

On Primitive Polynomials over $GF(2)$ the Duals of which are also Primitive

Yuri Borissov, Nickolai Manev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G.Bonchev, 1113 Sofia
Bulgaria
yborisov,nlmanev@moi.math.bas.bg

Svetla Nikova
Dept. Electrical Engineering - COSIC
Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, 3001 Leuven
Belgium
svetla.nikova@esat.kuleuven.ac.be

Abstract

In this paper we consider primitive polynomials over $GF(2)$ the duals of which are also primitive and prove some estimates on the number of such polynomials of an arbitrary prime degree p and of degree pq for different prime numbers p and q .

1 Introduction

A new way of constructing binary cascade clock-controlled LFSR sequence generators as building blocks for stream ciphers - the so called jump-controlled sequence generators have been presented in [3, 4]. The motivation behind this construction is that previously known ways of cascading clock-controlled FSRs suffer a worse efficiency of multiple clocking (i.e., FSRs step through their state space one or more times before using the corresponding output bit), which generally results in a decreased rate of sequence generation, rendering it less attractive for high speed implementation. In the proposed design this shortcoming is avoided by finding an efficient way to let an autonomous LFSM (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. This construction has also a nice mathematical background - a special property of irreducible polynomials over $GF(2)$, the so called Jump Index.

By changing the transition matrix of an autonomous LFSM from \mathbf{A} into $\mathbf{A} + \mathbf{I}$, (\mathbf{I} is the identity matrix) effectively J steps are made through the state space of the original LFSM regardless of the starting non-zero state. This gives rise to the following definition.

Definition 1 [4] *Let $f(x)$ be an irreducible polynomial over $GF(2)$. If $x^J \equiv x + 1 \pmod{f(x)}$ for some positive 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 $x^J \equiv x + 1 \pmod{f(x)}$ for some J . This can be formulated also in terms of roots of $f(x)$, i.e. if α is a root of $f(x)$ with jump index J then the equation $\alpha^J = \alpha + 1$ holds in the splitting field $GF(2^n)$ of $f(x)$.

Note also that for primitive polynomials (i.e. irreducible polynomials of maximal order) the jump index always exists since their roots are primitive elements of $GF(2^n)$, $n = \deg f$.

Let $f^\perp(x)$ denotes the characteristic polynomial of the modified transition matrix. It follows that

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

and leads to the following definition.

Definition 2 [4] *The dual of an irreducible polynomial $f(x)$ over $GF(2)$, denoted by $f^\perp(x)$ is defined as $f(x+1)$.*

It is easy to see that $f(x)$ is an irreducible polynomial if and only if its dual $f^\perp(x)$ is irreducible. However the duality operator does not necessarily preserve being primitive. The jump index of $f^\perp(x)$ does not always exist too. *Order* of $f(x)$, denoted by $ord(f)$, is the minimum integer m , such that $f|(x^m+1)$. (Often order is also called period.) According to Theorem 2 from [4] the jump index J^\perp of $f^\perp(x)$ only exists if the jump index J of the original polynomial $f(x)$ is relatively prime with the order of $f(x)$. In this case $J^\perp = J^{-1}ord(f)$.

An irreducible polynomial f is called *self-dual* if and only if $f^\perp = f$. Dodunekov has given in [2] a very elegant proof of the existence of self-dual polynomials over $GF(q)$, q - prime number, for some infinite series. Note also that any self-dual polynomial over $GF(2)$ possesses a jump index. For more details about properties of self-dual polynomials we refer to [4].

The recently proposed stream ciphers Pomaranch [5] Mickey and Mickey-128 [6, 7] based on jumping FSRs suggest using primitive polynomials such that their duals are also primitive. In fact, this is necessary in order to provide maximal period and sufficient to ensure large linear complexity of the generated keystream sequence. In this paper we investigate when such polynomials exist. In particular, we prove the existence of such polynomials of prime degrees and of degrees which are product of two different prime numbers.

