The Trace Spectra of Polynomial Bases for $\mathbb{F}_{2^n}$

Omran Ahmadi

Department of Combinatorics & Optimization
University of Waterloo, Canada
oahmadid@uwaterloo.ca

Abstract. In this paper we study the trace spectra of polynomial bases for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Shparlinski showed that there exists a polynomial basis having $O(\log n)$ elements of trace one. Here we show that for every $t \leq n$, there exists a polynomial basis having $t + O(\log n)$ elements of trace one. We also study consequences of our results to the existence of irreducible polynomials of certain weights.

Key words: Finite Fields, Polynomial Bases, Irreducible Polynomials.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the degree n extension field of $\mathbb{F}_2$. Then $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_2$. The element $\alpha = x$ is a root of f in $\mathbb{F}_{2^n}$, and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, called a polynomial basis. The trace of an element $z \in \mathbb{F}_{2^n}$ is defined to be $\mathrm{Tr}(z) = \sum_{i=0}^{n-1} z^{2^i}$.

Ahmadi and Menezes [1] studied the possible spectra of the number of trace-zero elements of a polynomial basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. They were interested in the problem because a polynomial basis having more elements of trace zero results in faster and simpler implementation of the trace function. This is beneficial, for example, when halving a point on an elliptic curve over $\mathbb{F}_{2^n}$ (see [4, 7, 9]), or when generating pseudorandom sequences using elliptic curves [5] or the Welch-Gong transformation sequence generator [6]. They showed that if $f(x)$ is a trinomial, having three non-zero terms, or a pentanomial, having five non-zero terms, with some additional properties (e.g. $f(x) = x^n + x^m + 1$ with $m < n/2$ or $f(x) = x^n + x^{m_1} + x^{m_2} + x^{m_3} + 1$ with $n/2 > m_1 > m_2 > m_3$), then one has a polynomial basis for which most of the elements have trace zero. We note that trinomials do not exist for some values of n and although there is evidence for the existence of pentanomials, there are no theoretical results proving the existence of infinitely many of them. Based on some experimental evidence, Ahmadi and Menezes [1] conjectured that for $n \geq 7$ and $t \in [1, n]$ when n is odd and $t \in [1, n-1]$ when n is even there exists a polynomial basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ having exactly t elements of trace one.

Using Weil's bound for exponential sums, Shparlinski [12] showed that for every n there exists a polynomial basis having at most $\log n + 1$ elements of trace one. In this paper adopting his method we generalize this result and prove that for every t, $1 \leq t \leq n$, there exists a polynomial basis having $t + O(\log n)$ trace-one elements.

There is interest in the weight pattern of irreducible polynomials over $\mathbb{F}_2$ (for example see [2, 10, 11, 13]). In [1] with the assumption of the existence of the aforementioned fewnomials of degree n over $\mathbb{F}_2$, the possible trace spectrum of the elements of polynomial bases was studied. Another interesting direction one can pursue is proving the existence of polynomial bases having special trace spectrum and from that deducing the existence of irreducible polynomials of degree n over $\mathbb{F}_2$ of certain weights. We present one result of this flavor.

The paper is organized as follows. The results about the trace spectra of polynomial bases are presented in §2. In §3 we present our result about the existence of irreducible polynomials of degree n over $\mathbb{F}_2$ of weight roughly $n/2$ which have special structure.

2 The traces of the elements of polynomial bases

As in [12] we denote by $\mathcal{A}_n$ the set of roots α of irreducible polynomials of degree n over $\mathbb{F}_2$. The proofs of the following lemmas can be found in [12].

Lemma 1 For $\mathcal{A}_n$ we have

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

Lemma 2 If $g(x) \in \mathbb{F}_2[x]$ is of odd degree k, then

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

For every k we denote by J_k the set of the positive odd numbers not greater than k. The following theorem is about the possible trace spectra of polynomial bases.

