Canad. J. Math. Vol. 70 (6), 2018 pp. 1373–1389
http://dx.doi.org/10.4153/CJM-2017-022-1

A New Proof of the Hansen–Mullen Irreducibility Conjecture

Aleksandr Tuxanidy and Qiang Wang

Abstract. We give a new proof of the Hansen–Mullen irreducibility conjecture. The proof relies on an application of a (seemingly new) sufficient condition for the existence of elements of degree n in the support of functions on finite fields. This connection to irreducible polynomials is made via the least period of the discrete Fourier transform (DFT) of functions with values in finite fields. We exploit this relation and prove, in an elementary fashion, that a relevant function related to the DFT of characteristic elementary symmetric functions (that produce the coefficients of characteristic polynomials) satisfies a simple requirement on the least period. This bears a sharp contrast to previous techniques employed in the literature to tackle the existence of irreducible polynomials with prescribed coefficients.

1 Introduction

Let q be a power of a prime p, let $\mathbb{F}_q$ be the finite field with q elements, and let $n \geq 2$. Hansen and Mullen [18, Conjecture B] conjectured that, except for a few genuine exceptions, there exist irreducible (and more strongly primitive [18, Conjecture A]) polynomials of degree n over $\mathbb{F}_q$ with any *one* of its coefficients prescribed to any value. Wan [29] proved Conjecture B (appearing as Theorem 1.1) for $q > 19$ or $n \geq 36$, with the remaining cases being computationally verified soon after [16]. Building on some of the work of Fan–Han [12] on p-adic series, Cohen [8] proved that there exists a primitive polynomial of degree $n \geq 9$ over $\mathbb{F}_q$ with any one of its coefficients prescribed. The remaining cases of Conjecture A were settled by Cohen and Prešern [8–10] who also gave theoretical explanations for the small cases of q, n, missed out in Wan's original proof [29]. For a polynomial $h(x) \in \mathbb{F}_q[x]$ and an integer w, we denote by $[x^w]h(x)$ the coefficient of x^w in $h(x)$.

Theorem 1.1 *Let q be a power of a prime, let $c \in \mathbb{F}_q$, and let $n \geq 2$ and w be integers with $1 \leq w \leq n$. If $w = n$, assume that $c \neq 0$. If $(n, w, c) = (2, 1, 0)$, further assume q is odd. Then there exists a monic irreducible polynomial $P(x)$ of degree n over $\mathbb{F}_q$ with $[x^{n-w}]P(x) = c$.*

The Hansen–Mullen conjectures have since been generalized to encompass results on the existence of irreducible and particularly primitive polynomials with *several* prescribed coefficients (see [14, 15, 23, 25, 28] for general irreducibles and [7, 17, 26, 27]

Received by the editors April 27, 2016; revised June 19, 2016.
Published electronically June 14, 2018.
The research of Qiang Wang is partially supported by NSERC of Canada.
AMS subject classification: **11T06**.
Keywords: irreducible polynomial, primitive polynomial, Hansen–Mullen conjecture, symmetric function, q-symmetric, discrete Fourier transform, finite field .

for primitives). In particular Ha [15], building on some of the work of Pollack [25] and Bourgain [3], has recently proved that, for large enough q, n, there exist irreducibles of degree n over $\mathbb{F}_q$ with roughly any $n/4$ coefficients prescribed to any value. This seems to be the current record on the number of *arbitrary* coefficients one may prescribe to any values in an irreducible polynomial of degree n.

The above are existential results obtained through asymptotic estimates. However there is also intensive research on the exact number of irreducible polynomials with some prescribed coefficients. See for instance [5, 13, 20, 22] and references therein for some work in this area. See also [24] for primitives and N-free elements in special cases.

There are some differences in approach to tackling existence questions of either general irreducible or primitive polynomials with prescribed coefficients. For instance, when working on irreducibles, and following in the footsteps of Wan [29], it has been common practice to exploit the $\mathbb{F}_q[x]$-analogue of Dirichlet's theorem for primes in arithmetic progressions; all this is done via Dirichlet characters on $\mathbb{F}_q[x]$, L-series, zeta functions, etc. (see [28]). Recently Pollack [25] and Ha [15], building on some ideas of Bourgain [3], applied the circle method to prove the existence of irreducible polynomials with several prescribed coefficients. On the other hand, in the case of primitives, the problem is usually approached via p-adic rings or fields (to account for the inconvenience that Newton's identities "break down", in some sense, in fields of positive characteristic) together with Cohen's sieving lemma, Vinogradov's characteristic function, etc. [8,12]. However there is one common feature these methods share, namely, when bounding the "error" terms comprised of character sums, the function field analogue of Riemann's hypothesis (Weil's bound) is used (perhaps without exception here). Nevertheless, as a consequence of its $O(q^{n/2})$ nature, a difficulty arises in extending the $n/2$ threshold for the number of coefficients one can prescribe in irreducible or particularly primitive polynomials of degree n.

As the reader can take from all this, there seems to be a preponderance of the analytic methods to tackle the existence problem of irreducibles and primitives with several prescribed coefficients. One then naturally wonders whether other viewpoints may be useful for tackling such problems. As Panario points out [19, p. 115],

> The long-term goal here is to provide existence and counting results for irreducibles with any number of prescribed coefficients to any given values. This goal is completely out of reach at this time. Incremental steps seem doable, but it would be most interesting if new techniques were introduced to attack these problems.

In this work we take a different approach and give a new proof of the Hansen–Mullen irreducibility conjecture (or theorem) stated in Theorem 1.1. We attack the problem by studying the least period of certain functions related to the discrete Fourier transform (DFT) of characteristic elementary symmetric functions (which produce the coefficients of characteristic polynomials). This bears a sharp contrast to previous techniques in the literature. The proof theoretically explains, in a unified way, every case of the Hansen–Mullen conjecture. These include the small cases missed out in Wan's original proof [29] and computationally verified in [16]. However we should point out that, in contrast, our proof has the disadvantage of not yielding estimates for the number of irreducibles with a prescribed coefficient. It merely asserts their existence. We wonder whether some of the techniques introduced here can be extended to tackle the existence question for several prescribed coefficients, but for now we leave this to the consideration of the interested reader.

The proof relies on an application of the sufficient condition in Lemma 1.3, which follows from that of Lemma 1.2 (i). First for a primitive element ζ of $\mathbb{F}_q$ and a function $f:\mathbb{Z}_{q-1}\to\mathbb{F}_q$, the DFT of f based on ζ is the function $\mathcal{F}_\zeta[f]:\mathbb{Z}_{q-1}\to\mathbb{F}_q$ given by $\mathcal{F}_\zeta[f](m)=\sum_{j\in\mathbb{Z}_{q-1}} f(j)\zeta^{mj}$, $m\in\mathbb{Z}_{q-1}$. Here $\mathbb{Z}_{q-1}:=\mathbb{Z}/(q-1)\mathbb{Z}$. The inverse DFT is given by $\mathcal{F}_\zeta^{-1}[f]=-\mathcal{F}_{\zeta^{-1}}[f]$. For a function $g:\mathbb{Z}_{q-1}\to\mathbb{F}_q$, we say that g has least period r if r is the smallest positive integer such that $g(m+\overline{r})=g(m)$ for all $m\in\mathbb{Z}_{q-1}$. Let $\Phi_n(x)\in\mathbb{Z}[x]$ be the n-th cyclotomic polynomial. For a function F on a set A, let $\operatorname{supp}(F):=\{a\in A:\ F(a)\neq 0\}$ be the support of F. It should be observed that, in practice, F will be defined on a subset of the field $\mathbb{F}_{q^n}$ or on a set of integers. For example, both usages occur in the proof of Lemma 1.2

Lemma 1.2 *Assume ζ is a primitive element of $\mathbb{F}_{q^n}$ where q is a prime power and $n\geq 2$. Given a function $F:\mathbb{F}_{q^n}\to\mathbb{F}_{q^n}$, define $f:\mathbb{Z}_{q^n-1}\to\mathbb{F}_{q^n}$ by $f(k)=F(\zeta^k)$ and let r be the least period of $\mathcal{F}_\zeta[f]$ (which is the same as the least period of $\mathcal{F}_\zeta^{-1}[f]$). Then the following results hold.*

(i) *Suppose $r\nmid (q^n-1)/\Phi_n(q)$. Then $\operatorname{supp}(F)$ contains an element of degree n over $\mathbb{F}_q$.*
(ii) *Suppose $\operatorname{supp}(F)$ contains an element of degree n over $\mathbb{F}_q$. Then $r\nmid (q^d-1)$ for every positive divisor d of n with $d<n$.*
(iii) *Suppose $\operatorname{supp}(F)$ contains a primitive element of $\mathbb{F}_{q^n}$, or the least common multiple of the multiplicative orders of the elements in $\operatorname{supp}(F)$ equals q^n-1. Then $r=q^n-1$.*

In particular (i) implies the existence of an irreducible factor of degree n for any polynomial $h(x)\in\mathbb{F}_q[x]$ satisfying a constraint on the least period as follows. Here $\mathbb{F}_{q^n}^\times$ and $L^\times$ denote the set of all invertible elements in $\mathbb{F}_{q^n}$ and L, respectively. A cyclic sequence $(s_i)_0^{N-1}\in\mathbb{F}_q$ has period N because $s_{i+N}=s_i$ for all $i\geq 0$. We say that a periodic $(s_i)_{i=0}^{N-1}$ has least period r if r is the smallest positive integer such that $s_{i+r}=s_i$ for all $0\leq i\leq N-1$. If we define a function $f:\mathbb{Z}_{q^n-1}\to\mathbb{F}_q$ by $f(i)=s_i$ for $0\leq i\leq q^n-2$, then both f and $(s_i)_{i=0}^{q^n-2}$ have the same least period.

