GENERATORS AND IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Daqing Wan
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
E-mail: wan@math.psu.edu

Abstract. Weil's character sum estimate is used to study the problem of constructing generators for the multiplicative group of a finite field. An application to the distribution of irreducible polynomials is given, which confirms an asymptotic version of a conjecture of Hansen-Mullen

1. Introduction

Let $\mathbf{F}_q$ be a finite field of q elements with characteristic p. For a positive integer $m > 1$, let $\mathbf{F}_{q^m}$ be an extension field of $\mathbf{F}_q$ of degree m. One of the basic problems in computational finite field theory is to construct a set of generators for the multiplicative group $\mathbf{F}_{q^m}^*$. Ideally, one would like to have a primitive element of $\mathbf{F}_{q^m}^*$. However, the construction (even testing) of a primitive root is at present deterministically difficult. In this paper, we consider three weaker questions about generators of finite fields. The first one is as follows.

Question 1.1. *For which pair (q, m), the multiplicative group $\mathbf{F}_{q^m}^*$ is generated by the line $\mathbf{F}_q + \alpha$ for every α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$.*

This question also arises from several applications such as graph theory [Ch] and number theoretic algorithms [Le2]. For a given α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$, define the difference graph $G(m, q, \alpha)$ to be the graph whose vertices are the elements of the multiplicative group $\mathbf{F}_{q^m}^*$, where two elements β_1 and β_2 are connected if and only if $\beta_1/\beta_2 = (\alpha + a)$ for some a in the ground field $\mathbf{F}_q$. This is a regular graph of degree q, i.e., each vertex is connected to exactly q other vertices. The difference graph is studied in [Ch] and more generally in [Li]. It is clear that the graph $G(m, q, \alpha)$

Partially supported by NSF
1991 Mathematics Subject Classification Numbers: 11T24, 11T55

is connected if and only if $\mathbf{F}_{q^m}^*$ is generated by the line $\mathbf{F}_q + \alpha$. Thus, the graph $G(m, q, \alpha)$ is connected for every α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$ if and only if Question 1.1 has a positive answer for the pair (q, m).

It is not hard to prove that if $q > (m-1)^2$, then the answer of Question 1.1 is positive and thus the graph $G(m, q, \alpha)$ is connected, see [Ch]. If $q^m - 1$ $(m > 1)$ is a (Mersenne) prime, the answer of Question 1.1 is clearly positive. Thus, we can assume that $q^m - 1$ is not a prime. It is unknown if the bound $q > (m-1)^2$ can be substantially weakened. In order to understand how close to the truth the bound $q > (m-1)^2$ might be, here we investigate when Question 1.1 has a negative answer. We have

Theorem 1.2. *If $q^m - 1$ has a divisor $d > 1$ such that*

$$m \geq 2(q \log_q d + \log_q(q+1)), \tag{1.1}$$

then the multiplicative group $\mathbf{F}_{q^m}^*$ is not generated by the line $\mathbf{F}_q + \alpha$ for some α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$.

This result shows that in some sense the bound $q > (m-1)^2$ is not too far from being sharp, although we still do not know what would happen for those m in the interval

$$\sqrt{q} + 1 \leq m < 2(q \log_q d + \log_q(q+1)).$$

If q is odd, we can take $d = 2$ in Theorem 1.2. If $q > 2$, we can take $d = (q-1) > 1$ and the bound in (1.1) essentially reduces to the bound $m \geq 2(q+1)$ first observed by Lenstra. I owe entirely to Lenstra for suggesting to me the problem and the possibility of getting a better bound if $q^m - 1$ has a small divisor d. If $q = 2$, no obvious factor of $2^m - 1$ is known unless m is a composite number. See section 3 for a complete result of Lenstra in the case $q = 2$ and m composite.

Our second question concerns the distribution of primitive normal elements. Even though the construction of a primitive element for $\mathbf{F}_{q^m}^*$ is difficult, Shoup constructed a subset of small size which contains a primitive element of $\mathbf{F}_{q^m}^*$. More precisely, Shoup [Sh] showed that if α in $\mathbf{F}_{q^m}$ is of degree m over $\mathbf{F}_q$, then there is a monic irreducible polynomial $g(T)$ in $\mathbf{F}_q[T]$ of degree at most $\lceil 6 \log_q m + C \log_q \log q \rceil$ such that $g(\alpha)$ is a primitive element of $\mathbf{F}_{q^m}^*$, where C is an absolute constant. If q is small, this result gives a polynomial size subset containing a primitive element and thus yields a polynomial time search algorithm in the sense of Shoup. A closely related result was obtained by Shparlinski [Shp, Theorem 2.4], see Corollary 4.3 for a unified description. A natural question is then to try to extend Shoup's result to primitive normal elements. Namely,

Question 1.3. *Let α be a normal element of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$. Is there an irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of small degree such that $g(\alpha)$ is a primitive normal element of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$.*

In this question, we assumed that the given α is already normal. If α is not normal, then the answer can be negative. For example, if the minimal polynomial of α is $T^m - aT - b$, Newton's formula shows that for each $0 \leq i \leq m-2$, the power α^i has trace zero. This implies that if $g(T)$ is a polynomial over $\mathbf{F}_q$ of degree less than $m-1$, then $g(\alpha)$ is not normal. Thus, we should assume that α is normal. This is not a severe restriction because a normal element can always be constructed deterministically in polynomial time, see Lenstra [Le1] or Bach-Driscoll-Shallit [BDS].

Theorem 1.4. *There are absolute positive constants C_1 and C_2 such that if*

$$q \geq C_1 m \log^2 m \tag{1.2}$$

and if α is a normal element of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, then there is a primitive normal element of the form $g(\alpha)$, where $g(T)$ is a monic irreducible polynomial over $\mathbf{F}_q$ of degree at most $\lceil 6\log_q m + C_2 \log_q \log q \rceil$.

This result shows that Question 1.3 has a positive answer if q is suitable large compared to m. We do not know if the condition in (1.2) can be removed.

Our third question concerns the distribution of irreducible polynomials. Based on various tables, Hansen-Mullen [HM, Conjecture B] proposed the following conjecture about uniform distribution of irreducible polynomials. We assume that the degree is at least three as the linear and quadratic cases are easy.

Conjecture 1.5 (Hansen-Mullen). *Let m and n be positive integers with $m \geq 3$ and $m \geq n \geq 1$. For any given element $a \in \mathbf{F}_q$ with $a \neq 0$ if $n = 1$, there exists a monic irreducible polynomial over $\mathbf{F}_q$ of degree m such that the coefficient of T^{n-1} is the given element a.*

Hansen-Mullen showed that their conjecture is true if $n = 1$ by a very simple argument: If α is a primitive element of $\mathbf{F}^*_{q^m}$, then the norm $c = \alpha^{(q^m-1)/(q-1)}$ is a primitive element of $\mathbf{F}^*_q$ and thus one can write $a = c^k$ for some $k \leq q-2$ if $a \neq 0$. The element α^k is not in any proper subfield of $\mathbf{F}_{q^m}$ and has norm equal to a. Thus, the conjecture is true if $n = 1$. By a result of Cohen [Co] on primitive elements, the conjecture is also true if $n = m$. By a recent ressut of Han [Ha1-2] on primitive roots, the conjecture is true if m is large and $n = m-1$. The following result confirms an asymptotic version of the Hansen-Mullen conjecture.

Theorem 1.6. *If either $m \geq 36$ or $q > 19$, then there is a monic irreducible polynomial in $\mathbf{F}_q[T]$ of the form $g(T) = T^m + a_{m-1}T^{m-1} + \cdots + a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + 1$ with $a_{n-1} = a$, where m, n and a are as in the above conjecture.*

Actually, the number of possible exceptions is much smaller. It should be quite realistic to completely settle Conjecture 1.5 by more detailed arguments with perhaps some computer calculations. In our proof here, we use only crude estimates in favor of their simplicity.

