} = \alpha^{-1} + 1$. Hence, $\alpha$ must satisfy $\alpha^2 + \alpha + 1 = 0$ and consequently can only be a root of the second degree polynomial $x^2 + x + 1$.

- Self-duality of $f_3$ implies that $\beta^J = \beta^{2^k}$, for some $k$, $0 \le k < n$. Also, the dual jump index is equal to $J$, so that $J^2 = 1 \bmod \mathrm{per}(f_3)$ and therefore $\mathrm{per}(f_3)|2^{2k} - 1$. As $\mathrm{per}(f_3)$ divides $2^n - 1$, but does not divide $2^j - 1$ for any $j < n$, it follows that $k = \frac{n}{2}$.

- Applying (8) for the jump index of $f_3$ yields $2^{\frac{n}{2}} \leq \mathrm{per}(f_3) + 1 - n$, resulting in $\mathrm{per}(f_3) \geq 2^{\frac{n}{2}} - 1 + n$.
- Self-duality of $f_3$ also implies $J^2 = 1 \bmod p$. Hence, if $p$ is prime, then $J$ either equals 1 or $p - 1$. Both values are excluded by inequality (8), i.e. $n \leq J \leq p + 1 - n$, and so $p$ cannot be prime.

$\square$

Another way to see that self-reciprocal irreducible polynomials of degree $n > 2$ over $GF(2)$ cannot have a jump index is the following. Suppose $f$ is self-reciprocal with jump index $J$ and period $p$, then $J = 1 - J \bmod p$ and so $J = \frac{p+1}{2}$. The jump index of the dual of $f$ then exists and equals $J^{\perp} = (\frac{p+1}{2})^{-1} \bmod p = 2$. However, as the degree of $f$ is higher than 2, so is the degree of $f^{\perp}$ and consequently $J^{\perp} > 2$, contradicting $J^{\perp} = 2$.

The relation between the periods of the polynomials forming an $\mathcal{S}_3$ set is further specified by the following theorem.

**Theorem 5** *Let $f_1$, $f_2$ and $f_3$ be irreducible polynomials of degree $n$ over $GF(2)$ forming an $\mathcal{S}_3$ set, such that $f_1^* = f_1$, $f_3^{\perp} = f_3$ and $f_1^{\perp} = f_2 = f_3^*$, and let $p_1$, $p_2$ and $p_3$ denote their respective periods. Then $p_2 = p_3$, and $p_1$ and $p_3$ are related as follows.*

- *If $p_3$ is maximal, i.e. $p_3 = 2^n - 1$, then $p_1 = 2^{\frac{n}{2}} + 1$.*
- *If $p_3$ is less than maximal, i.e. $p_3 = \frac{2^n-1}{d}$, with $d > 1$, then $p_1 = \frac{2^{\frac{n}{2}}+1}{d_+}$, where $d = d_+d_-$, $d_+, d_- \geq 1$ and $d_+|2^{\frac{n}{2}} + 1$, $d_-|2^{\frac{n}{2}} - 1$.*

**Proof.**

- Clearly, the reciprocal polynomial has the same period as the original, hence $p_2 = p_3$.
- If $p_3 = 2^n - 1$, then $f_2$ has a jump index $J^* = 2^n - 2^{\frac{n}{2}}$. So $\gcd(J^*, p_3) = \gcd(2^{\frac{n}{2}}(2^{\frac{n}{2}} - 1), 2^n - 1) = 2^{\frac{n}{2}} - 1$, as $n$ is even. Therefore, as $f_1$ is the dual of $f_2$, $p_1 = 2^{\frac{n}{2}} + 1$.
- Let $p_3 = \frac{2^n-1}{d} = \frac{2^{\frac{n}{2}}+1}{d_+} \cdot \frac{2^{\frac{n}{2}}-1}{d_-} = p_+p_-$. Note that $d_+$ and $d_-$ are both odd. Also, any odd divisor of $2^{\frac{n}{2}} - 1$ greater than 1 does not divide $2^{\frac{n}{2}} + 1$ and vice versa, because of the difference of 2. The jump index $J^*$ of $f_2$ in this case equals $J^* = p_3 + 1 - 2^{\frac{n}{2}} = p_+p_- - d_-p_- = (p_+ - d_-)p_-$. So $\gcd(J^*, p_3) = \gcd(p_+p_- - d_-p_-, p_+p_-) = p_-$. Hence $p_1 = p_+ = \frac{2^{\frac{n}{2}}+1}{d_+}$.