Lemma 1.3 *Let q be a prime power and $n\geq 2$. Suppose $h(x)\in\mathbb{F}_q[x]$ and L is any subfield of $\mathbb{F}_{q^n}$ containing the image $h(\mathbb{F}_{q^n}^\times)$. Define the polynomial*

$$S(x)=(1-h(x)^{\#L^\times}) \bmod (x^{q^n-1}-1)\in\mathbb{F}_q[x].$$

Write $S(x)=\sum_{i=0}^{q^n-2} s_i x^i$ for some coefficients $s_i\in\mathbb{F}_q$. If the cyclic sequence $(s_i)_{i=0}^{q^n-2}$ has least period r satisfying $r\nmid (q^n-1)/\Phi_n(q)$, then $h(x)$ has an irreducible factor of degree n over $\mathbb{F}_q$.

Lemma 1.3 immediately yields the following sufficient condition for a polynomial to be irreducible because $h(x)$ has an irreducible factor of the same degree.

Proposition 1.4 *With the notations of Lemma 1.3, assume $h(x) \in \mathbb{F}_q[x]$ has degree $n \geq 2$. If the cyclic sequence $(s_i)_{i=0}^{q^n-2}$ of the coefficients of $S(x)$ has least period r satisfying $r \nmid (q^n-1)/\Phi_n(q)$, then $h(x)$ is irreducible.*

We present the following small example to give the reader a flavor of the essence of our proof as an application of Lemma 1.3.

Example 1.5 Let $q = 2$, $n = 4$, and

$$h(x) = \sum_{0 \leq i_1 < i_2 \leq 3} x^{2^{i_1}+2^{i_2}} = x^{12} + x^{10} + x^9 + x^6 + x^5 + x^3 \in \mathbb{F}_2[x].$$

Note that $h(\mathbb{F}_{2^4}) \subseteq \mathbb{F}_2$. In fact, for any $\xi \in \mathbb{F}_{2^4}$, $h(\xi)$ is the coefficient of x^2 in the characteristic polynomial of degree 4 over $\mathbb{F}_2$ with root ξ. We may take $L = \mathbb{F}_2$ in Lemma 1.3; hence $\#L^\times = 1$. Thus

$$\begin{aligned} S(x) &:= (1 + h(x)^{\#L^\times}) \bmod (x^{2^4-1}+1) = h(x) + 1 \\ &= x^{12} + x^{10} + x^9 + x^6 + x^5 + x^3 + 1 \in \mathbb{F}_2[x]. \end{aligned}$$

The cyclic sequence of coefficients $\mathbf{s} = s_0, s_1, \ldots, s_{2^4-2}$ of $S(x) = \sum_{i=0}^{2^4-2} s_i x^i$ is given by $\mathbf{s} = 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0$. One can easily check that the least period r of $\mathbf{s}$ is $r = 2^4 - 1$, the maximum possible. Because $2^4 - 1 > (2^4-1)/\Phi_4(2)$, Lemma 1.3 implies that $h(x)$ has an irreducible factor $P(x)$ of degree 4 over $\mathbb{F}_2$. Any root ξ of $P(x)$ must satisfy $h(\xi) = 0$. This is the coefficient of x^2 in $P(x)$. Hence there exists an irreducible polynomial of degree 4 over $\mathbb{F}_2$ with its coefficient of x^2 being zero. Indeed, $x^4 + x + 1$ is one such irreducible polynomial.

The rest of this work goes as follows. In Section 2 we review some preliminary concepts regarding the DFT on finite fields, convolution, least period of functions on cyclic groups, and cyclotomic polynomials. In Section 3 we study the connection between the least period of the DFT of functions and irreducible polynomials. In particular, we explicitly describe in Proposition 3.1 the least period of the DFT of functions, as well as prove Lemmas 1.2 and 1.3. In Section 4 we introduce the characteristic delta functions as the DFTs of characteristic elementary symmetric functions. We then apply Lemma 1.3 to give a sufficient condition in Lemma 4.2 for the existence of an irreducible polynomial with any one of its coefficients prescribed. This is given in terms of the least period of a certain function $\Delta_{w,c}$, closely related to the delta functions. We also review some basic results on q-symmetric functions and their convolutions; this will be needed in Section 5. Finally in Section 5 we prove that the $\Delta_{w,c}$ functions have periods that are not divisors of $(q^n-1)/\Phi_n(q)$ (and are sufficiently large in many cases). The proof of Theorem 1.1 then immediately follows from this.

2 Preliminaries

We recall some preliminary concepts regarding the DFT for finite fields, convolution, least period of functions on cyclic groups, and cyclotomic polynomials.

Let q be a power of a prime p, let $N \in \mathbb{N}$ such that $N \mid q-1$, and let ζ_N be a primitive N-th root of unity in $\mathbb{F}_q^*$ (the condition on N guarantees the existence of ζ_N). We shall use the common notation $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. Now the DFT based on ζ_N, on the $\mathbb{F}_q$-vector space of functions $f: \mathbb{Z}_N \to \mathbb{F}_q$, is defined by $\mathcal{F}_{\zeta_N}[f](i) = \sum_{j \in \mathbb{Z}_N} f(j)\zeta_N^{ij}$, for all $i \in \mathbb{Z}_N$. Note that $\mathcal{F}_{\zeta_N}$ is a bijective linear operator with inverse given by $\mathcal{F}_{\zeta_N}^{-1} = N^{-1}\mathcal{F}_{\zeta_N^{-1}}$. For $f, g: \mathbb{Z}_N \to \mathbb{F}_q$, the convolution of f, g is the function $f \otimes g: \mathbb{Z}_N \to \mathbb{F}_q$ given by

$$(f \otimes g)(i) = \sum_{\substack{j+k=i \\ j,k \in \mathbb{Z}_N}} f(j)g(k).$$

Inductively, $f_1 \otimes f_2 \otimes \cdots \otimes f_k = f_1 \otimes (f_2 \otimes \cdots \otimes f_k)$ and so

$$(f_1 \otimes \cdots \otimes f_k)(i) = \sum_{\substack{j_1+\cdots+j_k=i \\ j_1,\ldots,j_k \in \mathbb{Z}_N}} f_1(j_1)\cdots f_k(j_k).$$

For $m \in \mathbb{N}$, we let $f^{\otimes m}$ denote the m-th convolution power of f, that is, the convolution of f with itself, m times. The DFT and convolution are related by the fact that $\prod_{i=1}^k \mathcal{F}_{\zeta_N}[f_i] = \mathcal{F}_{\zeta_N}\big[\bigotimes_{i=1}^k f_i\big]$. Since $f, \mathcal{F}_{\zeta_N}[f]$, have values in $\mathbb{F}_q$ by definition, it follows from the relation above that $f^{\otimes q} = f$. The convolution is associative, commutative, and distributive with identity $\delta_0: \mathbb{Z}_N \to \{0,1\} \subseteq \mathbb{F}_p$, the Kronecker delta function defined by $\delta_0(i) = 1$ if $i = 0$, and $\delta_0(i) = 0$ otherwise. We set $f^{\otimes 0} = \delta_0$.

Next we recall the concepts of a period and least period of a function $f: \mathbb{Z}_N \to \mathbb{F}_q$. For $r \in \mathbb{N}$, we say that f is *r-periodic* if $f(i) = f(i + \overline{r})$ for all $i \in \mathbb{Z}_N$. Clearly f is r-periodic if and only if it is $\gcd(r, N)$-periodic. The smallest such positive integer r is called the *least period* of f. Note the least period r satisfies $r \mid R$ whenever f is R-periodic. If the least period of f is N, we say that f has *maximum least period*.

There are various operations on cyclic functions which preserve the least period. For instance the *k-shift* function $f_k(i) := f(i+k)$ of f has the same least period as f. The *reversal* function $f^*(i) := f(-(1+i))$ of f also has the same least period. Let σ be a permutation of $\mathbb{F}_q$. The function $f^\sigma(i) := \sigma(f(i))$ keeps the least period of f as well.

Next we recall a few elementary facts about cyclotomic polynomials. For $n \in \mathbb{N}$, the n-th cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is defined by

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^k),$$

where $\zeta_n \in \mathbb{C}$ is a primitive n-th root of unity and $(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the unit group modulo n. Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$, the Möbius inversion formula gives $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$, where μ is the Möbius function.

For any divisor m of n, with $0 < m < n$, we note that

$$\frac{x^n - 1}{x^m - 1} = \frac{\prod_{d|n} \Phi_d(x)}{\prod_{d|m} \Phi_d(x)} = \prod_{\substack{d|n \\ d\nmid m}} \Phi_d(x).$$

Hence

$$\Phi_n(x) \;\Big|\; \frac{x^n - 1}{x^m - 1} \in \mathbb{Z}[x]. \tag{2.1}$$

In fact, one can show that for $n \geq 2$,

$$\Phi_n(q) = \gcd\Big\{ \frac{q^n - 1}{q^d - 1} : 1 \leq d \mid n,\ d < n \Big\}$$

and so $\frac{q^n-1}{\Phi_n(q)} = \operatorname{lcm}\{q^d - 1 : 1 \leq d \mid n,\ d < n\}$.

