Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 341 (2005) 311–343
Theoretical Computer Science
www.elsevier.com/locate/tcs

Results on multiples of primitive polynomials and their products over GF(2)☆

Subhamoy Maitra[a,*], Kishan Chand Gupta[b], Ayineedi Venkateswarlu[c]

[a] *Applied Statistics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700 108, India*
[b] *Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*
[c] *Temasek Laboratories, National University of Singapore, 5 Sports Drive 2, Singapore-117508, Republic of Singapore*

Received 14 July 2003; received in revised form 14 February 2005; accepted 20 April 2005

Communicated by A. Fiat

Abstract

Linear feedback shift registers (LFSR) are important building blocks in stream cipher cryptosystems. To be cryptographically secure, the connection polynomials of the LFSRs need to be primitive over GF(2). Moreover, the polynomials should have high weight and they should not have sparse multiples at low or moderate degree. Here we provide results on *t*-nomial multiples of primitive polynomials and their products. We present results for counting *t*-nomial multiples and also analyse the statistical distribution of their degrees. The results in this paper helps in deciding what kind of primitive polynomial should be chosen and which should be discarded in terms of cryptographic applications. Further the results involve important theoretical identities in terms of *t*-nomial multiples which were not known earlier.

Keywords: Cryptology; Primitive polynomials; Product of primitive polynomials; Stream cipher; Sparse multiples; Statistical distribution

☆ This paper is based on the conference papers [4,5,14,19].

* Corresponding author.
E-mail addresses: subho@isical.ac.in (S. Maitra), kgupta@math.uwaterloo.ca (K.C. Gupta), tslav@nus.edu.sg (A. Venkateswarlu).

0304-3975/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2005.04.011

1. Introduction

Linear feedback shift register (LFSR) is one of the most important building blocks in stream ciphers. In almost all the well-known stream cipher designs, LFSRs play a very important role. The connection polynomials of the LFSRs are usually polynomials over GF(2). The relationship between a polynomial and the connection pattern of the corresponding LFSR is explained in [3,2,16]. It is important to note that towards resisting cryptanalytic attacks, the LFSRs should be designed keeping the following points in mind [15,1].

(1) The connection polynomial must be primitive over GF(2).
(2) The weight of the connection polynomial must be high.
(3) There should not be any sparse multiple of moderate degree for the connection polynomial.

Note that throughout this paper we only consider polynomials over GF(2). We always assume $d \geqslant 2$ for a primitive polynomial of degree d, i.e., $(x + 1)$ is not considered as a primitive polynomial in this paper. It is known that for a primitive polynomial $f(x)$ of degree d and any multiple $g(x)$ of $f(x)$, the recurrence relation (of the LFSR whose connection polynomial is $f(x)$) induced by $f(x)$ will also be satisfied by $g(x)$. In particular if $g(x)$ is of moderate degree and with low weight, then one can very well exploit the attack proposed in [15] by choosing the recurrence relation induced by $g(x)$. Whatever be the weight of the primitive polynomial $f(x)$ (it does not matter whether it is of high or low weight as we have a low weight multiple), it is possible to attack the system using $g(x)$. Note that we are interested in sparse multiples $g(x)$ with constant term 1, i.e., $g(0) = 1$. The reason is if $g(0) = 0$, then $g(x)$ can be written as $x^i h(x)$. This $h(x)$ satisfies the same recurrence relation as $g(x)$ and also of lower degree. With this context we analyse the sparse multiples (with constant term 1) of primitive polynomials. Similarly, it is also important in some situations to find out sparse multiples of product of primitive polynomials [1]. We also analyse that case in detail.

The main issue is, one should not use a primitive polynomial which by itself is of low weight or which has a sparse multiple at lower degree. We discuss this in Section 3. In this direction, we identify a class of primitive polynomials having sparse multiples at a very low degree. If $f(x)$ is a primitive t-nomial of degree d, then there exists primitive polynomial of degree d with a t-nomial multiple of degree sd where $\gcd(s, 2^d - 1) = 1$. Using this we show that there are trinomial multiples of degree sd (which is low when s is small) for a large class of primitive polynomials of degree d. These primitive polynomials should not be used in stream cipher systems.

Given a primitive polynomial $f(x)$ of degree d, we will present a recurrence formula for the number of t-nomial multiples (with constant term 1) of $f(x)$ having degree at most $2^d - 2$. We denote this number by $N_{d,t}$ and it can be seen that

$$N_{d,t} = \frac{\binom{2^d-2}{t-2} - N_{d,t-1} - \frac{t-1}{t-2}(2^d - t + 1)N_{d,t-2}}{t-1},$$

with initial conditions $N_{d,2} = N_{d,1} = 0$. Section 4 discusses this result and related issues. Note that the count in more general setting has been discussed in [9]. Further the count