Acknowledgment. Portion of this paper (most of sections 2-3) is based on some unpublished notes of H. W. Lenstra Jr. on L-functions over finite fields. I would like to thank him for valuable discussions and for allowing me to include some of his unpublished notes here.

2. Estimates of character sums

In this section, we recall several forms of Weil's character sums arising from L-functions on the affine line. Our exposition of this section was greatly influenced by Lenstra's unpublished notes.

Let $\mathbf{F}_q[T]$ be the polynomial ring in one variable over $\mathbf{F}_q$. A multiplicative character for $\mathbf{F}_q[T]$ is a pair (χ, f), where $f \in \mathbf{F}_q[T]$ is a monic polynomial and $\chi : (\mathbf{F}_q[T]/f\mathbf{F}_q[T])^* \longrightarrow \mathbf{C}^*$ is a group homomorphism from the invertible elements of the residue class ring to the non-zero complex numbers. Though it is important to keep track of f, one often just refers to χ as the character. For $g \in \mathbf{F}_q[T]$, define

$$\chi(g) = \begin{cases} \chi(g \bmod f), & \text{if } \gcd(g, f) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

This defines a multiplicative function of the polynomial ring $\mathbf{F}_q[T]$. The L-function $L(\chi, t)$ associated to such a character is defined to be

$$L(\chi, t) = \sum_g \chi(g) t^{\deg g}, \tag{2.1}$$

where the summation is over all monic polynomials in $\mathbf{F}_q[T]$. The Euler product form of $L(\chi, t)$ is (by unique factorization)

$$\begin{aligned} L(\chi, t) &= \prod_{g \text{ irred.}} \frac{1}{(1 - \chi(g) t^{\deg g})} \\ &= \exp\Big(\sum_{d=1}^{\infty} S_d \frac{(\chi)}{d} t^d\Big), \end{aligned} \tag{2.2}$$

where $S_d(\chi)$ is the character sum

$$S_d(\chi) = \sum_{k|d} k \sum_{\deg(g)=k, g \text{ irred.}} \chi(g^{d/k}) = \sum_{\deg(g)=d} \Lambda(g)\chi(g) \tag{2.3}$$

and $\Lambda(g)$ is the von Mangoldt function: $\Lambda(g)$ is equal to $\deg(P)$ if g is a power of an irreducible polynomial P, and is otherwise equal to zero. In the case $d = 1$, we get the character sum

$$S_1(\chi) = \sum_{a \in \mathbf{F}_q} \chi(T - a). \tag{2.4}$$

If $\chi \neq 1$, one checks that $L(\chi, t)$ is a polynomial of degree at most $\deg(f) - 1$ with constant term 1. To see this, let $n \geq \deg(f)$. For each $h(\bmod\ f)$, there are exactly $q^{n-\deg(f)}$ monic polynomials g of degree n such that $g \equiv h(\bmod\ f)$. Thus, for $n \geq \deg(f)$,

$$\sum_{\deg g = n} \chi(g) = q^{n - \deg f} \sum_{h(\bmod f)} \chi(h) = 0.$$

This shows that for some positive integer $r \leq \deg f - 1$, one has $L(\chi, t) = \prod_{i=1}^{r}(1 - \rho_i t)$, where the ρ_i are complex numbers. In terms of character sums, one sees that for all positive integers $d \geq 1$,

$$S_d(\chi) = -\rho_1^d - \rho_2^d - \cdots - \rho_r^d. \tag{2.5}$$

Weil's result on the Riemann hypothesis of L-functions gives (see [We] and [Le2])

Theorem 2.1 (Weil). *(i). If $\chi \neq 1$, then*

$$|S_d(\chi)| \leq (\deg\ f - 1)q^{d/2}. \tag{2.6.1}$$

(ii). If $\chi \neq 1$ but $\chi(\mathbf{F}_q^*) = 1$, then

$$|1 + S_d(\chi)| \leq (\deg\ f - 2)q^{d/2}. \tag{2.6.2}$$

Note that in case (ii), the degree of f is automatically at least two since $\chi \neq 1$ but $\chi(\mathbf{F}_q^*) = 1$. Now, we use (2.6.1) to derive several interesting consequences. The first one was conjectured by Katz [Ka], observed by Lenstra to be a consequence of Theorem 2.1 by restricting the following character χ to the cyclic subalgebra $\mathbf{F}_q[x]$ of A.

Corollary 2.2. *Suppose that we are given an arbitrary finite n-dimensional commutative $\mathbf{F}_q$-algebra A, an element $x \in A$, and a character χ of the multiplicative group A^* (extended by zero to all of A) which is non-trivial on $\mathbf{F}_q[x]$. Then,*

$$|\sum_{a \in \mathbf{F}_q} \chi(a - x)| \leq (n - 1)\sqrt{q}. \tag{2.7}$$

Corollary 2.3. *Let $f_1(T), \ldots, f_n(T)$ be n monic pairwise prime polynomials in $\mathbf{F}_q[T]$ whose largest squarefree divisors have degrees $d_1, \ldots, d_n$. Let $\chi_1, \ldots, \chi_n$ be multiplicative non-trivial characters of the finite field $\mathbf{F}_q$. Assume that for some $1 \leq i \leq n$, the polynomial $f_i(T)$ is not of the form $g(T)^{\mathrm{ord}(\chi_i)}$ in $\mathbf{F}_q[T]$, where ord(χ) is the smallest positive integer d such that $\chi^d = 1$. Then, we have the estimate*

$$|\sum_{x \in \mathbf{F}_q} \chi_1(f_1(x)) \cdots \chi_n(f_n(x))| \leq (\sum_{i=1}^{n} d_i - 1)\sqrt{q}. \tag{2.8}$$

If $\chi_i^{d_i} = 1$ for all i, then the right side of (2.8) can be improved to $(\sum_{i=1}^{n} d_i - 2)\sqrt{q} + 1$.

Proof. By factoring the $f_i(T)$ if necessary, we may assume that the $f_i(T)$ are distinct, monic and irreducible. Furthermore, there is at least one i such that χ_i is non-trivial. Let $f(T) = f_1(T) \cdots f_n(T)$. For each $1 \leq i \leq n$, let ξ_i be a root of the irreducible polynomial $f_i(T)$ in some extension field. Then, the residue class ring $\mathbf{F}_q[T]/(f)$ is isomorphic to the direct sum of the fields $\mathbf{F}_q[\xi_i]$, where T is mapped to the vector $(\xi_1, \ldots, \xi_n)$. Define a character χ of $\mathbf{F}_q[T]/(f)$ as follows: For $g(T) \in \mathbf{F}_q[T]$, define $\chi(g)$ to be the product $\prod_{i=1}^{n} \chi_i(\, \mathrm{Norm}_{\mathbf{F}_q[\xi_i]/\mathbf{F}_q}(g(\xi_i)))$. Since the norm function from $\mathbf{F}_q[\xi_i]$ to $\mathbf{F}_q$ is surjective, the character $\chi_{f_i}(g) = \chi_i(\, \mathrm{Norm}(g(\xi_i)))$ is non-trivial on $\mathbf{F}_q[T]$ if χ_i is non-trivial on $\mathbf{F}_q$. By the Chinese remainder theorem, the product character $\chi = \prod_i \chi_{f_i}$ is a non-trivial character on $(\mathbf{F}_q[T]/(f))^*$. One computes that

$$\chi(a - T) = \chi_1(f_1(a)) \cdots \chi_n(f_n(a)),$$

where $a \in \mathbf{F}_q$. Estimate (2.8) then follows from (2.7). If $\chi_i^{d_i} = 1$ for all i, then $\chi(a) = \prod_i \chi_i(a^{d_i}) = 1$ for all $a \in \mathbf{F}_q$ and estimate (2.8) can be improved as stated.