$\square$

A consequence of Theorem 5 is that different $p_3$ can go together with the same $p_1$, but not vice versa. Moreover, $p_3 > 2^{\frac{n}{2}} + 1$ by Theorem 4, so that always $p_1 < p_3$. In general, as $p_1 = p_+$, which divides $p_3$, we have, using the smallest odd divisor 3, that $p_1 \leq p_3/3$, which is obtained with equality for $n = 4$.

Theorem 4 implies that self-dual irreducible polynomials are always divisors of $x^{2^{\frac{n}{2}}} + x + 1$, a property that can be used for the generation of such polynomials.

### 5.3 The class of $\mathcal{S}_2$ sets

The set $\mathcal{S}_2$ was introduced in the beginning of Section 5 as a set consisting of two polynomials, which are each others dual-reciprocals, meaning that $f^* = f^\perp$. The question to be answered first is about the existence conditions of these polynomials. The answer is given by the following lemma and theorems.

**Lemma 6** *Let $f_1$ and $f_2$ be degree $n$ irreducible polynomials over $GF(2)$, forming a dual-reciprocal pair, i.e. $f_1^* = f_1^\perp = f_2$ and $f_2^* = f_2^\perp = f_1$. Also, let $J_1$ and $J_2$ denote their respective jump indices and $p = \mathrm{per}(f_1) = \mathrm{per}(f_2)$ their period. Then $J_1 = -2^{k_1} \bmod p$, and $J_2 = -2^{k_2} \bmod p$, with $k_1 + k_2 = n$.*

**Proof.** Let $\alpha$ be a root of $f_1$, then $\alpha + 1$ is a root of $f_2$. However, as $f_2$ is also the reciprocal of $f_1$, $\alpha^{-1}$ is also a root of $f_2$. Hence, $\alpha + 1 = \alpha^{-2^{k_1}}$, for some $k_1$, with $0 \le k_1 < n$, and consequently $J_1 = -2^{k_1} \bmod p$. The same reasoning can be applied to a root of $f_2$, yielding a similar expression for $J_2$. As $f_1$ and $f_2$ are each others duals, relation (6) can be applied: $J_1 J_2 = 2^{k_1+k_2} = 1 \bmod p$. The trivial case $k_1 = k_2 = 0$ is ruled out, as it applies to $\mathcal{S}_1$. Taking into account that $p|2^j - 1$, for $j = n$, but for no $j < n$, we obtain $k_1 + k_2 = n$. □

**Theorem 7** *Let dual-reciprocal irreducible polynomials be defined as before. Dual-reciprocal irreducible polynomials over $GF(2)$ only exist for degrees $n \equiv 0 \bmod 3$.*

**Proof.** Let $f_1$ and $f_2$ be irreducible polynomials forming a dual-reciprocal pair, let $J_1$ and $J_2$ be their respective jump indices and let $p$ denote their period. First note that, as $f_1$ and $f_2$ are each others reciprocals, relation (7) holds for their jump indices. Using Lemma 6 we obtain $J_2 = 1 + 2^{k_1} = -2^{k_2} \bmod p$ and $J_1 = 1 + 2^{k_2} = -2^{k_1} \bmod p$. The latter implies that

$$1 + 2^{k_1} + 2^{k_2} = 0 \bmod p, \tag{18}$$

or equivalently $p|1 + 2^{k_1} + 2^{k_2}$. Secondly, as the duals are also reciprocals, we have $J_i J_i^* = 1 \bmod p$, and so $-2^{k_i}(1 + 2^{k_i}) = 1 \bmod p$, for $i = 1, 2$. Combined with (18) this gives $2^{2k_1} = 2^{k_2} \bmod p$ and $2^{2k_2} = 2^{k_1} \bmod p$. Hence, $2^{4k_i} = 2^{k_i} \bmod p$, or, equivalently $2^{k_i}(2^{3k_i} - 1) = 0 \bmod p$, for $i = 1, 2$. The trivial case $k_1 = k_2 = 0$ is again ruled out. It then follows that either $3k_i = n$ or $3k_i = 2n$ and as a consequence $n \equiv 0 \bmod 3$. □

The polynomials belonging to a set $\mathcal{S}_2$ also have special properties with regards to their periods and jump indices. These properties are now easily obtained.