Note also that

$$\Phi_n(q) = |\Phi_n(q)| = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} |q - \zeta_n^k| > q - 1 \tag{2.2}$$

for $n \geq 2$, since $|q - \zeta_n^k| > q - 1$ for any primitive n-th root $\zeta_n^k \in \mathbb{C}$, whenever $n \geq 2$ (as can be seen geometrically by looking at the complex plane) [1].

3 Least Period of the DFT and Connection to Irreducible Polynomials

In this section we study a connection between the least period of the DFT of a function and irreducible polynomials. We start off by giving an explicit formula in Proposition 3.1 for the least period of the DFT of a function $f : \mathbb{Z}_N \to \mathbb{F}_q$ in terms of the values in its support. Then we prove Lemmas 1.2 and 1.3.

First we can identify, in the usual way, elements of $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ with their canonical representatives in $\mathbb{Z}$ and vice versa. In particular this endows $\mathbb{Z}_N$ with the natural ordering in $\mathbb{Z}$. We sometimes also abuse notation and write $a \mid \overline{b}$ for $a \in \mathbb{Z}$ and $\overline{b} \in \mathbb{Z}_N$ to state that a divides the canonical representative of $\overline{b}$, and write $a \nmid \overline{b}$ to state the opposite. For an integer k and a non-empty set $A = \{a_1, \ldots, a_s\}$, we write $\gcd(k, A) := \gcd(k, a_1, \ldots, a_s)$.

Proposition 3.1 *Let q be a power of a prime, $N \mid q - 1$, $f : \mathbb{Z}_N \to \mathbb{F}_q$, and let ζ_N be a primitive N-th root of unity in $\mathbb{F}_q^*$. The least period of $\mathcal{F}_{\zeta_N}[f]$ and $\mathcal{F}_{\zeta_N}^{-1}[f]$ is given by $N/\gcd(N, \operatorname{supp}(f))$.*

Proof Note that $d := N/\gcd(N, \operatorname{supp}(f))$ is the smallest positive divisor of N with the property that N/d divides every element in $\operatorname{supp}(f)$. For the sake of brevity write $\widehat{f} = \mathcal{F}_{\zeta_N}[f]$. Now for $i \in \mathbb{Z}_N$, note that

$$\widehat{f}(i + d) = \sum_{j \in \mathbb{Z}_N} f(j)\zeta_N^{(i+d)j} = \sum_{k=0}^{d-1} f\Big(\frac{N}{d}k\Big)\zeta_N^{(i+d)\frac{N}{d}k} = \sum_{k=0}^{d-1} f\Big(\frac{N}{d}k\Big)\zeta_N^{i\frac{N}{d}k} = \widehat{f}(i).$$

Thus if r is the least period of $\widehat{f}$, necessarily $r \leq d$.

[1]The elementary facts in (2.1) and (2.2) have some historical significance. For instance, these make an appearance in Witt's classical proof of Wedderburn's theorem that every finite division ring is a field (see [1, Chapter 5] for example).

Since $f = \mathcal{F}_{\zeta_N}^{-1}[\widehat{f}]$, then $f(i) = N^{-1}\sum_{j\in\mathbb{Z}_N}\widehat{f}(j)\zeta_N^{-ij}$, $i \in \mathbb{Z}_N$. Hence for $i \in \mathbb{Z}_N$, we have

$$\begin{aligned}
Nf(i) &= \sum_{j\in\mathbb{Z}_N}\widehat{f}(j)\zeta_N^{-ij} = \sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij} + \sum_{j=r}^{2r-1}\widehat{f}(j)\zeta_N^{-ij} + \cdots + \sum_{j=(\frac{N}{r}-1)r}^{N-1}\widehat{f}(j)\zeta_N^{-ij}\\
&= \sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij} + \sum_{j=0}^{r-1}\widehat{f}(j+r)\zeta_N^{-i(j+r)} + \cdots + \sum_{j=0}^{r-1}\widehat{f}\Big(j+\Big(\frac{N}{r}-1\Big)r\Big)\zeta_N^{-i(j+(\frac{N}{r}-1)r)}\\
&= \sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij} + \zeta_N^{-ir}\sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij} + \cdots + \zeta_N^{-i(\frac{N}{r}-1)r}\sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij}\\
&= \sum_{k=0}^{\frac{N}{r}-1}\zeta_N^{-irk}\sum_{j=0}^{r-1}\widehat{f}(j)\zeta_N^{-ij}.
\end{aligned}$$

If $\frac{N}{r} \nmid i$, then $\zeta_N^{-ir} \neq 1$ and $\sum_{k=0}^{\frac{N}{r}-1}\zeta_N^{-irk} = \frac{\zeta_N^{-iN}-1}{\zeta_N^{-ir}-1} = 0$. It follows that $f(i) = 0$ whenever $\frac{N}{r} \nmid i$. Equivalently, if $f(i) \neq 0$, then $\frac{N}{r} \mid i$. Now the minimality of d implies that $d \le r$. But $r \le d$ (see above) now yields $r = d$.

With regards to the least period of $\mathcal{F}_{\zeta_N}^{-1}[f]$, we know that $\mathcal{F}_{\zeta_N}^{-1}[f] = N^{-1}\mathcal{F}_{\zeta_N^{-1}}[f]$. Since ζ_N^{-1} is a primitive N-th root of unity in $\mathbb{F}_q^*$ as well, the previous arguments similarly imply that $\mathcal{F}_{\zeta_N^{-1}}[f]$ has the least period d. Then so does the function $N^{-1}\mathcal{F}_{\zeta_N^{-1}}[f]$, a non-zero scalar multiple of $\mathcal{F}_{\zeta_N^{-1}}[f]$. ∎

In particular, if ζ is primitive in $\mathbb{F}_q$ and $F(x) = \sum_{i\in I} a_i x^i \in \mathbb{F}_q[x]$ for some subset $I \subseteq [0, q-2]$ of integers with each $a_i \neq 0$, $i \in I$, then the least period of the $(q-1)$-periodic sequence $(F(\zeta^i))_{i\ge 0}$ is given by $(q-1)/\gcd(q-1, I)$. We now prove Lemma 1.2.

Proof of Lemma 1.2 (i) On the contrary, suppose that $\operatorname{supp}(F)$ contains no element of degree n over $\mathbb{F}_q$. Then for each $m \in \operatorname{supp}(f)$ there exists a proper divisor d of n with $(q^n-1)/(q^d-1) \mid m$. Since $\Phi_n(q) \mid (q^n-1)/(q^d-1)$ for all proper divisors d of n, then $\Phi_n(q) \mid m$ for all $m \in \operatorname{supp}(f)$. Thus for all $k \in \mathbb{Z}_{q^n-1}$,

$$\widehat{f}(k) = \sum_{j\in\mathbb{Z}_{q^n-1}} f(j)\zeta^{kj} = \sum_{a=1}^{(q^n-1)/\Phi_n(q)} f(a\Phi_n(q))\zeta^{ka\Phi_n(q)},$$

where $\widehat{f} = \mathcal{F}_\zeta[f]$. Note that $\widehat{f}(k + (q^n-1)/\Phi_n(q)) = \widehat{f}(k)$ for all $k \in \mathbb{Z}_{q^n-1}$. Thus $\widehat{f}$ is $\frac{q^n-1}{\Phi_n(q)}$-periodic. Necessarily the least period of $\widehat{f}$ divides $\frac{q^n-1}{\Phi_n(q)}$, a contradiction.

(ii) Assume $\operatorname{supp}(F)$ contains an element of degree n over $\mathbb{F}_q$. Then there exists $m \in \operatorname{supp}(f)$ with $(q^n-1)/(q^d-1) \nmid m$ for all proper divisors d of n. Let r be the least period of $\widehat{f}$. By Proposition 3.1, $(q^n-1)/r \mid m$. Since $(q^n-1)/(q^d-1) \nmid m$, then $r \nmid q^d - 1$ for all proper divisors d of n.

(iii) Assume $\operatorname{supp}(F)$ contains a primitive element of $\mathbb{F}_{q^n}$. Then there exists k relatively prime to q^n-1 such that $\overline{k} \in \operatorname{supp}(f)$. Thus, $(\mathbb{Z}/(q^n-1)\mathbb{Z})^\times \cap \operatorname{supp}(f) \neq \varnothing$. It follows from Proposition 3.1 that both $\mathcal{F}_\zeta[f]$ and $\mathcal{F}_\zeta^{-1}[f]$ have maximum least period q^n-1. The second part follows similarly. ∎

Note that, as the following three examples show, the sufficient (respectively, necessary) conditions in Lemma 1.2 are not necessary (respectively, sufficient). These may possibly be improved in accordance with the needs of whomever wishes to apply these tools. Let us start off by showing that the sufficient condition in (i) is not necessary.

Example 3.2 Recall that $(q^n-1)/\Phi_n(q) = \operatorname{lcm}\{q^d-1 : d \mid n,\ d<n\}$. Pick any n with at least two prime factors. Then $(q^n-1)/\Phi_n(q) \nmid q^d-1$ for all $d \mid n, d<n$. Thus $\zeta^{\Phi_n(q)}$ is of degree n over $\mathbb{F}_q$. Define the function $F\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ by $F(\zeta^{\Phi_n(q)}) = 1$ and $F(\xi) = 0$ for all other elements $\xi \in \mathbb{F}_{q^n}$. Thus $\operatorname{supp}(F)$ contains an element of degree n over $\mathbb{F}_q$. The associate function $f\colon \mathbb{Z}_{q^n-1} \to \mathbb{F}_{q^n}$ is defined by $f(k)=1$ if $k=\Phi_n(q)$ and $f(k)=0$ otherwise. By Proposition 3.1, the least period r of $\mathcal{F}_\zeta[f]$ is the smallest positive divisor of q^n-1 such that $(q^n-1)/r \mid \Phi_n(q)$, since $\operatorname{supp}(f) = \{\Phi_n(q)\}$. This is $r = (q^n-1)/\Phi_n(q)$. Thus we obtain an example of a function which contains an element of degree n over $\mathbb{F}_q$ in its support, but for which the corresponding least period is a divisor of $(q^n-1)/\Phi_n(q)$.