Weil's theorem can be used to give sharp estimates of certain types of incomplete character sums. Here we give the following example. Let $f_1(T), \ldots, f_n(T)$ be non-constant polynomials defined over the extension field $\mathbf{F}_{q^m}$. For $1 \leq i \leq n$, let χ_i be multiplicative non-trivial characters of the extension field $\mathbf{F}_{q^m}$. Define the following incomplete character sum

$$S(d; \chi) = \sum_{a \in \mathbf{F}_q} \chi_1(f_1(a)) \cdots \chi_n(f_n(a)), \tag{2.9}$$

where the sum is over all a in the subfield $\mathbf{F}_q$. Corollary 2.3 extends to this type of incomplete sums.

Corollary 2.4. *Let the $f_i(T)$ for $1 \leq i \leq n$ be pairwise prime polynomials. Let D be the degree of the largest squarefree divisor of $\prod_{i=1}^{n} f_i(t)$. Suppose that for some $1 \leq i \leq n$, there is a root ξ_i of multiplicity m_i of $f_i(T)$ such that the character $\chi_i^{m_i}$ is non-trivial on the set Norm$_{\mathbf{F}_{q^m}[\xi_i]/\mathbf{F}_{q^m}}(\mathbf{F}_q[\xi_i])$. Then, we have the estimate*

$$|S(d; \chi)| \leq (mD - 1)\sqrt{q}. \tag{2.10}$$

Proof. The proof is similar to the proof of Corollary 2.3. By factoring the $f_i(T)$ if necessary, we may assume that the $f_i(T)$ for $1 \leq i \leq n$ are distinct and monic irreducible over $\mathbf{F}_{q^m}$. Furthermore, there is some $1 \leq i \leq n$ such that χ_i is non-trivial on the set $\mathrm{Norm}_{\mathbf{F}_{q^m}[\xi_i]/\mathbf{F}_{q^m}}(\mathbf{F}_q[\xi_i])$. Let $F_i(T)$ be the product of all distinct conjugates of $f_i(T)$ over $\mathbf{F}_q$. Then, the $F_i(T)$ are defined and irreducible over the ground field $\mathbf{F}_q$. Let $f(T) = F_1(T) \cdots F_n(T)$. This is a squarefree polynomial of degree at most mD. Let ξ_i be a root of $f_i(T)$. Define a multiplicative character χ_f on $(\mathbf{F}_q[t]/(F))^*$ by $\chi_f(g) = \prod_{i=1}^n \chi_i(\mathrm{Norm}_{\mathbf{F}_{q^m}[\xi_i]/\mathbf{F}_{q^m}}(g(\xi_i)))$. One checks that $\chi_f(a - T) = \prod_{i=1}^n \chi_i(f_i(a))$. Using our assumption and the Chinese remainder theorem as in the proof of Corollary 2.3, we conclude that χ_f is non-trivial and the corollary follows from (2.7).

The following corollary gives a simple result on the number of subfield solutions of certain diophantine equations.

Corollary 2.5. *Let $f(T)$ be a polynomial in $\mathbf{F}_{q^m}[T]$ of degree D. Let d be a positive integer. Let N_f be the number of solutions of the equation $y^d = f(x)$ in $\mathbf{F}_{q^m}$ such that x belongs to the subfield $\mathbf{F}_q$. Assume that $f(T)$ has a root ξ of multiplicity m_0 such that $(m_0, d) = 1$ and $\mathrm{Norm}_{\mathbf{F}_{q^m}[\xi]/\mathbf{F}_{q^m}}(\mathbf{F}_q[\xi]) = \mathbf{F}_{q^m}$. Then,*

$$|N_f - q| \leq (mD - 1)(d - 1)\sqrt{q}. \tag{2.11}$$

Proof. We use χ to denote a multiplicative character of the extension field $\mathbf{F}_{q^m}$. Using Corollary 2.4, we deduce that

$$\begin{aligned} |N_f - q| &= \Big|\sum_{\substack{\chi^d=1 \\ \chi\neq 1}} \sum_{x\in\mathbf{F}_q} \chi(f(x))\Big| \\ &\leq (mD - 1)(d - 1)\sqrt{q}. \end{aligned}$$

The corollary is proved.

Remark 2.6. As an example of Corollary 2.5, we may take $f(T)$ to have a linear factor $T - \alpha$ of multiplicity one, where α has degree m over $\mathbf{F}_q$. Another example is to take $f(T)$ to have a monic irreducible factor $g(T)$ over $\mathbf{F}_{q^m}$ of multiplicity one such that $g(0)$ is a primitive element of $\mathbf{F}_{q^m}$. We note that Corollary 2.5 can be false without the assumption on ξ. An easy counterexample is to take $f(T) = \beta T$, where β is a d-th power non-residue in $\mathbf{F}_{q^m}$ and $(d, q - 1) = 1$.

A similar result on subfield solutions holds for the Artin-Schreier equation.

Corollary 2.7. *Let $f(T)$ be a polynomial in $\mathbf{F}_{q^m}[T]$ of degree D. Let N_f be the number of solutions of the equation $y^p - y = f(x)$ in $\mathbf{F}_{q^m}$ such that x belongs to the* *subfield $\mathbf{F}_q$. Assume that tr$(f(T))$ is not of the form $r(T)^p - r(T) + c$ in $\bar{\mathbf{F}}_q(T)$, where tr is the trace from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ and it acts trivially on T. Then,*

$$|N_f - q| \leq (D-1)(p-1)\sqrt{q}. \tag{2.12}$$

Proof. Let Ψ_p be a non-trivial additive character of $\mathbf{F}_p$. Let $g(T)$ be the polynomial $\mathrm{tr}(f(T))$ of degree D defined over $\mathbf{F}_q$. Then,

$$\begin{aligned}
|N_f - q| &\leq |\sum_{a\in\mathbf{F}_p^*}\sum_{x\in\mathbf{F}_q} \Psi_p\big(a\cdot \mathrm{tr}_{\mathbf{F}_{q^m}/\mathbf{F}_p}(f(x))\big)\ | \\
&= |\sum_{a\in\mathbf{F}_p^*}\sum_{x\in\mathbf{F}_q} \Psi_p\big(a\cdot \mathrm{tr}_{\mathbf{F}_{q}/\mathbf{F}_p}(g(x))\big)\ | \\
&\leq (p-1)(D-1)\sqrt{q},
\end{aligned}$$

where the last inequality follows from Weil's well known estimate for additive character sums.

For applications to the Hansen-Mullen conjecture, we give two estimates of character sums over irreducible polynomials. Let χ be a character of $(\mathbf{F}_q[T]/(f))^*$. For a positive integer d, define

$$S_d'(\chi) = \sum_{\deg(g)=d} \chi(g), \tag{2.13}$$

where g runs over all monic irreducible polynomials of degree d over $\mathbf{F}_q$.

Corollary 2.8. *(i). If $\chi \neq 1$, then*

$$|S_d'(\chi)| < \frac{1}{d}(\deg\ (f)+1)q^{d/2}. \tag{2.14.1}$$

(ii). If $\chi \neq 1$ but $\chi(\mathbf{F}_q^*) = 1$, then

$$|\frac{1}{d} + S_d'(\chi)| < \frac{1}{d}\deg\ (f)q^{d/2}. \tag{2.14.2}$$

Proof. Let π_d' be the number of elements which are in a proper subfield of $\mathbf{F}_{q^d}$. Clearly,

$$\pi_d' \leq (q^{d/2} + \sum_{k|d,\ k<d/2} q^k) < 2q^{d/2}. \tag{2.15}$$

If χ is non-trivial, then Weil's estimate (2.6.1) shows that

$$\begin{aligned}
|S_d'(\chi)| &\leq \frac{1}{d}(|S_d(\chi)| + \pi_d') \\
&< \frac{1}{d}((\deg\ (f)-1)q^{d/2} + 2q^{d/2}) \\
&= \frac{1}{d}(\deg\ (f)+1)q^{d/2}.
\end{aligned}$$

This proves (2.14.1). The proof of (2.14.2) is the same except that we need to use (2.6.2).

