On the Number of Zero Trace Elements in Polynomial Bases for $\mathbb{F}_{2^n}$

Igor E. SHPARLINSKI

Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Recibido: 16 de Junio de 2004
Aceptado: 8 de Julio de 2004

ABSTRACT

Let $\mathbb{F}_q$ denotes the finite field of q elements. O. Ahmadi and A. Menezes have recently considered the question about the possible number of elements with zero trace in polynomial bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Here we show that the Weil bound implies that there is such a basis with $n + O(\log n)$ zero-trace elements.

Key words: bases of finite fields, Weil bound.

2000 Mathematics Subject Classification: 11T30, 11T71, 9460.

1. Introduction

Let $\mathbb{F}_q$ denotes the finite field of q elements, and let

$$\mathrm{Tr}(z) = \sum_{j=0}^{n-1} z^{2^j} \tag{1}$$

denote the trace of $z \in \mathbb{F}_{2^n}$ in $\mathbb{F}_2$.

We also denote by $\mathcal{A}_n$ the set of roots α of all irreducible polynomials of degree n over $\mathbb{F}_2$, thus $\mathbb{F}_{2^n} = \mathbb{F}_2(\alpha)$ for every $\alpha \in \mathcal{A}_n$.

For $\alpha \in \mathcal{A}_n$, we denote by $N(\alpha)$ the number of zero trace elements in the polynomial basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

During the preparation of this paper, the author was supported in part by ARC grant DP0211459.

The question about the spectrum of possible values of $N(\alpha)$, when α runs through the set $\mathcal{A}_n$, has recently been introduced by O. Ahmadi and A. Menezes [1]. In particular elements with small values of $n - N(\alpha)$ are useful for speeding up finite field arithmetic. It is shown in [1] that under the assumption of the existence of certain irreducible trinomials $N(\alpha)$ achieves its largest (and thus optimal from the computational point of view) value $N(\alpha) = n - 1$. One can also find several other results in [1], which show that other irreducible fewnomials also lead to almost optimal values of $N(\alpha)$. We however remark that, although the existence of such irreducible fewnomials has never been doubted in practice, there are no theoretical results which guarantee the existence of infinitely many of them. Thus it is interesting to get a rigorous bound on the largest possible value of $N(\alpha)$.

Here we show that the Weil bound implies that for any sufficiently large n there are elements $\alpha \in \mathcal{A}_n$ with $N(\alpha) = n + O(\log n)$ (hereafter, $\log m$ denotes the binary logarithm of $m > 0$). In fact, we show a more explicit statement.

Theorem 1.1. *For every $n \geq 21$, there exists $\alpha \in \mathcal{A}_n$ such that $N(\alpha) \geq n - \log n - 2$.*

For smaller values of n one can certainly use the numerical results from [1].

2. Preparation

We need several well known results from the theory of finite fields.

Lemma 2.1. *The bound*

$$|\#\mathcal{A}_n - 2^n| \leq 2^{n/2+1}$$

holds.

Proof. It is known, see [2, Theorem 3.25], that there are

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d}$$

irreducible polynomials of degree n over $\mathbb{F}_{2^n}$, where $\mu(d)$ is the Möbius function and the sum is taken over all positive integer divisors of n. Therefore

$$\left| I_n - \frac{2^n}{n} \right| \leq \left| \frac{1}{n} \sum_{\substack{d|n \\ d<n}} \mu(d) 2^{n/d} \right| \leq \frac{1}{n} \sum_{\substack{d|n \\ d<n}} 2^{n/d} \leq \frac{1}{n} \sum_{k \leq n/2} 2^k \leq \frac{2^{n/2+1}}{n}.$$

Since each polynomial contributes exactly n elements to $\mathcal{A}_n$ (and distinct polynomials contribute distinct elements) we have $\#\mathcal{A}_n = nI_n$ and the result follows. □

Lemma 2.2. *For any polynomial $g(X) \in \mathbb{F}_2[x]$ of odd degree k, the bound*

$$\left| \sum_{\alpha \in \mathcal{A}_n} (-1)^{\mathrm{Tr}(g(\alpha))} \right| \le (k+1)2^{n/2}$$

holds.

Proof. By Lemma 2.1, we have,

$$\left| \sum_{\alpha \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(g(\alpha))} - \sum_{\alpha \in \mathcal{A}_n} (-1)^{\mathrm{Tr}(g(\alpha))} \right| \le 2^n - \#\mathcal{A}_n \le 2^{n/2+1}.$$

By the Weil bound, see [2, Theorem 5.38],

$$\left| \sum_{\alpha \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(g(\alpha))} \right| \le (k-1)2^{n/2}$$

and the result follows. □

3. Proof of Theorem 1.1

For a positive integer $s \le n-1$ we denote by $T_{n,s}$ the number of $\alpha \in \mathcal{A}_n$ satisfying the system of equations

$$\mathrm{Tr}(\alpha^{2j-1}) = 0, \qquad j = 1, \ldots, s. \tag{2}$$

We have

$$T_{n,s} = \frac{1}{2^s} \sum_{\alpha \in \mathcal{A}_n} \sum_{a_1,\ldots,a_s=0}^{1} (-1)^{a_1 \mathrm{Tr}(\alpha) + a_2 \mathrm{Tr}(\alpha^3) + \cdots + a_s \mathrm{Tr}(\alpha^{2s-1})}.$$

Changing the order of summation, separating the term $\#\mathcal{A}_n/2^s$ corresponding to $a_1 = \cdots = a_s = 0$, and using Lemma 2.2 for the other $2^s - 1$ terms, we deduce

$$\left| T_{n,s} - \frac{\#\mathcal{A}_n}{2^s} \right| \le \frac{2^s - 1}{2^s}(2s+1)2^{n/2}.$$

Hence, by Lemma 2.1 we have

$$|T_{n,s} - 2^{n-s}| \le \frac{2^s - 1}{2^s}(2s+1)2^{n/2} + \frac{1}{2^s}2^{n/2+1} < (2s+1)2^{n/2}.$$

It is now easy to verify that $2^{n-s} \ge (2s+1)2^{n/2}$ for $s = n/2 - \lceil \log n \rceil$ and thus $T_{n,s} > 0$ for the above choice of s. We note that (1) implies that for any $z \in \mathbb{F}_{2^n}$ we have $\mathrm{Tr}(z) = \mathrm{Tr}(z^2)$. Thus, if $2s - 1 \ge (n-1)/2$ then $\mathrm{Tr}(\alpha^{2i}) = 0$ for every positive integer $i \le (n-1)/2 \le 2s-1$. Therefore

$$N(\alpha) \ge \lfloor (n-1)/2 \rfloor + s = n/2 + s - 1 \ge n - \log n - 2$$

for every α which satisfies (2). We also remark that for $n \ge 21$, we have $2s - 1 = 2(n/2 - \lceil \log n \rceil) - 1 = n - 2\lceil \log n \rceil - 1 \ge (n-1)/2$ and the result follows. □

Acknowledgements. The author would like to thank Omran Ahmadi and Alfred Menezes for several useful discussions and a patient and careful reading of the manuscript.

References

[1] O. Ahmadi and A. Menezes, *On the number of trace-one elements in polynomial bases for* $\mathbb{F}_{2^n}$, Des. Codes Cryptogr., to appear.

[2] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.