The following example shows that the necessary condition in (ii) is not sufficient.

Example 3.3 Similarly as before, pick any n with at least two prime factors. Then $(q^n-1)/\Phi_n(q) \nmid q^d-1$ for all $d \mid n, d<n$. Define $F\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ by $F(\zeta^k)=1$ if $k = (q^n-1)/(q^d-1)$ for some $d \mid n, d<n$, and $F(\xi)=0$ for all other elements $\xi \in \mathbb{F}_{q^n}$. Thus $\operatorname{supp}(F)$ has no element of degree n over $\mathbb{F}_q$. This defines the associate function $f\colon \mathbb{Z}_{q^n-1} \to \mathbb{F}_{q^n}$ of F with

$$\operatorname{supp}(f) = \{(q^n-1)/(q^d-1) : d \mid n,\ d<n\}.$$

Consider the smallest positive divisor r of q^n-1, with $(q^n-1)/r \mid (q^n-1)/(q^d-1)$ for all proper divisors d of n. Note that r is divisible by each q^d-1, for $d \mid n, d<n$; it follows that $r = \operatorname{lcm}\{q^d-1 : d \mid n,\ d<n\} = (q^n-1)/\Phi_n(q)$ with $r \nmid q^d-1$ for all $d \mid n, d<n$. By Proposition 3.1, $r = (q^n-1)/\Phi_n(q)$ is the least period of $\mathcal{F}_\zeta[f]$. Thus we have constructed a function F with $\operatorname{supp}(F)$ having no element of degree n over $\mathbb{F}_q$ but for which the corresponding least period r satisfies $r \nmid (q^d-1)$ for all $d \mid n$, $d<n$.

This last example shows that the necessary condition in (iii) is not sufficient.

Example 3.4 Pick q, n such that q^n-1 has at least two non-trivial relatively prime divisors, say $a, b > 1$ with $a, b \mid (q^n-1)$ and $\gcd(a,b)=1$. The smallest positive divisor r of q^n-1 with $(q^n-1)/r \mid a, b$ is $r = q^n-1$. Now we note that the function $F\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined by $F(\zeta^a) = F(\zeta^b) = 1$ and $F(\xi)=0$ for all other elements ξ of $\mathbb{F}_{q^n}$, contains no primitive element in its support, but the corresponding least period of $\mathcal{F}_\zeta[f]$ is q^n-1, by Proposition 3.1.

Remark 3.5 We note that Example 3.4 together with Lemma 1.2 (i) imply that for any such a, b, there exists $k \in \{a,b\}$ such that $(q^n-1)/(q^d-1) \nmid k$ for all proper divisors d of n, *i.e.*, either ζ^a or ζ^b (or both) is an element of degree n over $\mathbb{F}_q$. This may also have applications in determining whether a polynomial $h(x) \in \mathbb{F}_q[x]$ has an irreducible factor of degree n. Specifically, if there exist divisors $a, b \geq 1$ of $q^n - 1$ with $\gcd(a, b) = 1$ and $h(\zeta^a) = h(\zeta^b) = 0$, then $h(x)$ has an irreducible factor of degree n.

Proof of Lemma 1.3 As a function on $\mathbb{F}_{q^n}^\times$, note that

$$S(\xi) = \begin{cases} 1 & \text{if } h(\xi) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Let ζ be a primitive element of $\mathbb{F}_{q^n}$ and define the function $f\colon \mathbb{Z}_{q^n-1} \to \mathbb{F}_q$ by $f(m) = s_m$. Thus f has least period r satisfying $r \nmid (q^n - 1)/\Phi_n(q)$. Note that $S(\zeta^i) = \sum_j s_j \zeta^{ij} = \sum_j f(j)\zeta^{ij} = \mathcal{F}_\zeta[f](i)$ for each $i \in \mathbb{Z}_{q^n-1}$. Since $\mathcal{F}_\zeta[S]$ has the same period as $\mathcal{F}_\zeta^{-1}[S]$ (the inverse is essentially a Fourier multiplied by a non-zero scalar), then by the criteria of Lemma 1.2 (i), there exists an element of degree n over $\mathbb{F}_q$ in the support of S. It follows that $h(x)$ has a root of degree n over $\mathbb{F}_q$ and hence has an irreducible factor of degree n over $\mathbb{F}_q$. ∎

4 Characteristic Elementary Symmetric and Delta Functions

In this section we apply Lemma 1.3 for the purposes of studying coefficients of irreducible polynomials. We first place the characteristic elementary symmetric functions in the context of their DFT, which we shall refer to here simply as delta functions. These delta functions are indicators, with values in a finite field, for sets of values in $\mathbb{Z}_{q^n-1}$ whose canonical integer representatives have certain Hamming weights in their q-adic representation and q-digits all belonging to the set $\{0, 1\}$. Essentially, characteristic elementary symmetric functions are characteristic generating functions of the sets that the delta functions indicate. Then in Lemma 4.2 we give sufficient conditions for an irreducible polynomial to have a prescribed coefficient. Because the delta functions are q-symmetric (see Definition 4.3), we also review some useful facts needed in Section 5.

For $\xi \in \mathbb{F}_{q^n}$, the characteristic polynomial $h_\xi(x) \in \mathbb{F}_q[x]$ of degree n over $\mathbb{F}_q$ with root ξ is given by $h_\xi(x) = \prod_{k=0}^{n-1}(x - \xi^{q^k}) = \sum_{w=0}^{n}(-1)^w \sigma_w(\xi)x^{n-w}$, where for $0 \leq w \leq n$, $\sigma_w(x) \in \mathbb{F}_q[x]$ is the *characteristic elementary symmetric* polynomial given by $\sigma_0(x) = 1$ and $\sigma_w(x) = \sum_{0 \leq i_1 < \cdots < i_w \leq n-1} x^{q^{i_1} + \cdots + q^{i_w}}$, for $1 \leq w \leq n$. In particular $\sigma_1 = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the (linear) trace function and $\sigma_n = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the (multiplicative) norm function. Whenever $q = 2$ and $\xi \neq 0$, then $\sigma_0(\xi) = \sigma_n(\xi) = 1$ always. If $\xi \neq 0$, then (in general) $h_{\xi^{-1}}(x) = (-1)^n \sigma_n(\xi^{-1}) x^n h_\xi(1/x) = h_\xi^*(x)$, where $h_\xi^*(x)$ is the (monic) *reciprocal* of $h_\xi(x)$. Thus $\sigma_w(\xi) = \sigma_n(\xi)\sigma_{n-w}(\xi^{-1})$. Clearly $h_\xi(x)$ is irreducible if and only if so is $h_\xi^*(x)$. This occurs if and only if $\deg_{\mathbb{F}_q}(\xi) = n$.

Next we introduce the characteristic delta functions and the sets they indicate. But first let us clarify some ambiguity in our notation. For $a, b \in \mathbb{Z}$, we denote by $a \bmod b$ the remainder of division of a by b. That is, $a \bmod b$ is the smallest integer c in $\{0, 1, \dots, b-1\}$ that is congruent to a modulo b, and write $c = a \bmod b$. Similarly if $\overline{a} = a + b\mathbb{Z}$ is an element of $\mathbb{Z}_b$, we use the notation $\overline{a} \bmod b := a \bmod b$ to express the canonical representative of $\overline{a}$ in $\mathbb{Z}$. But we keep the usual notation $k \equiv a \pmod{b}$ to state that $b \mid (k - a)$.

https://doi.org/10.4153/CJM-2017-022-1 Published online by Cambridge University Press

We can represent $a \in \mathbb{Z}_{q^n-1}$ uniquely by the q-adic representation $(a_0, \dots, a_{n-1})_q = \sum_{i=0}^{n-1} a_i q^i$, with each $0 \le a_i \le q-1$, of the canonical representative of a in

$$\{0, 1, \dots, q^n - 2\} \subset \mathbb{Z}.$$

For convenience, we write $a = (a_0, \dots, a_{n-1})_q$. For $w \in [0, n] := \{0, 1, \dots, n\}$, define the sets $\Omega(w) \subseteq \mathbb{Z}_{q^n-1}$ by $\Omega(0) = \{0\}$ and

$$\Omega(w) = \left\{ k \in \mathbb{Z}_{q^n-1} : k \bmod (q^n - 1) = q^{i_1} + \cdots + q^{i_w},\ 0 \le i_1 < \cdots < i_w \le n-1 \right\}$$

for $1 \le w \le n$. That is, $\Omega(w)$ consists of all the elements $k \in \mathbb{Z}_{q^n-1}$ whose canonical representatives in $\{0, 1, \dots, q^n - 2\} \subset \mathbb{Z}$ have Hamming weight w in their q-adic representation $(a_0, \dots, a_{n-1})_q = \sum_{i=0}^{n-1} a_i q^i$, with each $a_i \in \{0, 1\}$. Note this last condition that each $a_i \in \{0, 1\}$ is automatically redundant when $q = 2$, since in general each $a_i \in [0, q-1]$ in the q-adic representation $t = (a_0, \dots, a_m)_q$ of a non-negative integer $t = \sum_{i=0}^{m} a_i q^i$.