A closely related character sum is to let g run over all irreducible polynomials with constant term 1 instead of monic irreducible polynomials. Thus, we define

$$S''_d(\chi) = \sum_{\deg(g)=d} \chi(g), \tag{2.16}$$

where g runs over all irreducible polynomials over $\mathbf{F}_q$ (not necessarily monic) of degree d with constant term 1.

Corollary 2.9. *Let $\chi \neq 1$ but $\chi(\mathbf{F}_q^*) = 1$. For all $d > 1$, we have*

$$|\frac{1}{d} + S''_d(\chi)| < \frac{1}{d} deg(f) q^{d/2}. \tag{2.17}$$

Proof. Since $\chi(\mathbf{F}_q^*) = 1$, we have

$$\chi(g(T)) = \chi(\frac{g(T)}{g(0)})$$

for all monic irreducible polynomials $g(T) \neq T$. If $g(T)$ is a monic irreducible polynomial of degree $d > 1$, then $g(T)/g(0)$ is an irreducible polynomial of degree d with constant term 1 and vice versa. Thus,

$$S'_d(\chi) = S''_d(\chi).$$

The proof is complete by (2.14.2).

3. Multiplicative groups generated by linear expressions

We now apply the character sum estimates of §2 to study Question 1.1. We have

Theorem 3.1. *If $q^m - 1$ has a divisor $d > 1$ such that*

$$m \geq 2(q \log_q d + \log_q (q+1)),$$

then the multiplicative group $\mathbf{F}_{q^m}^*$ is not generated by the line $\mathbf{F}_q + \alpha$ for some α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$.

Proof. Let $d > 1$ be a divisor of $q^m - 1$. Let $N_m(d)$ be the number of α in $\mathbf{F}_{q^m}$ such that α has degree m over $\mathbf{F}_q$ and $\alpha + a$ is a d-th power in $\mathbf{F}_{q^m}$ for every $a \in \mathbf{F}_q$. Let A_m be the subset consisting of α in $\mathbf{F}_{q^m}$ which lies in a proper subfield of $\mathbf{F}_{q^m}$. To prove Theorem 3.1, it suffices to prove that $N_m(d) > 0$.

A standard character sum argument shows that

$$N_m(d) = \frac{1}{d^q} \sum_{\alpha \in \mathbf{F}_{q^m}} \prod_{a \in \mathbf{F}_q} (\sum_{\chi^d = 1} \chi(\alpha + a)) - \frac{1}{d^q} \sum_{\alpha \in A_m} \prod_{a \in \mathbf{F}_q} (\sum_{\chi^d = 1} \chi(\alpha + a)), \qquad (3.1)$$

where $\chi(0) = 1$ if χ is the trivial character. The second sum is at most $2q^{m/2}$ by (2.15). Corollary 2.3 then implies that

$$|N_m(d) - \frac{q^m}{d^q}| < \frac{d^q - 1}{d^q}(q-1)q^{m/2} + 2q^{m/2}. \qquad (3.2)$$

This shows that

$$\begin{aligned} d^q N_m(d) &> q^m - (d^q - 1)(q-1)q^{m/2} - 2d^q q^{m/2} \\ &= q^m - (qd^q - q + 1 + d^q)q^{m/2} \\ &> q^m - d^q(q+1)q^{m/2}. \end{aligned}$$

The last number is non-negative if

$$q^{m/2} \geq (q+1)d^q, \quad \text{namely,} \quad m \geq 2(q \log_q d + \log_q(q+1)).$$

The theorem is proved.

In the case $q = 2$, no obvious factor of $2^m - 1$ is known unless m is a composite number. If $q = 2$ and m is composite, the following complete result is due to Lenstra.

Theorem 3.2. *If $q = 2$ and m is composite, then the multiplicative group $\mathbf{F}_{q^m}^*$ is generated by the line $\mathbf{F}_q + \alpha$ for every α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$ if and only if $m = 4$ or $m = 6$.*

Proof. If $q = 2$, a detailed examination of the first sum in (3.1) gives a slightly better estimate:

$$|N_m(d) - \frac{2^m}{d^2}| < \frac{(d-1)^2}{d^2} 2^{m/2} + 2q^{m/2}. \qquad (3.3)$$

In order for Question 1.1 to have a negative answer, it suffices to have a proper divisor d of $2^m - 1$ satisfying the inequality

$$2^m \geq (d-1)^2 2^{m/2} + 2 \cdot d^2 2^{m/2}, \quad \text{namely,} \quad 2^{m/2} \geq 3 \cdot d^2 - 2d + 1. \qquad (3.4)$$

Since m is composite, let u be the smallest prime factor of m and write $m = uk$. Then $d = 2^u - 1$ is a proper divisor of $2^m - 1$ and the second inequality in (3.4) becomes

$$2^{uk/2} \geq 3(2^u - 1)^2 - 2(2^u - 1) + 1 = 3 \cdot 2^{2u} - 8 \cdot 2^u + 6. \qquad (3.5)$$

For $u = 2$, inequality (3.5) is satisfied whenever $k \geq 5$. For $u = 3$, inequality (3.5) is satisfied whenever $k \geq 5$. For $u \geq 5$, inequality (3.5) is satisfied whenever

$k \geq u \geq 5$. Since u is the smallest prime factor of m, we are left only with the following cases $m = 4, 6, 8, 9$.

Case $m = 8$. We take $d = 3$ (a factor of $2^8 - 1$) and use the method in the proof of Theorem 3.1. All proper subfields of $\mathbf{F}_{2^8}$ are contained in $\mathbf{F}_{2^4}$ and the last term of (3.3) can be improved to 2^4. By (3.3),

$$N_8(d) \geq \frac{2^8}{3^2} - \frac{2^2}{3^2}2^4 - 2^4 > 0.$$

This shows that the theorem is true for $q = 2$ and $m = 8$.

Case $m = 9$. All proper subfields of $\mathbf{F}_{2^9}$ are contained in $\mathbf{F}_{2^3}$. Let $\beta \in \mathbf{F}_{2^3} - \mathbf{F}_2$. We claim that the polynomial $g(T) = T^3 + \beta T^2 + (\beta + 1)T + 1$ is irreducible over $\mathbf{F}_{2^3}$. One checks that $g(0) = g(1) = 1$. This and the irreducibility of $g(T)$ shows that if α is a root of $g(T)$, then the norms of α and $\alpha + 1$ from $\mathbf{F}_{2^3}$ to $\mathbf{F}_{2^3}$ are 1. Thus, the two elements α and $\alpha + 1$ can not generate $\mathbf{F}_{2^9}$. To prove the claim, it suffices to prove that the polynomial $g(T)$ has no zeros in $\mathbf{F}_{2^3}$. Clearly, $g(T)$ has no zeros in $\mathbf{F}_2$. If γ is an element of $\mathbf{F}_{2^3} - \mathbf{F}_2$, then γ satisfies either $\gamma^3 + \gamma + 1 = 0$ or $\gamma^3 + \gamma^2 + 1 = 0$. In the first case, if $g(\gamma) = 0$, then $\beta(\gamma^2 + \gamma) = 0$ and we have a contradiction. In the second case, if $g(\gamma) = 0$, then $(\beta + 1)(\gamma^2 + \gamma) = 0$ and again we have a contradiction. The claim is proved.

Case $m = 4$. Since $2^4 - 1 = 3 \cdot 5$, if α and $\alpha + 1$ do not generate $\mathbf{F}_{2^4}^*$, both α and $\alpha + 1$ must be primitive 5-th roots of unity. This means that both α and $\alpha + 1$ satisfy the equation $T^4 + T^3 + T^2 + T + 1 = 0$. This implies that $\alpha(\alpha + 1) = 0$ and we have a contradiction. Thus, the theorem is true for $q = 2$ and $m = 4$.