**Corollary 8** *Let $f_1$ and $f_2$ be degree $n$ irreducible polynomials with period $p$ that form a dual-reciprocal pair, then the following properties hold:*

- *the jump indices $(\bmod p)$ are $-2^{\frac{n}{3}}$ and $-2^{\frac{2n}{3}}$, or equivalently $1+2^{\frac{2n}{3}}$ and $1+2^{\frac{n}{3}}$,*
- *$p|(2^{\frac{2n}{3}} + 2^{\frac{n}{3}} + 1)$.*

**Proof.**

- From the proof of Theorem 7 this follows immediately.
- The values for the $k_i$ obtained in Theorem 7 substituted in equation (18).

□

This result demonstrates the existence of irreducible polynomials with non-maximal periods that have jump indices. Corollary 8 implies that dual-reciprocal irreducible polynomials are always divisors of $x^{1+2^{\frac{n}{3}}} + x + 1$ or its reciprocal, a property that can be used for the generation of these polynomials. Moreover, as dual-reciprocal irreducible polynomials exist for all degrees $n \equiv 0 \bmod 3, n > 6$, as will be shown by the next two theorems, it follows that trinomials of the form $x^{2^m+1} + x + 1$ cannot be irreducible for $m > 3$.

Although Theorem 7 gives a necessary condition for the existence of dual-reciprocal polynomials, this condition is not sufficient, as shown by the following theorem.

**Theorem 9** *Dual-reciprocal irreducible polynomials of degree 6 over GF(2) do not exist.*

**Proof.** Recall that the jump index cannot be less than the degree of the irreducible polynomial. For dual-reciprocal polynomials this results in the condition $J = 1+2^{\frac{n}{3}} \geq n$. For all values of $n \equiv 0 \bmod 3$ except for $n = 6$ this condition is satisfied. □

Another way to see that degree 6 irreducible dual-reciprocals do not exist, is the fact that any such $f(x)$ must divide $x^5+x+1$ or its reciprocal $x^5+x^4+1$. Indeed, Table 1 shows that for degree 6 there is no set $\mathcal{S}_2$.

For degrees higher than 6 and divisible by 6, both $\mathcal{S}_2$ and $\mathcal{S}_3$ sets exist. Table 1 also seems to indicate that the number of dual-reciprocal irreducible polynomials is relatively sparse. The exact number of dual-reciprocals can be counted following for instance Berlekamp's refined approach ([1, pp. 76–84]), which uses the multiplicative form of the Möbius Inversion Formula. The result is given by the following theorem.

**Theorem 10** *Let $I_2^d(3m)$ denote the number of dual-reciprocal irreducible polynomials of degree $3m$, $m \geq 1$ over GF(2), and let $S_1(m)$, $S_3(m)$ and $S_6(m)$ denote the number of $\mathcal{S}_3$ and $\mathcal{S}_6$ sets of degree $m$ irreducible polynomials, then we have:*

$$I_2^d(3m) = I_2(m) - S_1(m) - S_3(m) - 2S_6(m) \tag{19}$$

$$S_2(3m) = S_2(m) + S_3(m) + 2S_6(m) \tag{20}$$

We suffice by giving a rough sketch of the proof. Suppose we count the number of dual-reciprocal polynomials of degree $n = 3m$, by assuming that they are comprised of dual-reciprocal *irreducible* polynomials only. Then, as the degrees of all dual-reciprocal irreducibles must be divisible by 3, this counting problem is exactly the same as counting ordinary irreducible polynomials of degree $m$ and, thus, gives a contribution of $I_2(m)$. However, when counting the composite polynomials of degree $n = 3m$, one has to also take into account products of three $m$-degree polynomials from the same set $\mathcal{S}_1$, $\mathcal{S}_3$ or $\mathcal{S}_6$. For if $f = f_1^3$, with $f_1 \in \mathcal{S}_1$, or $f = f_1 f_2 f_3$, with $f_1$, $f_2$,