2 Conditions for Existence of Primitive Polynomials of degree n , the Duals of which are also Primitive

Before we prove the first proposition, we recall some facts about irreducible polynomials (see e.g. [1]). The number of irreducible polynomials over $GF(2)$ of degree n is given by

$$\psi_2(n) = \frac{1}{n} \sum_{d|n} 2^d \mu\left(\frac{n}{d}\right), \quad (1)$$

where μ is the well known Möbius function. While the number of primitive polynomials of degree n is given by

$$\lambda_2(n) = \frac{\Phi(2^n - 1)}{n}, \quad (2)$$

where Φ is the Euler function (i.e. $\Phi(N)$ is the number of positive integers smaller than N and relatively prime with N). Since every primitive polynomial is irreducible clearly we have that $\lambda_2(n) \leq \psi_2(n)$. We also make use of the following upper bound $\psi_2(n) \leq (2^n - 2)/n$, which is tight when n is a prime number.

Proposition 3 *If $\lambda_2(n) > \frac{1}{2}\psi_2(n)$ then there exist at least $2\lambda_2(n) - \psi_2(n)$ primitive polynomials of degree n such that their duals are primitive too.*

Proof. Let A be the set of primitive polynomials of degree n and B is the set of irreducible polynomials, which are obtained by the substitution $x \mapsto x+1$ in some polynomial from A . Since when f and g are different polynomials from A their duals f^\perp and g^\perp are also different, the set A has the same cardinality as the set B . By the

equation $|A \cap B| = |A| + |B| - |A \cup B|$ and because $|A \cup B|$ is a subset of the set of irreducible polynomials of degree n , it follows that $|A \cap B| \geq 2\lambda_2(n) - \psi_2(n) > 0$. This completes the proof.

□

According to the table with the values of λ_2 and ψ_2 for $n = 2 \dots 24$ in [1, p.40], the only values of n for which the assumptions of Proposition 3 are not satisfied are $n = 12$ and $n = 20$. By computer simulations we obtained the following results given in Table 1 below.

Table 1: Values of σ_2 , λ_2 , ψ_2

n	σ_2	λ_2	ψ_2
2	1	1	1
3	2	2	2
4	1	2	3
5	6	6	6
6	3	6	9
7	18	18	18
8	9	16	30
9	42	48	56
10	35	60	99
11	166	176	186
12	55	144	335
13	630	630	630
14	486	756	1161
15	1486	1800	2182
16	1011	2048	4080

In this table $\sigma_2(n)$ denotes the number of primitive polynomials of degree n the duals of which are primitive too. Note that when $M_p = 2^p - 1$ is Mersenne prime number any irreducible polynomial of degree p is primitive and this is the reason why $\sigma_2(p) = \lambda_2(p)$ for $p = 2, 3, 5, 7$ and 13 .

3 Conditions for Existence of Primitive Polynomials of degree p and pq , the Duals of which are also Primitive

In this section we will show that the assumptions of Proposition 3 are satisfied for all $n = p$ and $n = 2p$, where p is an arbitrary prime integer. We will also consider the case $n = pq$, where p and q are odd prime numbers.

We make use of the following auxiliary result which can be found for example in [8, Ch.6, exc.1].

Lemma 4 *Let p be an odd prime number and a be an integer, $a > 1$. Then*

- (a) All odd prime divisors of $a^p - 1$ either divide $a - 1$ or are of the form $2pk + 1$, where k is a positive integer;
- (b) All odd prime divisors of $a^p + 1$ either divide $a + 1$ or are of the form $2pk + 1$, where k is a positive integer.

Proposition 5 For any prime $p \geq p_0$, we have:

$$\lambda_2(p) \geq E(p_0)\psi_2(p), \quad (3)$$

where $E(n) = e^{-\frac{1}{2\log_2(2n+1)}}$ for a positive integer n and e is the base of natural logarithms.