Case $m = 6$. Since $2^6 - 1 = 7 \cdot 9$, if α is a 7-th power, then α has to be a primitive 9-th root of unity. Since all primitive 9-th roots have trace zero to $\mathbf{F}_{2^2}$, $\alpha + 1$ can not be a primitive 9-th root of unity. Thus, α can not be a 7-th power and the set $\{\alpha, \alpha + 1\}$ generates the multiplicative group $\mathbf{F}_{2^6}^*$. By symmetry, if $\alpha + 1$ is a 7-th power, the same argument works. If both α and $\alpha + 1$ are a cubic power, then their norms to $\mathbf{F}_{2^2}$ are also a cubic power, which is necessarily 1. If $g(T) = T^3 + uT^2 + vT + w$ is the irreducible polynomial of α over $\mathbf{F}_{2^2}$. Then both $g(0)$ and $g(1)$ are 1. That gives $w = 1$ and $u + v = 1$. But then $u^3 + u \cdot u^2 + vu + 1 = 0$ (note that $u, v \in \mathbf{F}_{2^2} - \mathbf{F}_2$) shows that $g(T)$ is still reducible. Thus, α and $\alpha + 1$ can not both be a cubic power. This implies that α and $\alpha + 1$ generate the multiplicative group of $\mathbf{F}_{2^6}$. Thus, the theorem is true for $q = 2$ and $m = 6$. The theorem is proved.

To conclude this section, we include a more precise version of the bound $q > (m-1)^2$ mentioned in the introduction. Let $d(m, q)$ be the smallest positive integer d such that for all α with $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$, each element β in $\mathbf{F}_{q^m}^*$ can be expressed as a product of at most d elements from $\mathbf{F}_q + \alpha$, that is, there are $a_i \in \mathbf{F}_q$ $(1 \leq i \leq d)$ such that $\beta = (\alpha + a_1) \cdots (\alpha + a_d)$. If such a positive integer d does not exist, we define $d(m,q) = \infty$. The number $d(m,q)$ is simply the maximal diameter of the family of difference graphs $G(m,q,\alpha)$ parametrized by α.

Theorem 3.3. *Assume that $q > (m-1)^2$. Then*

$$d(m,q) \leq \lceil 2m + \frac{4m\log(m-1)}{\log q - 2\log(m-1)} \rceil,$$

where $\lceil x \rceil$ denotes the smallest integers $\geq x$.

Proof. Let k be a positive integer. For $\beta \in \mathbf{F}_{q^m}^*$, let $N_k(\beta,\alpha)$ be the number of solutions of the equation $\beta = (\alpha + a_1)\cdots(\alpha + a_k)$, where the a_i take values in the ground field $\mathbf{F}_q$. Then,

$$\begin{aligned} N_k(\beta,\alpha) &= \frac{1}{q^m-1}\sum_{a_i\in\mathbf{F}_q}\sum_{\chi}\chi^{-1}(\beta)\chi((\alpha+a_1)\cdots(\alpha+a_k)) \\ &= \frac{q^k}{q^m-1} + \frac{1}{q^m-1}\sum_{\chi\neq 1}\chi^{-1}(\beta)(\sum_{a\in\mathbf{F}_q}\chi(\alpha+a))^k, \end{aligned} \tag{3.6}$$

where χ runs over all multiplicative characters of $\mathbf{F}_{q^m}^*$. By corollary 2.2, we deduce that

$$|N_k(\beta,\alpha) - \frac{q^k}{q^m-1}| < (m-1)^k\sqrt{q}^k. \tag{3.7}$$

In order for $N_k(\beta,\alpha) > 0$ for all β, it suffices to have the inequality

$$q^{k/2} \geq q^m(m-1)^k.$$

Solving this inequality, one gets

$$k \geq 2m + \frac{4m\log(m-1)}{\log q - 2\log(m-1)}.$$

The theorem is proved.

Theorem 3.3 is essentially the same as Chung's diameter bound

$$d(m,q) \leq \lceil 2m + \frac{4m\log m}{\log q - 2\log(m-1)} \rceil.$$

It is slightly better if q is very close to $(m-1)^2$.

4. Primitive elements and primitive normal elements

An element $\alpha \in \mathbf{F}_{q^m}$ is said to be normal over $\mathbf{F}_q$ if the set $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ forms a basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$. The element α is said to be primitive if α generates the multiplicative group of $\mathbf{F}_{q^m}$. The element α is said to be a primitive normal element if it is both primitive and normal. A primitive normal element always exists, see Lenstra and Schoof [LS]. An interesting question is then to construct primitive normal elements. Since the construction of primitive elements is difficult, the construction of primitive normal elements will certainly not be easier. Motivated by Shoup's work on primitive elements, here we are interested in the following weaker question: Given a normal element α of degree m over $\mathbf{F}_q$, we hope to have a polynomial $g(T)$ of small degree such that $g(\alpha)$ is a primitive normal element of $\mathbf{F}_{q^m}$. The following result is a more precise version of Theorem 1.4.

Theorem 4.1. *Let Ω_m be the number of distinct prime factors of $T^m - 1$ over $\mathbf{F}_q$. There are absolute positive constants C_1 and C_2 such that if*

$$q \geq C_1 \Omega_m \log^2 m$$

and if α is a normal element of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, then there is a primitive normal element of the form $g(\alpha)$, where $g(T)$ is a monic irreducible polynomial over $\mathbf{F}_q$ of degree at most $\lceil 6 \log_q m + C_2 \log_q \log q \rceil$.

To prove this theorem, we need the following result of Shoup [Sh] on primitive elements of low degrees.

Lemma 4.2. *Let ω_m be the number of distinct prime factors of $q^m - 1$. Let α be an element of $\mathbf{F}_{q^m}$ with degree m over $\mathbf{F}_q$. For a positive integer k, let $P_k(\alpha)$ be the number of monic irreducible polynomials $g(T)$ over $\mathbf{F}_q$ of degree k such that $g(\alpha)$ is primitive in $\mathbf{F}_{q^m}^*$. There are absolute positive constants C_1 and C_2 such that*

$$P_k(\alpha) \geq C_1 \frac{q^k}{(\log \omega_m + 1)^2} - C_2 \omega_m^2 m q^{k/2}. \tag{4.1}$$

This result was proved by Shoup [Sh] for $q = p$ using Weil's character sum estimate together with Iwaniec's shifted sieve. For general q, the proof is the same. Replacing q by q^u, Lemma 4.2 gives

Corollary 4.3. *Let u be a positive integer. Let α be an element of $\mathbf{F}_{q^{um}}$ with degree m over $\mathbf{F}_{q^u}$. For a positive integer k, let $P_{k,u}(\alpha)$ be the number of monic irreducible polynomials $g(T)$ over $\mathbf{F}_{q^u}$ of degree k such that*

$$Norm(g(\alpha)) = g(\alpha)^{(q^{um}-1)/(q^m-1)}$$

is primitive in $\mathbf{F}_{q^m}^*$. There are absolute positive constants C_1 and C_2 such that

$$P_{k,u}(\alpha) \geq C_1 \frac{q^{uk}}{(\log \omega_{mu} + 1)^2} - C_2 \omega_{mu}^2 m q^{uk/2}.$$

In fact, if $g(\alpha)$ is primitive in $\mathbf{F}_{q^{um}}$, then $\mathrm{Norm}(g(\alpha))$ is primitive in $\mathbf{F}_{q^m}$. Thus, Corollary 4.3 follows from Corollary 4.2. Taking $k=1$, Corollary 4.3 reduces to Shparlinski's result [Shp]. Taking $u=1$, Corollary 4.3 reduces to Lemma 4.2.