$f_3$ from one set $\mathcal{S}_3$, then $f^* = f^\perp = f$. Also, if $\mathcal{S}_6$ is given by $\{f_1 \xrightarrow{\perp} f_2 \xrightarrow{*} f_3 \xrightarrow{\perp} f_4 \xrightarrow{*} f_5 \xrightarrow{\perp} f_6 \xrightarrow{*} f_1\}$, then for $f_a = f_1 f_3 f_5$ and $f_b = f_2 f_4 f_6$ we have that $f_a^* = f_a^\perp = f_b$. So the number of $S_1$ and $S_3$ sets and twice the number of $S_6$ sets have to be subtracted from the total number of irreducible polynomials of degree $m$.

The number of sets $\mathcal{S}_2$ is obviously equal to half the number $I_2^d(3m)$. Equation (20) follows from (19), because $I_2(m) = S_1(m) + 2S_2(m) + 3S_3(m) + 6S_6(m)$.

Additionally, for $m > 2$, the following equations can be derived from (20):

$$S_2(3m) = \frac{1}{3}(I_2(m) + S_2(m)) \tag{21}$$

$$I_2^d(3m) = \begin{cases} \frac{2}{3}(I_2(m) + S_2(m)) & m \equiv 0 \bmod 3 \\ \frac{2}{3} I_2(m) & \text{otherwise} \end{cases} \tag{22}$$

Note: it can be observed from Table 1 and can be derived from equation (17) that a relation similar to (21) holds for $S_3$ sets, i.e.

$$S_3(2m) = \frac{1}{2}(I_2(m) + S_3(m)) \tag{23}$$

By repeated application of equation (21) one can obtain a closed form expression similar to (17) for the number of $S_2$ sets.

$$S_2(3n) = \frac{1}{3n} \sum_{d|m} \mu(d) 2^{\frac{n}{d}};\ n = 3^e m, m > 2 \tag{24}$$

Note that, using Corollary 8, a good approximation for $S_2(n)$ is given by $\lfloor \frac{2^{\frac{n}{3}}+1}{n} \rfloor$.

### 5.4 The class of $\mathcal{S}_6$ sets

With the results of the previous subsections it should be clear that all irreducible polynomials over $GF(2)$, not being self-reciprocal, self-dual or dual-reciprocal must form sets of six polynomials under alternated application of the two operators $*$ and $\perp$. Therefore, if $n$ is odd and $n \neq 0 \bmod 3$, then $I_2(n) = 0 \bmod 6$, i.e. the number of irreducible polynomials of that degree is divisible by 6. For other degrees, the number of $\mathcal{S}_3$ and $\mathcal{S}_2$ sets are determined first, using equations (16) and (19). The numbers in Table 1 are thus accounted for.

## 6 Composite polynomials

In the previous sections we considered irreducible polynomials only. The theory developed sofar can be extended to include composite polynomials. In this section some results of Section 3 and Section 5 are generalized in this way.

As a starting point, it should be noted that in the first two definitions the word "irreducible" can be omitted. Clearly, Theorem 1 implies that the number of irreducible factors of a polynomial, as wel as their multiplicities remain the same for the dual polynomial. Theorem 2 also holds for composite polynomials $f$ of degree $n$ over $GF(2)$ with a jump index $J$, having irreducible factors of degree at least 2. Let $x^J + x + 1 = k(x)f(x)$, then

$$\begin{aligned} x^J + x^{J-1} + 1 &= (x^J + x + 1)^* = k^*(x)f^*(x) \\ x^p + 1 &= l(x)f^*(x), \quad p = \mathrm{per}(f^*) \\ x^J + x^{J-1} + x^p &= (l(x) + k^*(x))f^*(x) \\ &= x^{(J-1)}(x + 1 + x^{p+1-J}), \end{aligned}$$

so:

$$x^{p+1-J} + x + 1 \equiv 0 \bmod f^*(x), \text{ as } f^* \text{ has no factor } x.$$