When $q = 2$, note that $\Omega(n) = \varnothing$ since there is no integer in $\{0, 1, \dots, 2^n - 2\}$ with Hamming weight n in its binary representation. Observe also that $|\Omega(w)| = binomnw$ for each $0 \le w \le n$, unless $(q, w) = (2, n)$. Moreover, $\Omega(v) \cap \Omega(w) = \varnothing$ whenever $v \ne w$ by the uniqueness of base representation of integers. For $w \in [0, n]$, define the characteristic (finite field valued) function $\delta_w : \mathbb{Z}_{q^n-1} \to \mathbb{F}_p$ of the set $\Omega(w)$ by

$$\delta_w(k) = \begin{cases} 1 & \text{if } k \in \Omega(w), \\ 0 & \text{otherwise.} \end{cases}$$

Note that our δ_0 is the Kronecker delta function on $\mathbb{Z}_{q^n-1}$ with values in $\{0, 1\} \subseteq \mathbb{F}_p$.

Lemma 4.1 *Let ζ be a primitive element of $\mathbb{F}_{q^n}$ and let $w \in [0, n]$. If $q = 2$, further assume that $w \ne n$. Then $\sigma_w(\zeta^k) = \mathcal{F}_\zeta[\delta_w](k)$, $k \in \mathbb{Z}_{q^n-1}$.*

Proof Note $\sigma_0(\zeta^k) = 1$ for each k and so $\sigma_0(\zeta^k) = \mathcal{F}_\zeta[\delta_0](k)$. Now let $1 \le w \le n$. By definition and the assumption that $(q, w) \ne (2, n)$, we have

$$\sigma_w(\zeta^k) = \sum_{0 \le i_1 < \cdots < i_w \le n-1} \zeta^{k(q^{i_1} + \cdots + q^{i_w})} = \sum_{j \in \mathbb{Z}_{q^n-1}} \delta_w(j) \zeta^{kj} = \mathcal{F}_\zeta[\delta_w](k). \qquad \blacksquare$$

These functions are related to various mathematical objects in the literature. Let $m < q$, let $r_1, \dots, r_m \in [1, n-1]$, and let $c_0, \dots, c_{n-1} \in [0, m-1]$ such that $\sum_{i=1}^{m} r_i = \sum_{j=0}^{n-1} c_j$. View each $\delta_{r_1}, \dots, \delta_{r_m}$ as having values in $\mathbb{Z}$. Then one can show that

$$\delta_{r_1} \otimes \cdots \otimes \delta_{r_m}((c_0, \dots, c_{n-1})_q)$$

is the number of $m \times n$ matrices, with entries in $\{0, 1\} \subset \mathbb{Z}$, such that the sum of the entries in row i, $1 \le i \le m$, is r_i, and the sum of the entries in column j, $0 \le j \le n-1$, is c_j. Matrices with 0–1 entries and prescribed row and column sums are classical objects appearing in numerous branches of pure and applied mathematics, such as combinatorics, algebra and statistics. See the surveys in [2] and [21, Chapter 16].

An application of Lemma 1.3 yields the following sufficient condition for the existence of irreducible polynomials with a prescribed coefficient.

Lemma 4.2 *Fix a prime power q and integers $n \geq 2$ and $1 \leq w \leq n$. Fix $c \in \mathbb{F}_q$. If $q = 2$, further assume that $w \neq n$. If the function $\Delta_{w,c}: \mathbb{Z}_{q^n-1} \to \mathbb{F}_q$ given by*

$$\Delta_{w,c} = \delta_0 - ((-1)^w \delta_w - c\delta_0)^{\otimes(q-1)}$$

has least period r satisfying $r \nmid (q^n - 1)/\Phi_n(q)$, then there exists an irreducible polynomial $P(x)$ of degree n over $\mathbb{F}_q$ with $[x^{n-w}]P(x) = c$.

Proof Take $h(x) = (-1)^w \sigma_w(x) - c \in \mathbb{F}_q[x]$ in Lemma 1.3. Since $\sigma_w(\mathbb{F}_{q^n}) \subseteq \mathbb{F}_q$, we can pick $L = \mathbb{F}_q$. Thus $S(x) \in \mathbb{F}_q[x]$ is given by

$$S(x) = [1 - ((-1)^w \sigma_w(x) - c)^{q-1}] \bmod (x^{q^n-1} - 1).$$

Let ζ be a primitive element of $\mathbb{F}_{q^n}$. By Lemma 4.1, the linearity of the DFT, and the fact that $c = \mathcal{F}_\zeta[c\delta_0]$, we have

$$S(\zeta^i) = 1 - ((-1)^w \sigma_w(\zeta^i) - c)^{q-1} = \mathcal{F}_\zeta[\delta_0](i) - (\mathcal{F}_\zeta[(-1)^w \delta_w - c\delta_0](i))^{q-1}.$$

Since the product of DFTs is the DFT of the convolution, then as a function on $\mathbb{F}_{q^n}$

$$\begin{aligned} S &= \mathcal{F}_\zeta[\delta_0] - \mathcal{F}_\zeta\Big[\big((-1)^w \delta_w - c\delta_0\big)^{\otimes(q-1)}\Big] = \mathcal{F}_\zeta\Big[\delta_0 - \big((-1)^w \delta_w - c\delta_0\big)^{\otimes(q-1)}\Big] \\ &= \mathcal{F}_\zeta[\Delta_{w,c}]. \end{aligned}$$

Thus $S(\zeta^m) = \sum_{i=0}^{q^n-2} \Delta_{w,c}(i)\zeta^{mi}$ for each $m \in \mathbb{Z}_{q^n-1}$. As $S(x)$ is already reduced modulo $x^{q^n-1}-1$, it follows (from the uniqueness of the DFT of a function) that $S(x) = \sum_{i=0}^{q^n-2} \Delta_{w,c}(i)x^i$. Since the least period of $\Delta_{w,c}$ is not a divisor of $(q^n-1)/\Phi_n(q)$ by assumption, Lemma 1.3 implies $h(x)$ has an irreducible factor $P(x)$ of degree n over $\mathbb{F}_q$. Any of the roots ξ of $P(x)$ must satisfy $h(\xi) = 0$, that is, $(-1)^w \sigma_w(\xi) = c$. This is the coefficient of x^{n-w} in $P(x)$. Hence $[x^{n-w}]P(x) = c$ with $P(x)$ irreducible of degree n over $\mathbb{F}_q$. ∎

Note that the delta functions also satisfy the property that

$$\delta_w((a_0, \ldots, a_{n-1})_q) = \delta_w((a_{\rho(0)}, \ldots, a_{\rho(n-1)})_q) \tag{4.1}$$

for every permutation ρ of the indices in $[0, n-1]$. In particular such functions have a natural well-studied dyadic analogue in the *symmetric Boolean* functions. These are Boolean functions $f: \mathbb{F}_2^n \to \mathbb{F}_2$ with the property that

$$f(x_0, \ldots, x_{n-1}) = f(x_{\rho(0)}, \ldots, x_{\rho(n-1)})$$

for every permutation $\rho \in \mathcal{S}_{[0,n-1]}$; hence the value of $f(x_0, \ldots, x_{n-1})$ depends only on the Hamming weight of $(x_0, \ldots, x_{n-1})$. (See [4, 6] for some works on symmetric Boolean functions.) Nevertheless in our case the domain of these δ_w functions is $\mathbb{Z}_{q^n-1}$ rather than $\mathbb{F}_2^n$. Although one may still represent the elements of $\mathbb{Z}_{q^n-1}$ as n-tuples, say by using the natural q-adic representation, the arithmetic here is not as nice as in $\mathbb{F}_2^n$. One must consider the possibility that a "carry" may occur when adding or subtracting (this can make things quite chaotic) and also worry about reduction modulo $q^n - 1$ (although this is much easier to deal with). These issues will come up again in the following section. The symmetry property in (4.1) of δ_w and of its convolutions will be exploited in the proof of Lemma 5.1 for the case when $(w, c) = (n/2, 0)$.

Before we move on to the following section, we need the fact asserted in Lemma 4.4 below. First for a permutation $\rho \in \mathcal{S}_{[0,n-1]}$ of the indices in the set $[0, n-1]$, define the map $\varphi_\rho: \mathbb{Z}_{q^n-1} \to \mathbb{Z}_{q^n-1}$ by $\varphi_\rho((a_0, \dots, a_{n-1})_q) = (a_{\rho(0)}, \dots, a_{\rho(n-1)})_q$. Note φ_ρ is a permutation of $\mathbb{Z}_{q^n-1}$ with inverse $\varphi_\rho^{-1} = \varphi_{\rho^{-1}}$, for each $\rho \in \mathcal{S}_{[0,n-1]}$. For $k \in \mathbb{Z}_{q^n-1}$, let $\epsilon_i(k)$, $0 \le i \le n-1$, denote the digit of q^i in the q-adic form of its canonical representative. Thus $0 \le \epsilon_i(k) \le q-1$. For $a, b \in \mathbb{Z}_{q^n-1}$ with $a + b \ne 0$, it is clear that if $\epsilon_i(a) + \epsilon_i(b) \le q-1$, then $\epsilon_i(a+b) = \epsilon_i(a) + \epsilon_i(b)$. One can also check, for any $a, b \in \mathbb{Z}_{q^n-1}$ such that $\epsilon_i(a) + \epsilon_i(b) \le q-1$ holds for every $0 \le i \le n-1$, that $\varphi_\rho(a+b) = \varphi_\rho(a) + \varphi_\rho(b)$ for every $\rho \in \mathcal{S}_{[0,n-1]}$, regardless of whether or not $a+b = 0$. By induction, $\varphi_\rho(a_1 + \cdots + a_s) = \varphi_\rho(a_1) + \cdots + \varphi_\rho(a_s)$, whenever $a_1, \dots, a_s \in \mathbb{Z}_{q^n-1}$ satisfy $\epsilon_i(a_1) + \cdots + \epsilon_i(a_s) \le q-1$ for every $0 \le i \le n-1$.