Proof of Theorem 4.1. We can assume that $m>1$. The idea is to remove those elements $g(\alpha)$ that are not normal and then apply Shoup's lemma. Let σ be the Frobenius automorphism $\sigma(\beta)=\beta^q$. The additive group $\mathbf{F}_{q^m}$ is a cyclic $\mathbf{F}_q[T]$-module under the action $T(\beta)=\sigma(\beta)$. For an element $\beta\in\mathbf{F}_{q^m}$, the order of β in $\mathbf{F}_q[T]$ is the monic polynomial $r(T)$ of smallest degree such that $r(T)\beta=0$. Such an order is a monic factor of T^m-1. An element β is normal if and only if the order of β is T^m-1. Alternatively, an element β is not normal if and only if there is an irreducible factor $s(T)$ of T^m-1 $(m>1)$ over $\mathbf{F}_q$ such that $(T^m-1)/s(T)$ annihilates the element β.

Now, for a positive integer k, let $M(k)$ be the set of elements of the form $g(\alpha)$, where $g(T)$ is a monic polynomial in $\mathbf{F}_q[T]$ of degree k. We claim that $M(k)$ contains at least $q^k-\Omega_m q^{k-1}$ normal elements. In fact, if $s(T)$ is an irreducible factor of T^m-1 and $(a_{k-1},\cdots,a_2,a_0)$ is a given $(k-1)$-tuple of elements from $\mathbf{F}_q$, then $(T^m-1)/s(T)$ annihilates at most one of the elements in the family $\alpha^k+a_{k-1}\alpha^{k-1}+\cdots+a_1\alpha+a_0$ parametrized by a_1, because α is normal. Thus, the polynomial $(T^m-1)/s(T)$ annihilates at most q^{k-1} elements of $M(k)$. Since T^m-1 has Ω_m distinct irreducible factors, there are at most $\Omega_m q^{k-1}$ non-normal elements in $M(k)$ and the claim follows.

Let $N_k(\alpha)$ be the number of normal elements in $M(k)$. To prove the theorem, it suffices to prove that $N_k(\alpha)+P_k(\alpha)>q^k$. By the above claim and Shoup's lemma, we are led to solve the inequality

$$(q^k-\Omega_m q^{k-1})+(C_1\frac{q^k}{(\log\omega_m+1)^2}-C_2\omega_m^2 m q^{k/2})>q^k. \tag{4.2}$$

Since $\omega_m=O(m\log q)$, it suffices to solve

$$C_1'\frac{q^k}{(\log m+\log\log q)^2}\geq C_2' m^3(\log^2 q)q^{k/2}+\Omega_m q^{k-1}. \tag{4.3}$$

Inequality (4.3) clearly holds if

$$\frac{1}{2}C_1'\frac{q^k}{(\log m+\log\log q)^2}\geq\Omega_m q^{k-1},\quad \frac{1}{2}C_1'\frac{q^k}{(\log m+\log\log q)^2}\geq C_2' m^3(\log^2 q)q^{k/2}. \tag{4.4}$$

The first inequality in (4.4) gives $q\geq C_1''\Omega_m\log^2 m$. This together with the second inequality in (4.4) gives $k\geq 6\log_q m+C_2''\log_q\log q$. Since k is an integer, the theorem is proved.

Corollary 4.4. *There are absolute positive constants C_1 and C_2 such that if*

$$q \geq C_1 m^6 \log^{C_2} m$$

and if α is a normal element of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, then there is a primitive normal element of $\mathbf{F}_{q^m}$ of the form $\alpha + a$, where $a \in \mathbf{F}_q$.

5. Distribution of irreducible polynomials

Let $m \geq n \geq 1$ be positive integers and let a be a given element in $\mathbf{F}_q$. The Hansen-Mullen conjecture concerns the existence of irreducible polynomials over $\mathbf{F}_q$ of the form $g(T) = T^m + a_{m-1}T^{m-1} + \cdots + a_1 T + a_0$ with $a_{n-1} = a$. If n is small compared to m, the conjecture follows immediately from the following well known theorem on primes in an arithmetic progression by taking $f(T) = T^n$ and $\Phi(f) = q^{n-1}(q-1)$. For a related result on primes in arithmetic progressions, see Effinger and Hayes [EH].

Theorem 5.1. *Let $f(T)$ be a polynomial of degree n in $\mathbf{F}_q[T]$. Let m be a positive integer and let h be a polynomial in $\mathbf{F}_q[T]$ which is relatively prime to f. Let $\pi_m(h)$ be the number of monic irreducible polynomials g in $\mathbf{F}_q[T]$ of degree m such that $g \equiv h (\mathrm{mod} f)$. Then,*

$$|\pi_m(h) - \frac{q^m}{m\Phi(f)}| \leq \frac{1}{m}(n+1)q^{m/2}, \tag{5.1}$$

where $\Phi(f)$ is the number of elements in $(\mathbf{F}_q[T]/(f))^*$ (the Euler function in function fields).

Proof. For a character χ of $(\mathbf{F}_q[T]/(f))^*$, let $\bar{\chi}$ be its inverse or conjugate. Then, a standard character sum argument shows that

$$\pi_m(h) = \frac{1}{\Phi(f)} \sum_{\deg(g)=m,\ g \text{ monic irred.}} \sum_{\chi} \chi(g)\bar{\chi}(h). \tag{5.2}$$

Let π_m be the number of monic irreducible polynomials over $\mathbf{F}_q$ of degree m. Separating the trivial character in (5.2) and applying estimate (2.14.1), we deduce

$$|\pi_m(h) - \frac{1}{\Phi(f)}\pi_m| \leq \frac{\Phi(f)-1}{m\Phi(f)}(n+1)q^{m/2}.$$

Using (2.15), we obtain

$$\begin{aligned} |\pi_m(h) - \frac{q^m}{m\Phi(f)}| &\leq \frac{1}{m\Phi(f)}\{(\Phi(f)-1)(n+1)q^{m/2} + 2 \cdot q^{m/2}\} \\ &\leq \frac{1}{m}(n+1)q^{m/2}. \end{aligned}$$

The proof is complete.

The above theorem can be applied only when the degree n of $f(T)$ is small. If the degree n is close to $m/2$, then (5.1) gives no information. For the purpose of Hansen-Mullen conjecture, the desired irreducible polynomial $g(T)$ can be chosen flexibly from many residue classes modulo T^n. A suitable large subset of these residue classes can be given a nice structure. An exploitation of structures among these residue classes would then permit us to get useful information for larger n. We now carry out this idea. Recall that a polynomial $h(T)$ over $\mathbf{F}_q$ is called primary if it is a power of an irreducible polynomial $r(T)$ over $\mathbf{F}_q$. The degree of $r(T)$ is denoted by $\Lambda(h)$, the von Mangoldt function. Working with primary polynomials instead of irreducible polynomials will result in simpler estimates.

We first assume that $a \neq 0$.

Let H_{n-1} be the set of all monic primary polynomials over $\mathbf{F}_q$ of degree $n-1$. Define the following weighted sum

$$w_a(m,n) = \sum_{h \in aH_{n-1}} \Lambda(h) \sum_{g \equiv h \pmod{T^n}} 1,$$

where g denotes a monic irreducible polynomial over $\mathbf{F}_q$ of degree m and $\Lambda(h)$ is defined to be 1 if h is a non-zero constant. For the purpose of the Hansen-Mullen conjecture, we want to have $w_a(m,n) > 0$. We now give an asymptotic formula for $w_a(m,n)$. Recall that π_m denotes the number of monic irreducible polynomials over $\mathbf{F}_q$ of degree m.