Similarly, let $x^{J^\perp} + x + 1 \equiv 0 \bmod f^\perp(x)$, then $(x^J)^{J^\perp} + x^J + 1 \equiv 0 \bmod f(x)$, and so $x^{JJ^\perp} \equiv x \bmod f(x)$, whence $J \cdot J^\perp \equiv 1 \bmod \mathrm{per}(f(x))$. As a consequence, the upper and lower bounds for the jump index of an irreducible polynomial as given by (8) also hold for the jump index of a composite polynomial with irreducible factors of degree at least 2.

Next, consider two irreducible polynomials $f_1$ and $f_2$, which both have the same jump index $J$. Clearly, $x^J + x + 1$ is divisible by both $f_1$ and $f_2$, and therefore this trinomial must be divisible by the product $f_1 f_2$. Now, suppose that $f_1$ and $f_2$ have unequal jump indices $J_1$ and $J_2$ and periods $p_1$ and $p_2$ resp. Let $\alpha_1$ be a root of $f_1$ and $\alpha_2$ a root of $f_2$. If the product $f_1 f_2$ has jump index $J$, then obviously $\alpha_i^J = \alpha_i + 1 = \alpha_i^{J_i}$, $i = 1, 2$. This means that $J \equiv J_i \bmod p_i$, $i = 1, 2$, and so the jump index of the product is obtained by application of the Chinese Remainder Theorem (CRT). These results prove the following theorem.

**Theorem 11** *Let $f = f_1 f_2 \cdots f_t$, where all the $f_i$ are distinct irreducible polynomials of degree at least 2 over $GF(2)$, having periods $p_i$ and jump indices $J_i$. The jump index $J$ of $f$ is given by the solution of $\forall_{i\in[1,t]}(J \equiv J_i \bmod p_i)$, if such a solution exists*

From the CRT it is known that a necessary condition for a solution to exist in the case of unequal jump indices is that the corresponding periods must be coprime.

The next natural question to ask is what the jump index is of an irreducible polynomial raised to some positive power. The answer is given by the following theorem.

**Theorem 12** *Let $f(x)$ be an irreducible polynomial over $GF(2)$ and let $g(x) = (f(x))^n$, $n > 1$, then $g(x)$ does not have a jump index.*

**Proof.** Let $\tau(x) = x^J + x + 1$ for some integer $J$ and let $\tau'(x)$ denote the formal derivative of $\tau(x)$. If $J$ is even, then $\tau'(x) = 1$, else $\tau'(x) = x^{J-1} + 1$. So for $J$ even $\gcd(\tau, \tau') = 1$, implying that $\tau(x)$ contains no repeated factors. For $J$ odd $\tau(x) = x\tau'(x) + 1$ holds. In this case suppose that $\tau(x)$ and $\tau'(x)$ have a common factor $f(x)$ of degree $> 0$, then $\tau(x) = k(x)f(x)$ and $\tau'(x) = l(x)f(x)$. Substitution yields $k(x)f(x) = xl(x)f(x) + 1$ resulting in $f(x)(k(x) + xl(x)) = 1$. The latter equation has one solution, $f(x) = 1$ and $k(x) = xl(x) + 1$, which contradicts the assumption that $f(x)$ has degree $> 0$. Hence, also for $J$ odd $\gcd(\tau, \tau') = 1$. This proves that $x^J + x + 1$ does not contain repeated factors and consequently, there exists no $J$ such that $(f(x))^n$ divides $x^J + x + 1$ for $n > 1$. □

From the two previous theorems it follows that the factors of the trinomial $x^J + x + 1$ are all distinct irreducible polynomials with jump indices equal to $J$ modulo their respective periods. This means that the factorization of $x^J + x + 1$ precisely gives the possible products of irreducible polynomials, resulting in a jump index $J$ as illustrated by the next example.