Theorem 3 Let J_{n-1} be as defined above and suppose $K \subseteq J_{n-1}$ such that $\#K \leq n/2 - \log n - 1$. Let $L \subseteq K$. Then there exists $\alpha \in \mathcal{A}_n$ such that $\mathrm{Tr}(\alpha^k) = 1$ if $k \in L$ and $\mathrm{Tr}(\alpha^k) = 0$ if $k \in K \setminus L$.

Proof. Let $T_{K,L}$ be the number of $\alpha \in \mathcal{A}_n$ such that $\mathrm{Tr}(\alpha^k) = 1$ if $k \in L$ and $\mathrm{Tr}(\alpha^k) = 0$ if $k \in K \setminus L$, and let $\#K = m$. We define $b_k = 1$ if $k \in L$ and $b_k = 0$ if $k \in K \setminus L$. Then

$$T_{K,L} = \frac{1}{2^m} \sum_{\alpha\in\mathcal{A}_n} \sum_{\substack{a_k=0\\k\in K}}^{1} (-1)^{\sum_{k\in K} a_k(\mathrm{Tr}(\alpha^k)+b_k)}. \tag{3}$$

The middle sum is taken over all the $\{0,1\}$ m-tuples whose elements are indexed by the elements of K. Now if we change the order of summations in the above equation and separate the term corresponding to $a_k = 0$ for $k \in K$, namely $\#\mathcal{A}_n/2^m$, then using Lemma 2 for the other terms we have

$$|T_{K,L} - \frac{\#\mathcal{A}_n}{2^m}| \leq \frac{2^m - 1}{2^m} n 2^{n/2}. \tag{4}$$

Using Lemma 1 we get

$$|T_{K,L} - 2^{n-m}| \leq n 2^{n/2}. \tag{5}$$

Now using the fact that $m \leq n/2 - \log n - 1$ we have $2^{n-m} > n2^{n/2}$. This implies $T_{K,L} > 0$ and the proof is complete. □

We can derive Shparlinski's result [12] from Theorem 3 as follows. Let $K \subseteq J_{n-1}$ consist of the odd numbers less than or equal to $n - 2\log n - 2$ and $L = \emptyset$. Then there exists $\alpha \in \mathcal{A}_n$ for which $\mathrm{Tr}(\alpha^k) = 0$ for all $k \in K$. Using the fact that $\mathrm{Tr}(z^2) = \mathrm{Tr}(z)$ for every $z \in \mathbb{F}_{2^n}$ we see that $\mathrm{Tr}(\alpha^k) = 0$ for $1 \leq k \leq n - 2\log n - 2$. Again using the fact that $\mathrm{Tr}(z^2) = \mathrm{Tr}(z)$ for every $z \in \mathbb{F}_{2^n}$ we see that $\mathrm{Tr}(\alpha^k) = 0$ for even k's where $n - 2\log n - 2 \leq k \leq n - 1$. So we see that there exists a polynomial basis having at least $n - \log n - 1$ element of trace zero.

In the remainder of this section we prove our main result that for every t, $1 \leq t \leq n$, there exists a polynomial basis having $t + O(\log n)$ elements of trace one. Our proof will use the following result.

Lemma 4 Let $n \geq 5$ and for $M \subseteq J_n$, let $S(M) = \{2^j l | l \in M, 2^j l \leq n\}$. Then for every t, $1 \leq t \leq n$, there exists $M_{n,t} \subseteq J_n$ such that $\#S(M_{n,t}) = t$.

Proof. It can be verified easily that the claim holds for $5 \leq n \leq 16$. We continue by induction. Suppose the claim holds for $n-1$: for every t, $1 \leq t \leq n-1$, there exists $M_{n-1,t} \subseteq J_{n-1}$ such that $\#S(M_{n-1,t}) = t$. We prove the claim for n. If n is odd and $1 \leq t \leq n-1$, then we can set $M_{n,t} = M_{n-1,t}$. Also for $t = n$ we can take $M_{n,n} = J_n$.

