Finite Fields and Their Applications 47 (2017) 242–255

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Counting perfect polynomials

U. Caner Cengiz [a], Paul Pollack [b,*], Enrique Treviño [a]

[a] *Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045, USA*
[b] *Department of Mathematics, University of Georgia, Athens, GA 30602, USA*

ARTICLE INFO

Article history:
Received 11 May 2017
Accepted 31 May 2017
Available online xxxx
Communicated by Gary L. Mullen

MSC:
primary 11T55
secondary 11T06

Keywords:
Perfect polynomial
One-ring
Sum-of-divisors

ABSTRACT

Let $A \in \mathbf{F}_2[T]$. We say A is *perfect* if A coincides with the sum of all of its divisors in $\mathbf{F}_2[T]$. We prove that the number of perfect polynomials A with $|A| \le x$ is $O_\epsilon(x^{1/12+\epsilon})$ for all $\epsilon > 0$, where $|A| = 2^{\deg A}$. We also prove that every perfect polynomial A with $1 < |A| \le 1.6 \times 10^{60}$ is divisible by T or $T+1$; that is, there are no small "odd" perfect polynomials.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

For each nonzero $A \in \mathbf{F}_2[T]$, let $\sigma(A) = \sum_{D|A} D$, where D runs over all of the divisors of A in $\mathbf{F}_2[T]$. We call A perfect if $\sigma(A) = A$. For example, $T(T+1)$ is perfect, because

$$\sigma(T(T+1)) = 1 + T + (T+1) + T(T+1) = T(T+1).$$

[*] Corresponding author.
E-mail addresses: cengizuc@mx.lakeforest.edu (U.C. Cengiz), pollack@uga.edu (P. Pollack), trevino@lakeforest.edu (E. Treviño).

http://dx.doi.org/10.1016/j.ffa.2017.05.006
1071-5797/© 2017 Elsevier Inc. All rights reserved.

The study of perfect polynomials was initiated by Canaday [1] in his doctoral work under Leonard Carlitz.[1] In the case when A splits over $\mathbf{F}_2$ — meaning that all of its roots in $\overline{\mathbf{F}_2}$ lie in $\mathbf{F}_2$ — Canaday discovered the following concrete characterization of when A is perfect:

Theorem A. *If A splits over $\mathbf{F}_2$, then A is perfect if and only if $A = (T(T+1))^{2^n-1}$ for some nonnegative integer n.*

For non-splitting perfect polynomials the situation is less clear. Canaday discovered 11 examples whose irreducible factorizations are exhibited in Table 1.

One immediately striking feature of Canaday's list is that all the polynomials appearing have a root in $\mathbf{F}_2$. Are there perfect polynomials ($\neq 1$) without such a root? Almost 80 years later we can do no better than echo Canaday's assessment: "it seems plausible that none of this type exist, but this is not proved." Let us agree to call A *even* if A has a root in $\mathbf{F}_2$ and to call A *odd* otherwise.[2] Then, in analogy with the integer case, Canaday's conjecture becomes:

Canaday's conjecture. *There are no odd perfect polynomials, other than $A = 1$.*

From now on, when we refer to an *odd perfect polynomial*, we will mean an odd perfect polynomial $\neq 1$. With this convention, Canaday's conjecture is that there are no odd perfect polynomials.

Various constraints are known on the multiplicative structure of any odd perfect polynomial. The following basic result can be considered the analogue of the classical Euler-form for odd perfect numbers:

Theorem B. *An odd perfect polynomial is a square.*

The proof of Theorem B is straightforward: if P^e is a unitary divisor of some odd perfect polynomial,[3] then both P and $\sigma(P^e)$ are odd. In particular, both P and $\sigma(P^e) = 1 + P + \cdots + P^e$ have constant term 1; this implies that e is even.

In [5], Gallardo and Rahavandrainy proved that an odd perfect polynomial has at least five distinct irreducible factors. In [3], they showed that an odd perfect polynomial that is a product of squares of distinct irreducibles has at least 10 distinct irreducible factors. Therefore, using Theorem B, we have:

Theorem C. *If A is an odd perfect polynomial, then the number of irreducible factors of A, counted with multiplicity, is at least 12.*

[1] Canaday did not name these polynomials *perfect*. He used the term *one-ring* for a perfect polynomial. The term *perfect polynomial* was first used by Beard, O'Connell and West in [7].

[2] These terms originated in several papers of Gallardo and Rahavandrainy (see [3,4]).

[3] Recall that A is said to be a *unitary divisor* of M if $M = AB$ with $\gcd(A, B) = 1$; in this case, we also write $A \parallel M$.

Download English Version:

https://daneshyari.com/en/article/5771621

Download Persian Version:

https://daneshyari.com/article/5771621

Daneshyari.com