Theorem 5.2. *Let $a \neq 0$. (i). If $n > 1$, then*

$$|w_a(m,n) - \frac{\pi_m}{q-1}| < \frac{1}{m}(n^2-1)q^{(m+n-1)/2}.$$

(ii). If $n = 1$, then

$$|w_a(m,1) - \frac{\pi_m}{q-1}| \leq \frac{1}{m}(\frac{q-2}{q-1})2q^{m/2}.$$

Proof. Let χ run over the $q^{n-1}(q-1)$ characters of $(\mathbf{F}_q[T]/(T^n))^*$. Weil's estimate (2.6.1) shows that if $n > 1$ and $\chi \neq 1$, then

$$|\sum_{h \in aH_{n-1}} \Lambda(h)\chi(h)| = |\chi(a) \sum_{h \in H_{n-1}} \Lambda(h)\chi(h)| \leq (n-1)q^{(n-1)/2}. \tag{5.3}$$

If χ is trivial, then the above sum is simply q^{n-1} for $n \geq 1$. By the definition of $w_a(m,n)$ and a standard character sum argument, one deduces

$$\begin{aligned} w_a(m,n) &= \sum_{h \in aH_{n-1}} \Lambda(h) \sum_g \frac{1}{q^{n-1}(q-1)} \sum_\chi \chi(g)\bar{\chi}(h) \\ &= \frac{1}{q^{n-1}(q-1)} \sum_\chi (\sum_g \chi(g))(\sum_{h \in aH_{n-1}} \Lambda(h)\bar{\chi}(h)), \end{aligned} \tag{5.4}$$

where g runs over all monic irreducible polynomials over $\mathbf{F}_q$ of degree m. By (2.14.1) and (5.3), we conclude that for $n > 1$,

$$\begin{aligned}|w_a(m,n) - \frac{\pi_m}{q-1}| &< \frac{1}{m}(n+1)q^{m/2}(n-1)q^{(n-1)/2} \\ &= \frac{1}{m}(n^2-1)q^{(m+n-1)/2}.\end{aligned}$$

If $n = 1$, there are $(q-2)$ non-trivial characters χ in (5.4) and the estimate in (5.3) becomes 1 instead of zero. The rest of the argument is the same. The proof is complete.

Corollary 5.3. *Let $a \in \mathbf{F}_q^*$. Let $m \geq 3$ and $m \geq n \geq 1$. If*

$$q^{m-n+1} \geq (q-1)^2 n^4,$$

then there is a monic irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of degree m such that the coefficient of T^{n-1} is a.

Proof. If $n = 1$, the result is always true by the simple argument of Hansen-Mullen. One can also use the second estimate of Theorem 5.2. We now assume that $n > 1$. By Theorem 5.2 and (2.15),

$$|m(q-1)w_a(m,n) - q^m| < (q-1)(n^2-1)q^{(m+n-1)/2} + 2q^{m/2} \leq (q-1)n^2 q^{(m+n-1)/2},$$

where the exceptional case $n = q = 2$ needs a little extra treatment using the middle term of (2.15). The corollary follows.

The above corollary implies that the Hansen-Mullen conjecture is true for $a \neq 0$ if $1 \leq n < m-1$ and q is large compared to m. One can use the above method to derive a similar estimate in the case $a = 0$. We shall not do so. Instead, we shall derive an estimate which handle the case when $m - n$ is small and by symmetry this also includes the case $a = 0$. For this purpose, we need to consider irreducible polynomials of degree m whose constant term is always 1, namely, irreducible polynomials of the form $1 + a_1 T + \cdots + a_m T^m$ with $a_m \neq 0$.

For $n \geq 2$, let G_{n-2} be the set of primary polynomials over $\mathbf{F}_q$ of degree $n-2$ with constant term 1. Thus, we are considering primary polynomials of the form $1 + a_1 T + \cdots + a_{n-2} T^{n-2}$ with $a_{n-2} \neq 0$. For simplicity of estimates, we include the constant 1 as a special element of G_{n-2} and define $\Lambda(1) = 1$. This special element corresponds to the monic primary polynomial T^{n-2}. For a fixed $a \in \mathbf{F}_q$, define the following weighted sum

$$W_a(m,n) = \sum_{h \in G_{n-2}} \Lambda(h) \sum_{g \equiv h + aT^{n-1} \pmod{T^n}} 1,$$

where g denotes an irreducible polynomial over $\mathbf{F}_q$ of degree m with constant term 1. In the application to the Hansen-Mullen conjecture, we want to have $W_a(m,n) > 0$. The following is an asymptotic formula for $W_a(m,n)$.

Theorem 5.4. *Let $a \in \mathbf{F}_q$. (i). If $n > 2$, we have*

$$|W_a(m,n) - \frac{\pi_m}{q}| < \frac{1}{m}(n-1)^2 q^{(m+n-2)/2}.$$

(ii). If $n = 2$, we have

$$|W_a(m,2) - \frac{\pi_m}{q}| < \frac{2}{m} q^{m/2}.$$

Proof. Let U_1 be the set of polynomials of the form $1 + a_1T + \cdots + a_{n-1}T^{n-1}$ over $\mathbf{F}_q$. The set U_1 is an abelian group of order q^{n-1} under multiplication modulo T^n. The direct product of U_1 with $\mathbf{F}_q^*$ gives the full group $(\mathbf{F}_q[T]/(T^n))^*$.

Let χ run over the q^{n-1} characters of the subgroup U_1, namely, the characters of $(\mathbf{F}_q[T]/(T^n))^*$ which are trivial on $\mathbf{F}_q^*$. For $h \in G_{n-2}$, one checks that

$$h + aT^{n-1} \equiv h(1 + aT^{n-1}) \pmod{T^n}.$$

Weil's estimate (2.6.2) shows that if $\chi \neq 1$ and $n > 2$, then

$$|\sum_{h \in G_{n-2}} \Lambda(h)\chi(h + aT^{n-1})| = |\chi(1 + aT^{n-1}) \sum_{h \in G_{n-2}} \Lambda(h)\chi(h)| \leq (n-2)q^{(n-2)/2}, \tag{5.5}$$

where we used the fact that $\chi(\mathbf{F}_q^*) = 1$ and our convention about the special element 1 of G_{n-2}. If χ is trivial, then the above sum is simply q^{n-2} for $n \geq 2$.

By the definition of $W_a(m,n)$ and a standard character sum argument, one deduces

$$\begin{aligned} W_a(m,n) &= \sum_{h \in G_{n-2}} \Lambda(h) \sum_g \frac{1}{q^{n-1}} \sum_\chi \chi(g)\bar{\chi}(h + aT^{n-1}) \\ &= \frac{1}{q^{n-1}} \sum_\chi (\sum_g \chi(g))(\sum_{h \in G_{n-2}} \Lambda(h)\bar{\chi}(h + aT^{n-1})), \end{aligned} \tag{5.6}$$

where g runs over all irreducible polynomials over $\mathbf{F}_q$ of degree m with constant term 1. By (2.17) and (5.5), we conclude that if $n > 2$, then

$$\begin{aligned} |W_a(m,n) - \frac{\pi_m}{q}| &< \frac{1}{m}(nq^{m/2} + 1)(n-2)q^{(n-2)/2} \\ &\leq \frac{1}{m}(n-1)^2 q^{(m+n-2)/2}. \end{aligned}$$

If $n = 2$, then (2.17) and (5.6) show that

$$|W_a(m,2) - \frac{\pi_m}{q}| < \frac{q-1}{q}\frac{1}{m}(2q^{m/2} + 1) < \frac{2}{m} q^{m/2}.$$

The proof is complete.

Corollary 5.5. *Let $a \in \mathbf{F}_q$. Let $m \geq n \geq 2$ be positive integers. If*

$$q^{m-n} \geq n^4,$$

then there is an irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of degree m with constant term 1 such that the coefficient of T^{n-1} is a.

Proof. By Theorem 5.4, one obtains that for $n > 2$,

$$|mqW_a(m,n) - q^m| < q(n-1)^2 q^{(m+n-2)/2} + 2q^{m/2} \leq qn^2 q^{(m+n-2)/2} = n^2 q^{(m+n)/2}.$$

This proves that $W_a(m,n) > 0$ if $q^{m-n} \geq n^4$. If $n = 2$, Theorem 5.4 gives

$$|mqW_a(m,2) - q^m| < (2q+2)q^{m/2} < q2^2 q^{m/2}.$$

This inequality shows that $W_a(m,2) > 0$ if $q^{m-2} \geq 2^4$. The corollary is proved.