Definition 4.3 **(q-symmetric)** For a function f on $\mathbb{Z}_{q^n-1}$, we say that f is *q-symmetric* if for all $a = (a_0, \dots, a_{n-1})_q \in \mathbb{Z}_{q^n-1}$ and all permutations $\rho \in \mathcal{S}_{[0,n-1]}$, we have $f(\varphi_\rho(a)) = f(a)$, *i.e.*, $f((a_{\rho(0)}, \dots, a_{\rho(n-1)})_q) = f((a_0, \dots, a_{n-1})_q)$.

Note that the δ_w functions are q-symmetric. Because $\epsilon_i(m) \le 1$ for each

$$m \in \operatorname{supp}(\delta_w) = \Omega(w)$$

and each $0 \le i \le n-1$, it follows from Lemma 4.4 that the convolution of at most $q-1$ delta functions is also q-symmetric.

Lemma 4.4 *Let R be a ring and let $f_1, \dots, f_s: \mathbb{Z}_{q^n-1} \to R$ be q-symmetric functions such that for each $a_k \in \operatorname{supp}(f_k)$, $1 \le k \le s$, we have $\epsilon_i(a_1) + \cdots + \epsilon_i(a_s) \le q-1$ for every $0 \le i \le n-1$. Then $f_1 \otimes \cdots \otimes f_s$ is q-symmetric.*

Proof Recall that the assumption on the supports imply that $\varphi_\tau(a_1 + \cdots + a_s) = \varphi_\tau(a_1) + \cdots + \varphi_\tau(a_s)$ for any $a_k \in \operatorname{supp}(f_k)$, $1 \le k \le s$, and any $\tau \in \mathcal{S}_{[0,n-1]}$. Since each f_k is q-symmetric, $1 \le k \le s$, then $f_k(a) = f_k(\varphi_\tau(a))$ for every $a \in \mathbb{Z}_{q^n-1}$. In particular $a \in \operatorname{supp}(f_k)$ if and only if $\varphi_\tau(a) \in \operatorname{supp}(f_k)$; hence $\varphi_\tau(\operatorname{supp}(f_k)) = \operatorname{supp}(f_k)$. Now let $m \in \mathbb{Z}_{q^n-1}$ and let $\rho \in \mathcal{S}_{[0,n-1]}$. Then it follows from the aforementioned observations that

$$\begin{aligned}
(f_1 \otimes \cdots \otimes f_s)(\varphi_\rho(m)) &= \sum_{\substack{j_1+\cdots+j_s=\varphi_\rho(m)\\ j_1,\dots,j_s\in\mathbb{Z}_{q^n-1}}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{j_1+\cdots+j_s=\varphi_\rho(m)\\ j_1\in\operatorname{supp}(f_1),\dots,j_s\in\operatorname{supp}(f_s)}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{\varphi_{\rho^{-1}}(j_1+\cdots+j_s)=m\\ j_1\in\operatorname{supp}(f_1),\dots,j_s\in\operatorname{supp}(f_s)}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{\varphi_{\rho^{-1}}(j_1)+\cdots+\varphi_{\rho^{-1}}(j_s)=m\\ j_1\in\operatorname{supp}(f_1),\dots,j_s\in\operatorname{supp}(f_s)}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{j_1+\cdots+j_s=m\\ \varphi_\rho(j_1)\in\operatorname{supp}(f_1),\dots,\varphi_\rho(j_s)\in\operatorname{supp}(f_s)}} f_1(\varphi_\rho(j_1))\dots f_s(\varphi_\rho(j_s))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{j_1+\cdots+j_s=m\\ \varphi_\rho(j_1)\in\operatorname{supp}(f_1),\dots,\varphi_\rho(j_s)\in\operatorname{supp}(f_s)}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{j_1+\cdots+j_s=m\\ j_1\in\varphi_{\rho^{-1}}(\operatorname{supp}(f_1)),\dots,j_s\in\varphi_{\rho^{-1}}(\operatorname{supp}(f_s))}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{j_1+\cdots+j_s=m\\ j_1\in\operatorname{supp}(f_1),\dots,j_s\in\operatorname{supp}(f_s)}} f_1(j_1)\dots f_s(j_s)\\
&= \sum_{\substack{j_1+\cdots+j_s=m\\ j_1,\dots,j_s\in\mathbb{Z}_{q^n-1}}} f_1(j_1)\dots f_s(j_s)\\
&= (f_1\otimes\cdots\otimes f_s)(m),
\end{aligned}
$$

as required. ∎

5 The Least Period of $\Delta_{w,c}$ and the Proof of Theorem 1.1

In this section we prove in Lemma 5.1 that the least period of the $\Delta_{w,c}$ function of Lemma 4.2 is not a divisor of $(q^n-1)/\Phi_n(q)$, at least in the cases which suffice for a proof of Theorem 1.1. We note that the proof of Lemma 5.1 is of a rather elementary and constructive type nature. There we treat the cases when $c\neq 0$ and $c=0$ separately. We remark that a version of the case when $c\neq 0$ and its combinatorial argument was given in [11]. For the sake of completeness, for the case when $c\neq 0$, we include a proof in the same spirit (see Case 1 of the proof that follows).

First, for an integer $k=\sum_{i=0}^{\infty}\epsilon_i(k)q^i$, we let $s_q(k)=\sum_{i=0}^{\infty}\epsilon_i(k)$ denote the sum of the q-digits of k.

Lemma 5.1 *Let q be a power of a prime, let $n\geq 2$, let w be an integer with $1\leq w<n$, and let $c\in\mathbb{F}_q$. If $c=0$ and $n=2$, assume that q is odd. If $c\neq 0$, further assume that $w<n-1$. Then the least period r of $\Delta_{w,c}$ is not a divisor of $(q^n-1)/\Phi_n(q)$.*

Proof First, by the binomial theorem for convolution,

$$
\begin{aligned}
\big((-1)^w\delta_w-c\delta_0\big)^{\otimes(q-1)} &= \sum_{s=0}^{q-1}\binom{q-1}{s}(-c)^{q-1-s}(-1)^{ws}\delta_w^{\otimes s}\\
&= \sum_{s=0}^{q-1}\binom{q-1}{s}\big((-1)^{w+1}c\big)^{-s}\delta_w^{\otimes s}.
\end{aligned}
$$

Hence

$$
\Delta_{w,c}:=\delta_0-\big((-1)^w\delta_w-c\delta_0\big)^{\otimes(q-1)}=-\sum_{s=1}^{q-1}\binom{q-1}{s}\big((-1)^{w+1}c\big)^{-s}\delta_w^{\otimes s}.
$$

By Lucas' theorem, none of the binomial coefficients above are 0 modulo p, where p is the characteristic of $\mathbb{F}_q$. Now note that for any $m\in\mathbb{Z}_{q^n-1}$, $\delta_w^{\otimes s}(m)$ is the number, modulo p, of ways to write m as a sum of s ordered values in $\Omega(w)$. Next we treat the cases when $c\neq 0$ and $c=0$ separately.

Case 1 ($c\neq 0$): Here we closely follow the combinatorial argument given in [11].

Now it is known that $m \in \operatorname{supp}(\Delta_{w,c})$ if and only if there exists a unique $1 \le s \le q-1$ such that $m \in \operatorname{supp}(\delta_w^{\otimes s})$. In particular if $m \in \operatorname{supp}(\Delta_{w,c})$, then $s_q(m \bmod (q^n-1)) \le (q-1)w$. This implies that $\operatorname{supp}(\Delta_{w,c}) \cap \{q^n-1, q^n-2, \dots, q^n-q\} = \varnothing$ if $w < n-1$.

By Lemma 4.4, $\Delta_{w,c}$ is q-symmetric. For each $m \in \operatorname{supp}(\Delta_{w,c})$ and each permutation $\rho \in \mathcal{S}_{[0,n-1]}$, we have $\Delta_{w,c}(\varphi_\rho(m)) = \Delta_{w,c}(m)$ and thus $\varphi_\rho(m) \in \operatorname{supp}(\Delta_{w,c})$. If $r \mid (q^n-1)/\Phi_n(q)$, then $\operatorname{supp}(\Delta_{w,c})$ is closed under addition and subtraction of $(q^n-1)/\Phi_n(q)$ modulo q^n-1, namely, $\Delta_{w,c}(m+kr) = \Delta_{w,c}(m)$ implies that if $m \in \operatorname{supp}(\Delta_{w,c})$, then $m+kr \in \operatorname{supp}(\Delta_{w,c})$.