Suppose n is even and $n = 2^i u$ where u is an odd number, and let $1 \leq t \leq n-1$. Now if $u \notin M_{n-1,t}$, then we let $M_{n,t} = M_{n-1,t}$. If $u \in M_{n-1,t}$ then we cannot take $M_{n,t}$ to be $M_{n-1,t}$, because then $n \in S(M_{n,t})$ and so $\#S(M_{n,t}) = t + 1$. In this situation we have two cases. Either there is $l \in M_{n-1,t}$ such that $l > n/2$ or there is no such l. In the former case we let $M_{n,t} = M_{n-1,t} \setminus \{l\}$. In the latter case we let $M_{n,t} = (M_{n-1,t} \setminus \{u\}) \bigcup \{l_1, l_2, \ldots, l_i\}$ where we have $l_j > n/2$ for $j = 1, 2, \ldots, i$. Note that here we remove $i+1$ elements from $S(M_{n-1,t})$, namely $u, 2u, \ldots, 2^i u$, and add i elements to it by choosing l_j's. The l_j's can be chosen since there are $\lfloor n/4 \rfloor$ odd numbers greater than $n/2$ and $\lfloor n/4 \rfloor \geq \lfloor \log n \rfloor \geq i$ when $n > 16$. Finally $\#S(J_n) = n$ and the proof is complete. □

Note that when for every $l \in M$ we have $\mathrm{Tr}(\alpha^l) = 1$, then using the fact that $\mathrm{Tr}(z^2) = \mathrm{Tr}(z)$ we have $\mathrm{Tr}(\alpha^m) = 1$ for every $m \in S(M)$.

Theorem 5 For every t, $1 \leq t \leq n-1$, there exists a polynomial basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ having at least $t - \log n - 1$ and at most $t + \log n + 1$ elements of trace 1.

Proof. Let K be the set consisting of the odd numbers from 1 to $n-2\log n-2$. Let $L = M_{n-1,t}\bigcap K$. Now using Theorem 3, there exists $\alpha \in \mathcal{A}_n$ such that $\mathrm{Tr}(\alpha^k) = 1$ if $k \in L$ and $\mathrm{Tr}(\alpha^k) = 0$ if $k \in K\setminus L$. So we have $\mathrm{Tr}(\alpha^k) = 1$ for every $k \in S(L)$, and a similar argument shows that $\mathrm{Tr}(\alpha^k) = 0$ for every $k \in S(K\setminus L)$. We show that $|\#S(L)-t| \leq \log n+1$. We have $\#S(M_{n-1,t}) = t$. Since K consists of the odd numbers less than $n-2\log n-2$, there are at most $\log n+1$ odd numbers from $M_{n-1,t}$ which are not in L. But since $n-2\log n-2 > n/2$, provided that $n > 21$, the contribution of the odd numbers greater than $n-2\log n-2$ to $S(M_{n-1,t})$ is at most $\log n+1$. Hence $\#S(L) \geq t-\log n-1$ and we have at least $t-\log n-1$ trace-one elements in the corresponding polynomial basis. With a similar argument we can show $\#S(K\setminus L) \geq n-t-\log n-1$. So we conclude that there is a polynomial basis having at least $t-\log n-1$ and at most $t+\log n+1$ trace-one elements. □

3 Irreducible polynomials

In this section we study the relation between weights of irreducible polynomials and traces of elements of the corresponding polynomial bases.

Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ be an irreducible polynomial of degree n over $\mathbb{F}_2$, and let α be a root of $f(x)$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$. Then it is well known that the roots of $f(x)$ in $\mathbb{F}_{2^n}$ are precisely $x_i = \alpha^{2^i}$ for $0 \leq i \leq n-1$. Now define

$$s_k = \mathrm{Tr}(\alpha^k) \ \text{ for } \ 0 \leq k \leq n-1. \tag{6}$$

Then we have $f(x) = \prod_{i=0}^{n-1}(x-x_i)$ and $s_k = \sum_{i=0}^{n-1} x_i^k$. Thus the coefficients a_i are the elementary symmetric polynomials of x_i, and s_k are the power sums. By Newton's identity [8, Theorem 1.75],

$$s_k + s_{k-1}a_1 + s_{k-2}a_2 + \cdots + s_1a_{k-1} + ka_k = 0 \tag{7}$$

for $1 \leq k < n$. Now the coefficients of the monomials of $f(x)$ can be related to the traces of the elements of the corresponding polynomial basis by the above identity. For example if we have $s_1 = s_3 = \cdots = s_{2l+1} = 0$, then $a_1 = a_3 = \cdots = a_{2l+1} = 0$. Using this observation Shparlinski [11] showed that there exists an irreducible polynomial of degree n over $\mathbb{F}_2$ having weight $n/4 + o(n)$.

In the following we prove the existence of an irreducible polynomial of degree n over $\mathbb{F}_2$ of weight $n/2 + o(n)$ and having some additional structure. Our proof will use the following result.

Lemma 6 If $\sum_{1\leq k\leq \alpha n/2}\binom{n/2}{k} \geq \frac{2^{n/2}}{4n}$, then $\alpha \geq 1/2 + o(1)$.

Proof. This result can be deduced easily from the Chernoff bound. (See page 11 of [3].) □

Theorem 7 There exists an irreducible polynomial $f(x) = x^n + x^{m_1} + x^{m_2} + \cdots + x^{m_l} + g(x)$ in $\mathbb{F}_2[x]$ such that:

(i) $n > m_1 > m_2 > \cdots > m_l > \deg(g(x))$.
(ii) $g(x)$ is of degree at most $2\log n + 2$.
(iii) $m_1 = n-1$, $m_{i+1} = m_i - 1$ for $i = 2, 4, \ldots, l-1$ and $n \equiv m_2 \equiv m_4 \equiv m_6 \equiv \cdots \equiv m_{l-1} \pmod 2$.
(iv) $f(x)$ is of weight $n/2 + o(n)$.

Proof. In Theorem 3, let $K \subseteq J_{n-1}$ consist of all the odd numbers less than or equal to $n - 2\log n - 2$, and let $L = K$. Then Theorem 3 implies that there exists a polynomial basis for which $s_k = 1$ for all $k \in K$ and this fact in turn implies that $s_k = 1$ for every $1 \le k \le n - 2\log n - 2$. Now, careful examination of inequality (5) reveals that not only does it imply the existence of a polynomial basis having this property but also the existence of at least $n2^{n/2}$ of them. In inequality (5) we have

$$|T_{K,L} - 2^{n-m}| \le n2^{n/2}, \tag{8}$$

so $T_{K,L} \ge 2^{n-m} - n2^{n/2}$. Here m is taken to be less than or equal to $n/2 - \log n - 1$. Hence $T_{K,L} \ge n2^{n/2}$.

Since every irreducible polynomial contributes n roots to $\mathcal{A}_n$, the number of irreducible polynomials having a root for which $s_k = 1$ for $1 \le k \le n - 2\log n - 2$ is at least $n2^{n/2}/n = 2^{n/2}$. Given any of these irreducible polynomials, using the fact that $s_k = 1$ for every $1 \le k \le n - 2\log n - 2$ and applying identity (7) we have

$$a_{2i} = a_{2i+1} \text{ for every } i \le n/2 - \log n - 1. \tag{9}$$

Now let us see how many polynomials of degree n in $\mathbb{F}_2[x]$ have coefficients a_i that satisfy (9). Altogether we have $2^{n/2}$ choices for even-indexed coefficients and exactly $2n$ choices for a_{2i+1}'s where i is greater than $n/2 - \log n - 1$. Since $a_{2i} = a_{2i+1}$ for every $i \le n/2 - \log n - 1$, the total number of polynomials satisfying (9) is $2n2^{n/2}$. From this counting argument we deduce that there is a choice of a_{2i+1}'s, $i > n/2 - \log n - 1$, for which there are $2^{n/2}/2n$ irreducible polynomials having a_{2i+1} as coefficient of their $(2i+1)$-th term for every $i > n/2 - \log n - 1$ and satisfying (9). Call this set of polynomials T.

