SELF-RECIPROCAL IRREDUCIBLE PENTANOMIALS OVER $\mathbb{F}_2$

OMRAN AHMADI

Abstract. Joseph Yucas and Gary Mullen conjectured that there is no self-reciprocal irreducible pentanomial of degree n over $\mathbb{F}_2$ if n is divisible by 6. In this note we prove this conjecture for the case $n \equiv 0 \pmod{12}$, and disprove the conjecture for the case $n \equiv 6 \pmod{12}$.

1. Introduction

Let $f(x)$ be a polynomial in $\mathbb{F}_2[x]$ whose constant term is nonzero. Then the reciprocal of $f(x)$ is defined to be $f^*(x) = x^n f(1/x)$. If $f(x)$ is irreducible over $\mathbb{F}_2$, then so is $f^*(x)$. If $f^*(x) = f(x)$, then $f(x)$ is called a self-reciprocal polynomial. The weight of $f(x)$ is the number of the nonzero coefficients of it. The order of an irreducible polynomial $f(x)$ over $\mathbb{F}_2$ is the smallest integer e such that $f(x)|x^e - 1$ in $\mathbb{F}_2[x]$.

Let $f(x)$ be a self-reciprocal irreducible polynomial over $\mathbb{F}_2$ of degree $n > 1$. Then f is of even degree since α^{-1} is a root of f whenever α is. Thus $n = 2m$ for some m. Also if f is a pentanomial, i.e. has weight 5, then $f(x) = x^{2m} + x^{2m-j} + x^m + x^j + 1$ for some $j < n$.

Yucas and Mullen [2] conjectured that there is no self-reciprocal irreducible pentanomial of degree n over $\mathbb{F}_2$ if n is divisible by 6. In this note we show that their claim is true when n is divisible by 12 and it is not true when $n \equiv 6 \pmod{12}$. The main result of this note is the following:

Theorem 1. There is no self-reciprocal irreducible pentanomial of degree n over $\mathbb{F}_2$ if n is divisible by 12.

2. Proof of the Theorem

Our proof is based on the two following results.

Theorem 2. [2, Corollary 5] Let f be a self-reciprocal irreducible polynomial of degree $2m$ and order e over $\mathbb{F}_2$, and let D_m be the set of all positive divisors of $2^m + 1$ which do not divide $2^k + 1$ for $0 \leq k < m$. Then $e \in D_m$.

An immediate corollary is that if m is an even number then $2^m + 1$ is not divisible by 3 and thus 3 does not divide any element of D_m.

Date: February 16, 2005.

Key words and phrases. Finite Fields, Self-Reciprocal Irreducible Polynomials.

Theorem 3. [1, Theorem 3.9] Let $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n and order e and let t be a positive integer. Then $f(x^t)$ is irreducible over $\mathbb{F}_2$ if and only if

(i) $\gcd(t, \frac{2^n-1}{e}) = 1$ and
(ii) each prime divisor of t divides e.

Proof of Theorem 1: Let $f(x) = x^{2m} + x^{2m-j} + x^m + x^j + 1$ be a self-reciprocal pentanomial over $\mathbb{F}_2$ where $6|m$ and let $m = 3^s 2p$ and $j = 3^r q$ where p and q are not divisible by 3. We have two cases: either $s \leq r$ or $s > r$. First assume $s > r$ and let $m_1 = 3^{s-r}2p$ and $g(x) = x^{2m_1} + x^{2m_1-q} + x^{m_1} + x^q + 1$. Since $s > r$, m_1 is divisible by 3 and thus q and $2m_1 - q$ are nonzero and different modulo 3. Hence $g(x) \equiv x^2 + x + 1 \pmod{x^3+1}$, and so g is reducible. Since $f(x) = g(x^{3^r})$, it follows that f is also reducible. Now let $s \leq r$, $j_1 = 3^{r-s}q$ and $g(x) = x^{4p} + x^{4p-j_1} + x^{2p} + x^{j_1} + 1$. Notice that $f = g(x^{3^s})$. If g is reducible, then so is f and we are done. Thus assume g is irreducible and is of order e. Now applying Theorem 3, if $f = g(x^{3^s})$ is irreducible then e must be divisible by 3. But by the comments made after Theorem 2 we see that 3 does not divide e and thus f is reducible. $\square$

In the above we proved that there is no self-reciprocal irreducible pentanomial of degree n if 12 divides n. But this is not the case when n is divisible by 6 and not by 12. For example, since $f(x) = x^{10} + x^9 + x^5 + x + 1$ is a self-reciprocal irreducible pentanomial of order 33, Theorems 2 and 3 imply that $f(x^{3^s}) = x^{3^s 10} + x^{3^s 9} + x^{3^s 5} + x^{3^s} + 1$ is a self-reciprocal irreducible pentanomial of degree $3^s 10 \equiv 6 \pmod{12}$ for every positive integer s.

References

[1] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian *Applications of Finite Fields*, Kluwer, 1993.

[2] J. L. Yucas and G. L. Mullen, "Self-Reciprocal Irreducible Polynomials Over Finite Fields", *Designs, Codes and Cryptography*, 33 (2004), 275-281.

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: oahmadid@math.uwaterloo.ca