In the following, we prove our statement by contradiction. Namely, if $r \mid (q^n-1)/\Phi_n(q)$, then we can find an element in $\operatorname{supp}(\Delta_{w,c})$ that is greater than or equal to q^n-q. For $n \ne 2, 6$, we must have $(q^n-1)/r \ge \Phi_n(q) > q^2$. If $1 < \epsilon_{n-1}(m), \epsilon_{n-2}(m) < q-1$, we can add multiples of r to m so that $m' = m+kr$ satisfies that $\epsilon_{n-1}(m') = \epsilon_{n-1}(m)$ and $\epsilon_{n-2}(m') = \epsilon_{n-1}(m)+1$. Permuting the highest two significant positions (say σ) and subtracting kr, we obtain another element $m'' = \sigma(m') - kr \in \operatorname{supp}(\Delta_{w,c})$ such that $\epsilon_{n-1}(m'') = \epsilon_{n-2}(m)+1$ and $\epsilon_{n-2}(m'') = \epsilon_{n-1}(m)-1$. That is, we can find an element $m' \in \operatorname{supp}(\Delta_{w,c})$ such that $m'-m = q^{n-1}-q^{n-2}$. Continuing to do this, we can find an element, say m, by abuse of notation, in $\operatorname{supp}(\Delta_{w,c})$ such that one of $\epsilon_{n-1}(m)$ and $\epsilon_{n-2}(m)$ is 0 or $q-1$.

For each $m \in \operatorname{supp}(\Delta_{w,c})$, we can find a sequence of permutations so that any two digits $\epsilon_i(m)$ and $\epsilon_j(m)$ of m could be moved to the highest significant positions. This means that we have another element m' in $\operatorname{supp}(\Delta_{w,c})$ so that $\epsilon_{n-1}(m') = \epsilon_i(m)$, $\epsilon_{n-2}(m') = \epsilon_j(m)$, and $\epsilon_k(m')$ $(0 \le k \le n-3)$ must be one of $\epsilon_t(m)$ such that $t \ne i, j$. Hence, repeating the above procedures, we can find another element, say m, in $\operatorname{supp}(\Delta_{w,c})$ such that all digits except at most one equal to 0 or $q-1$. Without loss of generality, we assume $\epsilon_{n-1}(m) = a$. Because $w < n-1$, we have at least one j such that $\epsilon_j(m) = 0$. Again, without loss of generality, we assume that $\epsilon_{n-2}(m) = 0$. If $a \ne 0$, applying the same procedure as above, we can obtain an element $m' \in \operatorname{supp}(\Delta_{w,c})$ such that $\epsilon_{n-2}(m') = q-1$ and $\epsilon_{n-1}(m') = a-1$. Similarly, we can find an element in $\operatorname{supp}(\Delta_{w,c})$ such that all digits equal to $q-1$ except ϵ_0. This contradicts to $\operatorname{supp}(\Delta_{w,c}) \cap \{q^n-1, q^n-2, \dots, q^n-q\} = \varnothing$.

If $a = 0$, then all digits of m are either 0 or $q-1$. Applying the above procedure on $\epsilon_{n-1}(m) = q-1$ and $\epsilon_{n-2}(m) = 0$, we can obtain $m' \in \operatorname{supp}(\Delta_{w,c})$ such that $\epsilon_{n-1}(m') = q-2$ and $\epsilon_{n-2}(m') = q-1$. Then we always turn the other 0 digits into $q-1$ digits. Eventually we have an element in $\operatorname{supp}(\Delta_{w,c})$ such that each digit except the least significant digit is $q-1$. This contradicts $\operatorname{supp}(\Delta_{w,c}) \cap \{q^n-1, q^n-2, \dots, q^n-q\} = \varnothing$.

For $n = 2$, we have $r \mid q-1$. If $m \in \operatorname{supp}(\Delta_{w,c})$, then there exists a k such that $m + k(q-1) \in \operatorname{supp}(\Delta_{w,c})$ and $m + k(q-1) > q^2 - q$, a contradiction.

For $n = 6$, $(q^n-1)/\Phi_n(q) = q^4 + q^3 - q - 1$. If m contains at most three $q-1$ digits in its q-ary expansion, then $\epsilon_{n-2}(m + (q^n-1)/\Phi_n(q)) = \epsilon_{n-2}(m)+1$. Permuting the highest significant two digits of $m + (q^n-1)/\Phi_n(q)$ and subtracting $(q^n-1)/\Phi_n(q)$ from it, we obtain an element $m' \in \operatorname{supp}(\Delta_{w,c})$ such that $\epsilon_{n-1}(m') = \epsilon_{n-2}(m)+1$ and $\epsilon_{n-2}(m') = \epsilon_{n-1}(m)-1$. In this way, we can find an element in $\operatorname{supp}(\Delta_{w,c})$ with four $q-1$ digits. Without loss of generality, we can assume that $m \in \operatorname{supp}(\Delta_{w,c})$ such that $\epsilon_{n-1}(m) = q-1$ and $\epsilon_2(m) = \epsilon_1(m) = \epsilon_0(m) = q-1$, namely, m has the q-ary representation $q-1, a, b, q-1, q-1, q-1$. Subtracting $(q^n-1)/\Phi_n(q)$ from m, we obtain an element in the support such that its q-ary representation is $q-1, a-1, b, 0, 1, 0$. Permuting the highest two significant digits and adding $(q^n-1)/\Phi_n(q)$ back, we obtain $m' \in \operatorname{supp}(\Delta_{w,c})$ such that m' has q-ary representation $a, 0, b, q-1, q-1, q-1$. However, m' and m have different weights, which is a contradiction.

Case 2 ($c=0$): Note $\Delta_{w,0} = \delta_0 - \delta_w^{\otimes(q-1)}$ and $\Delta_{w,0}(0) = 1$. Thus $\Delta_{w,0}(r) = \Delta_{w,0}(0+r) = 1$. Since $0 < r < q^n - 1$, necessarily $\delta_w^{\otimes(q-1)}(r) = -1$. In particular, $r \in \operatorname{supp}(\delta_w^{\otimes(q-1)})$ and $s_q(r) = (q-1)w$. Because $1 \le r < q^n - 1$ is a period of $\Delta_{w,0}$, so is $r' = q^n - 1 - r$ with $1 \le r' < q^n - 1$. Then the previous arguments similarly imply that $s_q(r') = (q-1)w$. Given that $s_q(r') = (q-1)n - s_q(r)$, it follows $w = n/2$ and $s_q(r) = (q-1)n/2$. In particular, n is even and $\Delta_{w,0} = \Delta_{n/2,0} = \delta_0 - \delta_{n/2}^{\otimes(q-1)}$.

Consider the case when $n > 2$. Suppose not all digits of r are the same. (Since $s_q(r) = (q-1)n/2$, it is equivalent to supposing that $r \neq (q^n-1)/2$; this is the case in particular when q is even.) Clearly either there exists $k \in [0, n-2]$ such that $r_k > r_{k+1}$ or the sequence $r_0, \dots, r_{n-1}$ is non-decreasing. Suppose the former holds. Fix any such k and let σ be the permutation of $[0, n-1]$ which fixes each index in $[0, n-1] \setminus \{k, k+1\}$ and maps $k \mapsto k+1$ and $k+1 \mapsto k$. Thus

$$\begin{aligned}\varphi_\sigma(r) &= r_k q^{k+1} + r_{k+1} q^k + \sum_{i \in [0,n-1] \setminus \{k,k+1\}} r_i q^i \\ &> r_{k+1} q^{k+1} + r_k q^k + \sum_{i \in [0,n-1] \setminus \{k,k+1\}} r_i q^i = r,\end{aligned}$$

since $r_k > r_{k+1}$. Because $\varphi_\sigma(r)$ is obtained via a permutation of the digits of r, and $0 < r < q^n - 1$, then $0 < \varphi_\sigma(r) < q^n - 1$. Now note

$$\begin{aligned}\varphi_\sigma(r) - r &= (r_k - r_{k+1}) q^{k+1} - (r_k - r_{k+1}) q^k \\ &= (r_k - r_{k+1} - 1) q^{k+1} + (q - (r_k - r_{k+1})) q^k.\end{aligned}$$

Since $1 \le r_k - r_{k+1} \le q-1$, it follows that the above coefficients are contained in the set $[0, q-1]$; hence this is the q-adic form of $\varphi_\sigma(r) - r$ and one can see that $s_q(\varphi_\sigma(r) - r) = q - 1$.

Because $\delta_{n/2}$ is q-symmetric with $\epsilon_i(m) \le 1$ for each $m \in \operatorname{supp}(\delta_{n/2}) = \Omega(n/2)$ and each $0 \le i \le n-1$, it follows from Lemma 4.4 that $\delta_{n/2}^{\otimes(q-1)}$ is q-symmetric. In particular $\delta_{n/2}^{\otimes(q-1)}(\varphi_\sigma(r)) = \delta_{n/2}^{\otimes(q-1)}(r)$. Since $\varphi_\sigma(r) \neq 0$, then

$$\Delta_{n/2,0}(\varphi_\sigma(r)) = -\delta_{n/2}^{\otimes(q-1)}(\varphi_\sigma(r)) = -\delta_{n/2}^{\otimes(q-1)}(r) = 1;$$

hence $\varphi_\sigma(r) \in \operatorname{supp}(\Delta_{n/2,0})$. Given that $\Delta_{n/2,0}$ is r-periodic, we have

$$\varphi_\sigma(r) - r \in \operatorname{supp}(\Delta_{n/2,0}).$$

Since $0 < \varphi_\sigma(r) - r < q^n - 1$, then $\varphi_\sigma(r) - r \in \operatorname{supp}(\delta_{n/2}^{\otimes(q-1)})$. It follows that

$$s_q(\varphi_\sigma(r) - r) = (q-1)n/2,$$

contradicting $s_q(\varphi_\sigma(r) - r) = q - 1$ with $n > 2$. Necessarily the q-digits $r_0, \dots, r_{n-1}$ of r must form a non-decreasing sequence. Since not all digits of r are the same, in particular $r_{n-1} > r_0$.