**Example 2** *Consider the irreducible polynomials $f_1(x) = x^5 + x^3 + x^2 + x + 1$ of period 31 and $f_2 = x^4 + x^3 + 1$ of period 15. Both $f_1$ and $f_2$ have jump index 12 and therefore their product also has jump index 12 and divides $x^{12} + x + 1$. The remaining factor $f_3$ of this trinomial is $x^3 + x^2 + 1$, which has period 7 and jump index 5, indeed corresponding to* $12 \bmod 7$.

*The reciprocals of the three polynomials, i.e. $f_1^*$, $f_2^*$, $f_3^*$, have respective jump indices of 20, 4 and 3. Their product $f_1^* f_2^* f_3^* = x^{12} + x^{11} + 1$ has period* $7 \cdot 15 \cdot 31 = 3255$ *and using the CRT its jump index is found to be 3244, which corresponds to* $3255 + 1 - 12$. *Note that $x^{12} + x^{11} + 1$ divides $x^{3244} + x + 1$ but no such trinomial with a smaller $J$.*

The trinomial $x^J + x + 1$ does not have $x + 1$ as a factor, and therefore, as a direct result of Theorem 11 and Theorem 12, it must be the product of distinct irreducible factors of degree $\geq 2$. More specifically, given the value of $J$, the irreducible factors are obtained from calculating $J \bmod p_i$, for all periods $p_i$ of irreducible polynomials, as an alternative sieving method. For example, $x^2 + x + 1$ is a factor of $x^J + x + 1$ iff $J \equiv 2 \bmod 3$. Similary, $x^3 + x + 1$ is a factor of $x^J + x + 1$ iff $J \equiv 3 \bmod 7$, etc.

From Theorem 4 and Corollary 8 it is seen that for a given degree $n$ more than one irreducible polynomials with the same jump index can exist. This is the case for self-dual and dual-reciprocal polynomials, which have jump indices of $2^k$ and $1 + 2^l$ resp., for some $k$ and $l$. In this case the corresponding trinomials $x^J + x + 1$ are also self-dual and dual-reciprocal respectively, as can easily be verified. For example, $x^{1024} + x + 1$ factors into the 51 self-dual degree 20 polynomials and one self-dual polynomial of degree 4 and jump index $1024 \bmod 15 = 4$. As a second example consider $x^{1025} + x + 1$, which factors into the 33 degree 30 and the 2 degree 15 dual-reciprocal polynomials with jump index 1025, the remaining factors being $x^3 + x + 1$ with jump index $1025 \bmod 7 = 3$ and $x^2 + x + 1$ with jump index $1025 \bmod 3 = 2$.

The factorization of $x^J + x + 1$ for $2 \leq J \leq 33$ is given in Table 2 with the factors listed in octal notation. In the "Properties" column of this table the degrees of the factors are given or an 'i' is listed if the trinomial is irreducible. It is also indicated if the trinomial is self-dual or dual-reciprocal with 'sd' and 'dr' respectively.

# 7 Conclusions

In this paper the Jump Index of polynomials over $GF(2)$ was introduced as an important parameter in the design of efficient sequence generators based on clock-controlled

| Factorization of $x^J + x + 1$ | | |
|---|---|---|
| $J$ | Factors | Properties |
| 2 | (7) | i, $S_1$ |
| 3 | (13) | i, dr |
| 4 | (23) | i, sd |
| 5 | (15)(7) | 3-2, dr |
| 6 | (103) | i |
| 7 | (203) | i |
| 8 | (155)(7) | 6-2, sd |
| 9 | (1003) | i,dr |
| 10 | (271)(13) | 7-3 |
| 11 | (1555)(7) | 9-2 |
| 12 | (57)(31)(15) | 5-4-3 |
| 13 | (651)(73) | 8-5 |
| 14 | (345)(51)(7) | 7-5-2 |
| 15 | (100003) | i |
| 16 | (551)(573) | 8-8, sd |
| 17 | (17523)(13)(7) | 12-3-2, dr |
| 18 | (22637)(45) | 13-5 |
| 19 | (277)(67)(23)(15) | 7-5-4-3 |
| 20 | (27221)(75)(7) | 13-5-2 |
| 21 | (50331)(253) | 14-7 |
| 22 | (20000003) | i |
| 23 | (34641)(515)(7) | 13-8-2 |
| 24 | (13456271)(13) | 21-3 |
| 25 | (7621)(435)(147) | 11-8-6 |
| 26 | (12515)(1275)(15)(7) | 12-9-3-2 |
| 27 | (75310753)(31) | 23-4 |
| 28 | (2000000003) | i |
| 29 | (1555555555)(7) | 27-2 |
| 30 | (10000000003) | i |
| 31 | (13144661)(211)(13) | 21-7-3 |
| 32 | (3417)(3543)(3435)(7) | 10-10-10-2, sd |
| 33 | (166311)(103437)(15) | 15-15-3, dr |