Proof. By using (1) we have $\psi_2(p) = \frac{(2^p-2)}{p}$. Therefore (3) is equivalent to $\Phi(2^p - 1) > E(p_0)(2^p - 2)$. Denote by $M_p = 2^p - 1$. We will prove that $\frac{\Phi(M_p)}{M_p} > E(p_0)$. Let q_1, q_2, \dots, q_s be the different prime factors of M_p , i.e., $M_p = \prod_{i=1}^s q_i^{\alpha_i}$ and $\alpha_i \geq 1, i = 1, 2, \dots, s$. Using a well known fact from Number Theory and Lemma 1 (when $a = 2$) we obtain:

$$\frac{\Phi(M_p)}{M_p} = \prod_{i=1}^s \left(1 - \frac{1}{q_i}\right) > \left(1 - \frac{1}{2p+1}\right)^s$$

Denote by $t_0 = \log_2(2p_0 + 1)$. We will show that $s < \frac{p}{t_0}$. Indeed, $2^p > M_p = \prod_{i=1}^s q_i^{\alpha_i} > (2p+1)^{\alpha_1+\alpha_2+\dots+\alpha_s} \geq (2p+1)^s > (2^{\log_2(2p_0+1)})^s = 2^{t_0 s}$ and therefore $s < p/t_0$. So,

$$\frac{\Phi(M_p)}{M_p} > \left(1 - \frac{1}{2p+1}\right)^{\frac{p}{t_0}} = \left(1 - \frac{1}{2p+1}\right)^{\frac{2p}{2t_0}} = \left[\frac{1}{\left(1 + \frac{1}{2p}\right)^{2p}}\right]^{\frac{1}{2t_0}} = a_p$$

It is well known that the sequence $\{(1 + \frac{1}{n})^n\}$ is increasing and thus $\{a_p\}$ is decreasing, its limit (lower bound particularly) is $E(p_0) = e^{-\frac{1}{2t_0}}$, where e is the base of natural logarithms. □

Corollary 6 For any prime number p there exists a primitive polynomial of degree p such that its dual is primitive too.

The proof follows from the inequalities $E(2) > e^{-\frac{1}{4}} > \frac{1}{2}$ and Proposition 3.

Remark 7 Since $\lim_{p_0 \rightarrow \infty} E(p_0) = 1$ it follows that almost all irreducible polynomials of sufficient large prime degree are primitive.

Now consider the case of $n = 2p$, where p is an arbitrary prime number greater than 2. Let $p > p_0$. We will show that

$$\frac{\Phi(2^{2p} - 1)}{2^{2p} - 1} > \frac{2}{3}E^2(p_0),$$

where $E(p_0)$ is defined in Proposition 5.

In the proof of Proposition 5 we have already shown that $\frac{\Phi(2^p-1)}{2^p-1} > E(p_0)$. So,

$$\frac{\Phi(2^{2p} - 1)}{2^{2p} - 1} = \frac{\Phi(2^p - 1)}{2^p - 1} \frac{\Phi(2^p + 1)}{2^p + 1} > E(p_0) \frac{\Phi(2^p + 1)}{2^p + 1}.$$

Let $3, q_2, \dots, q_{s+1}$ be the different prime factors of $2^p + 1$, i.e., $2^p + 1 = 3^{\beta_1} \cdot q_2^{\beta_2} \cdots q_{s+1}^{\beta_{s+1}}$, $\beta_i \geq 1$, $i = 1, 2, \dots, s+1$. Proceeding as in the proof of Proposition 5 and using part (b) of Lemma 4, we obtain

$$\frac{\Phi(2^p + 1)}{2^p + 1} = \left(1 - \frac{1}{3}\right) \prod_{i=2}^{s+1} \left(1 - \frac{1}{q_i}\right) > \frac{2}{3} \left(1 - \frac{1}{2^p + 1}\right)^s,$$

where it is easy to see that $s < \frac{p}{\log_2(2p_0+1)} = \frac{p}{t_0}$. Therefore $\frac{\Phi(2^p+1)}{2^p+1} > \frac{2}{3} \left(1 - \frac{1}{2^p+1}\right)^{\frac{p}{t_0}} > \frac{2}{3} E(p_0)$ and finally $\frac{\Phi(2^{2^p-1})}{2^{2^p-1}} > \frac{2}{3} E^2(p_0)$. Thus the inequality $\lambda_2(2p) > \frac{2}{3} E^2(p_0) \psi_2(2p)$ holds. To prove that $\lambda_2(2p) > \frac{1}{2} \psi_2(2p)$ we use the fact that $\frac{2}{3} E^2(8) > \frac{1}{2}$ and the cases when $p = 2, 3, 5$ and 7 are considered separately. Therefore the following statement holds: For any prime p there exists primitive polynomial of degree $2p$ the dual of which is also primitive.