Since $\Delta_{n/2,0}$ is r-periodic, it is $r'' := (qr \bmod (q^n-1))$-periodic. Note that $0 < r'' < q^n - 1$ and $r'' = (r_{n-1}, r_0, r_1, \dots, r_{n-2})_q$. However observe that $r_0 = \epsilon_1(r'') < \epsilon_0(r'') = r_{n-1}$. Then we can reproduce the previous arguments with r and k substituted with r'' and 0, respectively, to obtain a contradiction. Thus for $n > 2$, it is impossible that $\Delta_{n/2,0}$ is r-periodic if $0 < r < q^n - 1$ and not all digits of r are the same. In particular when q is even and $n > 2$, $\Delta_{n/2,0}$ must have maximum least period $q^n - 1$.

Note that at this point we have proved that if $w \neq n/2$, or $n > 2$ and q is even with $w = n/2$, then $r = q^n - 1$. In the case when q odd with $n > 2$ and $w = n/2$, we have shown that either $r = (q^n - 1)/2$ (all digits of r are the same) or no such r with $0 < r < q^n - 1$ can be a period of $\Delta_{n/2,0}$ (when not all digits of r are the same), whence the least period of $\Delta_{n/2,0}$ must be the maximum, $q^n - 1$.

Consider now the case with $n = 2$ and q odd. Here $w = n/2 = 1$ and we claim that $r > q - 1$. On the contrary, suppose $r \le q - 1$. Since $s_q(r) = (q-1)n/2 = q - 1$, it follows that $r = q - 1$. Note that there is exactly one way to write $r = q - 1$ as a sum of $q - 1$ ordered elements in $\Omega(1) = \{1, q\}$, namely as $q - 1 = 1 + \cdots + 1$, a total of $q - 1$ times. Thus $\delta_1^{\otimes(q-1)}(r) = 1$. This contradicts the fact (see the beginning of the proof of Case 2) that $\delta_1^{\otimes(q-1)}(r) = -1$ with q odd. Hence the claim follows.

It remains to notice that the least period r of $\Delta_{w,c}$ satisfies $r > (q^n - 1)/\Phi_n(q)$ in every case here, and hence $r \nmid (q^n - 1)/\Phi_n(q)$. Indeed, this follows immediately from the fact that $\Phi_n(q) > q - 1$ for $n \ge 2$. In the case of $n = 2$ with $w = 1$, we have $r > q - 1 = (q^2 - 1)/(q + 1) = (q^2 - 1)/\Phi_2(q)$ as well. This concludes the proof of Lemma 5.1. ∎

Proof of Theorem 1.1 It is elementary to show that every element of $\mathbb{F}_q^*$ is the norm of an element of degree n over $\mathbb{F}_q$ [18]. Thus we may assume $w < n$. If $w = n - 1$, we claim that the number of monic irreducible polynomials with prescribed coefficient of x is positive. Indeed, by Carlitz's result [5], there exists an irreducible polynomial with both arbitrarily prescribed trace and nonzero norm coefficients, and then the claim follows by taking the appropriate monic reciprocal. The other cases follow from Lemma 5.1 together with Lemma 4.2. ∎

Acknowledgement We thank the anonymous referee for several helpful suggestions.

References

[1] M. Aigner and G. M. Ziegler, *Proofs from the book*. 4th ed., Springer-Verlag, Berlin, 2010.
[2] A. Barvinok, *Matrices with prescribed row and column sums*. Linear Algebra Appl. **436**(2012), no. 4, 820–844. http://dx.doi.org/10.1016/j.laa.2010.11.019
[3] J. Bourgain, *Prescribing the binary digits of primes, II*. Israel J. Math. **206**(2015), no. 1, 165–182. http://dx.doi.org/10.1007/s11856-014-1129-5
[4] A. Canteaut and M. Videau, *Symmetric boolean functions*. IEEE Transactions on Information Theory, Institute of Electrical and Electronics Engineers **51**(2005), no. 8, 2791–2811. http://dx.doi.org/10.1109/TIT.2005.851743
[5] L. Carlitz, *A theorem of Dickson on irreducible polynomials*. Proc. Amer. Math. Soc. **3**(1952), 693–700. http://dx.doi.org/10.1090/S0002-9939-1952-0049940-6
[6] F. N. Castro and L. A. Medina, *Linear recurrences and asymptotic behaviour of exponential sums of symmetric boolean functions*. Electr. J. Comb. **18**(2011), no. 2, paper #P9.
[7] S. D. Cohen, *Primitive polynomials over small fields*. In: Finite fields and applications. Lecture Notes in Comput. Sci., 2948. Springer, Berlin, 2004, pp. 197–214.

[8] ———, *Primitive polynomials with a prescribed coefficient*. Finite Fields Appl. **12**(2006), no. 3, 425–491. http://dx.doi.org/10.1016/j.ffa.2005.08.001
[9] S. D. Cohen and M. Prešern, *Primitive polynomials with prescribed second coefficient*. Glasgow Math. J. **48**(2006), 281–307. http://dx.doi.org/10.1017/S0017089506003077
[10] ———, *The Hansen–Mullen primitivity conjecture: completion of proof*. In: Number theory and polynomials. London Math. Soc. Lecture Note Ser., 352. Cambridge University Press, Cambridge, 2008, pp. 89–120.
[11] T. Dorsey and A. W. Hales, *Irreducible coefficient relations*. Sequences and their applications-SETA. 2012, Lecture Notes in Comput. Sci., 7280. Springer, Heidelberg, 2012 , pp. 117–125.
[12] S. Q. Fan and W. B. Han, *p-Adic formal series and primitive polynomials over finite fields*. Proc. Amer. Math. Soc. **132**(2004), 15–31. http://dx.doi.org/10.1090/S0002-9939-03-07040-0
[13] R. W. Fitzgerald and J. L. Yucas, *Irreducible polynomials over GF(2) with three prescribed coefficients*. Finite Fields Appl. **9**(2003), 286–299. http://dx.doi.org/10.1016/S1071-5797(03)00005-4
[14] T. Garefalakis, *Irreducible polynomials with consecutive zero coefficients*. Finite Fields Appl. **14**(2008), no. 1, 201–208. http://dx.doi.org/10.1016/j.ffa.2006.11.002
[15] J. Ha, *Irreducible polynomials with several prescribed coefficients*. Finite Fields Appl. **40**(2016), 10–25. http://dx.doi.org/10.1016/j.ffa.2016.02.006
[16] K. H. Ham and G. L. Mullen, *Distribution of irreducible polynomials of small degrees over finite fields*. Math. Comp. **67**(1998), no. 221, 337–341. http://dx.doi.org/10.1090/S0025-5718-98-00904-1
[17] W. B. Han, *On Cohen's problem*. Chinacrypt '96, Academic Press (China) (1996) 231–235 (Chinese).
[18] T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*. Math. Comp. **59**(1992), 639–643. http://dx.doi.org/10.1090/S0025-5718-1992-1134730-7
[19] Ç. K. Koç, *Open problems in mathematics and computational science*. Springer International Publishing, 2014.
[20] K. Kononen, M. Moisio, M. Rinta-aho, and K. Väänänen, *Irreducible polynomials with prescribed trace and restricted norm*. JP J. Algebra Number Theory Appl. **11**(2009), 223–248.
[21] J. H. van Lint and R. M. Wilson, *A course in combinatorics*. 2nd ed., Cambridge University Press, Cambridge, 2001.
[22] B. Omidi Koma, D. Panario, and Q. Wang, *The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms*. Discrete Math. **310**(2010), 1282–1292. http://dx.doi.org/10.1016/j.disc.2009.12.006
[23] D. Panario and G. Tzanakis, *A generalization of the Hansen–Mullen conjecture on irreducible polynomials over finite fields*. Finite Fields Appl. **18**(2012), no. 2, 303–315. http://dx.doi.org/10.1016/j.ffa.2011.09.003
[24] A. Tuxanidy and Q. Wang, *On the number of N-free elements with prescribed trace*. J. Number Theory **160**(2016), 536–565. http://dx.doi.org/10.1016/j.jnt.2015.09.008
[25] P. Pollack, *Irreducible polynomials with several prescribed coefficients*. Finite Fields Appl. **22**(2013), 70–78. http://dx.doi.org/10.1016/j.ffa.2013.03.001
[26] D.-B. Ren, *On the coefficients of primitive polynomials over finite fields*. Sichuan Daxue Xuebao **38**(2001), 33–36.
[27] I. E. Shparlinski, *On primitive polynomials*. Prob. Peredachi Inform. **23**(1988), 100–103 (Russian).
[28] G. Tzanakis, *On the existence of irreducible polynomials with prescribed coefficients over finite fields*. Master's thesis, Carleton University, 2010. //www.math.carleton.ca/~gtzanaki/mscthesis.pdf
[29] D. Wan, *Generators and irreducible polynomials over finite fields*. Math. Comp. **66**(1997), no. 219, 1195–1212. http://dx.doi.org/10.1090/S0025-5718-97-00835-1

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6
e-mail: aleksandrtuxanidytor@cmail.carleton.ca wang@math.carleton.ca