Table 2: Irreducible factors of $x^J + x + 1$ and their properties.

linear finite state machines such as LFSRs. The Jump Index was shown to exhibit interesting and useful properties and in particular it gives rise to the definition of the dual of a polynomial. It was also shown that all irreducible polynomials over $GF(2)$ form sets of six, three or two polynomials under the application of the dual and reciprocal operators. Expressions for the cardinalities of the sets of polynomials were derived and many properties regarding the periods and jump indices of the polynomials were given. The results obtained for the classes of self-dual, self-reciprocal and dual-reciprocal irreducible polynomials can effectively be used to generate such polynomials. The results given in Section 6 for composite polynomials show a different approach to the factorization of trinomials of the form $x^k + x + 1$.

Although not shown in great detail, it should be clear that the jumping LFSM construction can be used to implement clock controlled sequence generators in a very efficient way. Another advantage of the one-clock-multiple-step construction is it's inherent resistance against timing and power analysis attacks in hardware and software implementations.

# References


[1] E. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[2] L. Carlitz, Some Theorems on Irreducible Reciprocal Polynomials over a Finite Field, *J. reine angew. Math.*, no. 227(1967), pp. 212–220.

[3] W.G. Chambers, Clock-controlled Shift Registers in Binary Sequence Generators, *IEE Proceedings*, vol. 135, Part E, no. 1(1988).

[4] T.W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, North-Holland Mathematical Library, Elsevier, Amsterdam, 1998.

[5] Ecrypt Stream Cipher Project. `http://www.ecrypt.eu.org/stream/`

[6] European Patent No. EP 1038370, International Publication No. WO 9967918

[7] S. W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, Laguna Hills, 1982.

[8] K. Huber, Some Comments on Zech's Logarithms, *IEEE Transaction on Information Theory*, vol. 36, no. 4(1990), pp. 946–950.

[9] C.J.A. Jansen, Modern Stream Cipher Design: A new view on multiple clocking and irreducible polynomials, Actas de la VII Reunión Española sobre Criptología y Seguridad de la Información, *S. González, C. Martínez, Eds.* Tomo I, pp. 11–29, Oviedo (2002).

[10] C.J.A. Jansen, Stream Cipher Design: Make your LFSRs jump!, Workshop Record ECRYPT-State of the Art of Stream Ciphers, pp. 94–108, Brugge (2004).

[11] C.J.A. Jansen, Partitions of Polynomials: Stream Ciphers based on Jumping Shift Registers, Twenty-sixth Symposium on Information Theory in the Benelux, J. Cardinal et al, pp. 277–284, Brussels, Belgium (2005).

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Aplications 20, Cambridge University Press, Cambridge, 1997

[13] A. Menezes, P. Van Oorschot and S. Vanstone, *Handbook of Applied Cryptology*, CRC Press, 1996.

[14] H. Meyn and W. Götz, Self-reciprocal Polynomials over Finite Fields, *Séminaire Lotharingien de Combinatoire*, B2ld, Schloss Thurnau, Oberfranken, Germany, May 1989. (`http://www.mat.univie.ac.at/ slc/`)

[15] Micky. http://www.ecrypt.eu.org/stream/Micky.html

[16] The NESSIE Project. http://www.cryptonessie.org/

[17] W. Peterson, *Error Correcting Codes*, M.I.T. Press and Wiley & Sons, New york, 1961.

[18] Pomaranch. http://www.ecrypt.eu.org/stream/pomaranch.html

[19] B. J. M. Smeets, Some Results on Linear Recurring Sequences, *PhD-Thesis*, University of Lund, Sweden, 1987.