Putting the above two corollaries together, we have

Corollary 5.6. *Let $m \geq n \geq 1$ be positive integers with $m \geq 3$. Let a be a given element in $\mathbf{F}_q$. (i). Assume $a \neq 0$. Then there exists a monic irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of degree m such that the coefficent of T^{n-1} in $g(T)$ is equal to a if*

$$\text{either} \quad q^{m-n-1} \geq n^4 \quad \text{or} \quad q^{n-2} \geq (m-n+2)^4. \tag{5.7}$$

(ii). Assume $a = 0$ and $n > 1$. Then there exists a monic irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of degree m such that the coefficent of T^{n-1} in $g(T)$ is equal to a if

$$\text{either} \quad q^{m-n} \geq n^4 \quad \text{or} \quad q^{n-2} \geq (m-n+2)^4. \tag{5.8}$$

Proof. A monic polynomial of the form $g(T) = T^m + a_{m-1}T^{m-1} + \cdots + a_n T^n + \cdots + a_0$ is irreducible of degree m (> 1) if and only if the reciprocal polynomial $g^*(T) = 1 + a_{m-1}T + \cdots + a_0 T^m$ is irreducible of degree m. The coefficient of T^{n-1} in $g(T)$ corresponds to the coefficient of T^{m-n+1} in $g^*(T)$. Corollaries 3.3 and 3.5 imply the result for the case $a \neq 0$. If $a = 0$, the transformation $g(T) \longrightarrow g^*(T)/g(0)$ shows that there is a monic irreducible polynomial of degree m with $a_{n-1} = 0$ if and only if there is a monic irreducible polynomial of degree m with $a_{m-n+1} = 0$. Corollary 3.5 then gives the result for the case $a = 0$. The proof is complete.

Corollary 5.7. *Let $m \geq n \geq 1$ be positive integers with $m \geq 3$. Let a be a given element in $\mathbf{F}_q$ with $a \neq 0$ if $n = 1$. Then, there exists a monic irreducible polynomial $g(T)$ over $\mathbf{F}_q$ of degree m such that the coefficent of T^{n-1} in $f(T)$ is equal to a if*

$$q^{m-3} \geq (\frac{m+2}{2})^8. \tag{5.9}$$

Proof. Multiplying the two inequalities in (5.7) and (5.8), one sees that it suffices to have

$$q^{m-3} \geq n^4(m-n+2)^4.$$

The worst case occurs when $n = m - n + 2 = (m+2)/2$. The proof is complete.

Inequality (5.9) is satisfied for all prime powers q if m is large. It is also satisfied for all $m > 3$ if q is large. To prove that there are only finitely many cases left, there remains the case $m = 3$ and $n > 1$. This case can be easily excluded by a simple argument as follows. Let $f(T)$ be a cubic monic polynomial over $\mathbf{F}_q$. It is easy to see that there is a monic irreducible cubic polynomial over $\mathbf{F}_q$ in the family $f(T) + t$ parametrized by t, if and only if $f(T)$ is not a permutation polynomial over $\mathbf{F}_q$. Actually, there are at least $(q-1)/3$ irreducible cubic polynomials in the family $f(T) + t$ if $f(T)$ is not a permutation polynomial over $\mathbf{F}_q$, see [Wa]. Thus, to have an irreducible polynomial of the form $T^3 + aT^2 + bT + c$ with given a, we can just choose $b \in \mathbf{F}_q$ such that $T^2 + aT + b$ has a non-zero root. This can clearly be done. Similarly, to have an irreducible polynomial of the form $T^3 + bT^2 + aT + c$ with given a, it suffices to choose $b \in \mathbf{F}_q$ such that $T^2 + bT + a$ has a non-zero root. Again, this can clearly be done.

Corollary 5.8. *If either $q > 19$ or $m \geq 36$, then the Hansen-Mullen conjecture is true.*

Proof. If $q = 2$, Corollary 5.3 shows that the first inequality in (5.7) can be improved. The worse case occurs in (5.8). Thus, it suffices to have

$$2^{m-2} \geq (\frac{m+2}{2})^8.$$

This inequality is satisfied if $m \geq 36$. If $q \geq 3$, inequality (5.9) is satisfied for $m \geq 22$.

Next we turn to proving the result for $q > 19$. We may assume that $m \geq 4$. If $m \geq 7$, inequality (5.9) is satisfied if $q \geq 21$ and hence if $q > 19$ since q is a prime power. There remain the three cases $4 \leq m \leq 6$. We will be implicitly using the transformations occuring in the proof of Corollary 5.6. Part (ii) of Theorem 5.2 and part (ii) of Theorem 5.4 show that the conjecture is true for all $m \geq 4$ if $n = 1$ or if $n = m$. Corollary 5.6 covers the case $n = 2$ if $q \geq 16$. The first estimate of Theorem 5.4 covers the case $n = m - 1$ if $q \geq 17$. This takes care of all possibilities if $m = 4$ and $q > 19$. For $m = 5$, there remains the possibility that $n = 3$ and $a \neq 0$. In this case, a direct estimate of (5.4) using the fact that there are $(q^5 - q)/5$ monic irreducible polynomials of degree 5 gives the following better bound:

$$|w_a(5,3) - \frac{q^5 - q}{5(q-1)}| \leq \frac{1}{5}(2q^{5/2} + q)2q.$$

We need to have

$$q^5 - q > (2q^{5/2} + q)2q(q-1).$$

The last inequality is satisfied if $q \geq 18$. For $m = 6$, there remain the two possibilities that $n = 3$ ($a \neq 0$) and $n = 4$. For $m = 6$ and $n = 3$, Corollary 5.6 shows that the conjecture is true if $q \geq 9$. For $m = 6$ and $n = 4$, Corollary 5.6 shows that the conjecture is true if $q \geq 16$. The proof is complete.

References

[BDS] E. Bach, J. Driscoll and J. Shallit, *Factor refinement*, J. Algorithm, 15(1993), 199-222.

[Ch] F.R. Chung, *Diameters and eigenvalues*, J. Amer. Math. Soc., 2(1989), 187-196.

[Co] S.D. Cohen, *Primitive elements and polynomials with arbitrary trace*, Discr. Math., 83(1990), 1-7.

[EH] G.W. Effinger and D.R. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford Science Publications, 1991.

[Ha1] W.B. Han, *Some Applications of Character Sums in Finite Fields and Coding Theory*, Ph.D. Dissertation, Sichuan University, 1994.

[Ha2] W.B. Han, *The coefficients of primitive polynomials over finite fields*, Math. Comp., 65(1996), no. 213, 331-340.

[HM] T. Hansen and G.L. Mullen, *Primitive polynomials over finite fields*, Math. Comp., 59(1992), 639-643.

[Ka] N. M. Katz, *An estimate for character sums*, J. Amer. Math. Soc., 2(1989), 197-200.

[Le1] H.W. Lenstra Jr., *Finding isomorphisms between finite fields*, Math. Comp., 56(1991), 329-347.

[Le2] H.W. Lenstra Jr., *Multiplicative groups generated by linear expressions*, unpublished notes.

[LS] H.W. Lenstra Jr. and R. Schoof, *Primitive normal bases for finite fields*, Math. Comp., 48(1987), 217-231.

[Li] W.C. Li, *Character sums and abelian Ramanujan graphs*, J. Number Theory, 41(1992), 199-217.

[Sh] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp., 58(1992), 369-380.

[Shp] I.E. Shparlinski, *Computational and Algorithmic Problems in Finite Fields*, Kluwer Academic Publishers, 1992.

[Wa] D. Wan, *A p-adic lifting lemma and its application to permutation polynomials*, in Finite Fields, Coding Theory and Advances in Communications and Computing, eds: G.L. Mullen and P.J.S. Shiue, Marcel Dekker, 1992, 209-216.

[We] A. Weil, *Basic Number Theory*, third edition, Springer-Verlag, 1974.