Finally, we will consider the case $n = pq$, where p and q are odd prime numbers. By Lemma 4 all prime factors of $M_{pq} = 2^{pq} - 1$ are either of the form $2pk + 1$ or of the form $2qk + 1$, where k and l are positive integers. Let $d = 2pk + 1$ is a prime factor of M_{pq} such that $GCD(k, q) = 1$. We will show that d divides M_p . Indeed, we have $p = GCD(pq, d - 1)$. So, there exist positive integers u and v : $p = upq - v(d - 1)$ and hence: $2^p \equiv 2^{p+u(d-1)} = 2^{upq} = (2^{pq})^u \equiv 1 \pmod{d}$ i.e. d divides M_p . The first equality above follows from the little Fermat's theorem. Thus we have:

$$\begin{aligned} \frac{\Phi(M_{pq})}{M_{pq}} &= \prod_{d|M_p} \left(1 - \frac{1}{d}\right) \prod_{d|M_q} \left(1 - \frac{1}{d}\right) \prod_{d=2pqk+1} \left(1 - \frac{1}{d}\right) \\ &\geq \left(1 - \frac{1}{2p+1}\right)^{s_p} \left(1 - \frac{1}{2q+1}\right)^{s_q} \left(1 - \frac{1}{2pq+1}\right)^{s_{pq}}, \end{aligned}$$

where s_p and s_q are the numbers of prime divisors d of M_p and M_q respectively, and s_{pq} is the number of the remaining prime divisors d of M_{pq} (which divide neither M_p nor M_q) and are obligatory of the form $2pqk + 1$.

Let $p \geq p_0$ and $q \geq q_0$ where p_0 and q_0 are some constants. It is easy to see that $s_p < \frac{p}{\log_2(2p_0+1)}$, $s_q < \frac{q}{\log_2(2q_0+1)}$ and $s_{pq} < \frac{pq}{\log_2(2p_0q_0+1)}$ and therefore we have:

$$\frac{\Phi(M_{pq})}{M_{pq}} > E(p_0)E(q_0)E(p_0q_0) \geq E(3)E(5)E(15) > e^{-\frac{1}{2}} > \frac{1}{2}.$$

4 Conclusions

In this paper we consider primitive polynomials over $GF(2)$ the duals of which are also primitive and prove some lower bounds on number of such polynomials of degree p and of degree pq for two different prime numbers p and q . Our investigations show that in some sense the set of irreducible polynomials of sufficiently large prime degrees is one of the richest set containing such type of polynomials.

Acknowledgment

The authors would like to thank Cees Jansen for the valuable comments and discussions.

References

- [1] S.W. Golomb, "Shift register Sequences", Aegen Park press, 1982
- [2] S. M. Dodunekov, "Essentially different irreducible polynomials over finite fields", Ann. University of Sofia, Faculty of Mathematics and Mechanics 1971, 66, pp. 169-175.
- [3] 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.
- [4] C. J. A. Jansen, "Stream cipher design based on jumping finite state mashines", IACR e-Print Archive 2005/267.
- [5] C. J. A. Jansen, A. Kolosha, "POMARANCH, eSTREAM - the ECRYPT Stream Cipher Project", <http://www.ecrypt.eu.org/stream/pomaranch.html>
- [6] S. Babbage, M. Dodd, "MICKEY, eSTREAM - the ECRYPT Stream Cipher Project", <http://www.ecrypt.eu.org/stream/mickey.html>
- [7] S. Babbage, M. Dodd, "MICKEY-128, eSTREAM - the ECRYPT Stream Cipher Project", <http://www.ecrypt.eu.org/stream/mickey128.html>
- [8] I. M. Vinogradov, "Basics of Number Theory", Moscow 1972, Publishing House Nauka, in russian.