Now, there are $2^{n/2}$ polynomials in $\mathbb{F}_2[x]$ having the particular a_{2i+1} as coefficient of their $(2i+1)$-th term for every $i > n/2 - \log n - 1$ and satisfying (9). Suppose the polynomials in T have either $\le r$ even indexed coefficients equal to one or $\ge s$ even-indexed coefficients equal to one where $s > r$. Then $\#T \le \sum_{k=1}^{r} \binom{n/2}{k} + \sum_{k=s}^{n/2} \binom{n/2}{k}$. Since $\#T \ge 2^{n/2}/2n$, applying Lemma 6 we see that there exists an irreducible polynomial of degree n for which roughly half of the even-indexed coefficients are one and rest are zero. Using the fact that for even i's $a_i = a_{i+1}$, $i \le n - 2\log n - 2$, we see that for this polynomial roughly half of the odd-indexed coefficients are one and the rest are zero. This completes the proof. □

Notice that one can prove Shparlinski's result [11] by taking a polynomial basis having almost all the elements of trace zero and showing that there exists an irreducible polynomial of weight $n/4 + o(n)$. In Theorem 7 we took the other extreme case, namely almost all the elements of the polynomial basis are of trace

1, and found that there is an irreducible polynomial of weight $n/2 + o(n)$. So based on Theorem 3 one can hope to prove that for every $t, n/4 \leq t \leq n/2$, there exists an irreducible polynomial of degree n over $\mathbb{F}_2$ having weight $t + o(n)$.

Acknowledgments

I would like to thank Alfred Menezes and Igor Shparlinski for their helpful advice and comments.

References

1. O. Ahmadi and A. Menezes, "On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$", *Designs, Codes and Cryptography*, to appear.
2. I. Blake, S. Gao and R. Lambert, "Constructive problems for irreducible polynomials over finite fields", *Information Theory and Applications*, Lecture Notes in Computer Science 793 (1994), 1-23.
3. B. Bollobas, *Random Graphs*, Academic Press, 1985.
4. K. Fong, D. Hankerson, J. López and A. Menezes, "Field inversion and point halving revisited", *IEEE Transactions on Computers*, 53 (2004), 1047-1059.
5. G. Gong, T. Berson and D. Stinson, "Elliptic curve pseudorandom sequence generators", *Selected Areas in Cryptography—SAC '99*, Lecture Notes in Computer Science 1758 (2000), 34-48.
6. G. Gong and A. Youssef, "Cryptographic properties of the Welch-Gong transformation sequence generators", *IEEE Transactions on Information Theory*, 48 (2002), 2837-2846.
7. E. Knudsen, "Elliptic scalar multiplication using point halving", *Advances in Cryptology—ASIACRYPT '99*, Lecture Notes in Computer Science 1716 (1999), 135-149.
8. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1984.
9. R. Schroeppel, "Elliptic curve point halving wins big", 2nd Midwest Arithmetical Geometry in Cryptography Workshop, Urbana, Illinois, November 2000.
10. G. Seroussi, "Table of low-weight binary irreducible polynomials", Hewlett-Packard Technical Report HPL-98-135, 1998.
11. I. E. Shparlinski, "On primitive polynomials", *Problemy Peredachi Inform.*, 23 (1987), 100-103 (in Russian).
12. I. E. Shparlinski, "On the number of zero trace elements in polynomial bases for $\mathbb{F}_{2^n}$", *Revista Matemática Complutense*, to appear.
13. R. G. Swan , "Factorization of polynomials over finite fields", *Pacific Journal of Mathematics*, 12 (1962), 1099-1106.