J. Aust. Math. Soc. **112** (2022), 355–366
doi:10.1017/S1446788721000094

GENERATORS OF FINITE FIELDS WITH PRESCRIBED TRACES

LUCAS REIS and SÁVIO RIBAS

(Received 29 September 2020; accepted 18 March 2021; first published online 27 May 2021)

Communicated by Dzmitry Badziahin

Abstract

This paper explores the existence and distribution of primitive elements in finite field extensions with prescribed traces in several intermediate field extensions. Our main result provides an inequality-like condition to ensure the existence of such elements. We then derive concrete existence results for a special class of intermediate extensions.

2020 *Mathematics subject classification*: primary 12E20; secondary 11T24.

Keywords and phrases: character sums, field trace, finite fields, primitive elements.

1. Introduction

Given a prime power q and a positive integer $n > 1$, let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_{q^n}$ the unique n-degree field extension of $\mathbb{F}_q$. The intermediate extensions of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are exactly the finite fields $\mathbb{F}_{q^d}$ with d a divisor of n. It is well known that the multiplicative group $\mathbb{F}_{q^n}^*$ is cyclic; any generator of such group is called *primitive*. Primitive elements play important roles in a wide variety of applications in cryptography and, perhaps, the most notable one is the Diffie–Hellman key exchange [4]. Primitive elements with further specified properties have been extensively studied in the past few decades. The motivation comes from both theoretical and practical matters.

For instance, the celebrated *primitive normal basis theorem* states that for any $n \geq 1$ and any prime power q, there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that α is *normal* over $\mathbb{F}_q$, that is, the set $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ comprises an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$. The primitive normal basis theorem was proved by Lenstra and Schoof [6] and a proof without any use of computers was later given by Cohen and Huczynska [2]. Cohen [1] also explored the existence of primitive elements in $\mathbb{F}_{q^n}$ with prescribed *trace* $a \in \mathbb{F}_q$, that

is, primitive elements $\alpha \in \mathbb{F}_{q^n}$ such that

$$\mathrm{Tr}_{q^n/q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = a. \tag{1-1}$$

He has shown that, up to genuine exceptions, it is possible to find primitive elements in $\mathbb{F}_{q^n}$ satisfying equation (1-1). More specifically, we have the following result.

THEOREM 1.1. *Let q be a prime power, n a positive integer and $a \in \mathbb{F}_q$. Then there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q}(\alpha) = a$ unless $a = 0$ and $n = 2$ or $a = 0$, $n = 3$ and $q = 4$.*

In this paper, we discuss the existence of primitive elements in $\mathbb{F}_{q^n}$ with prescribed traces in several intermediate extensions $\mathbb{F}_{q^d}$ of $\mathbb{F}_{q^n}$. In other words, for given $n > 1$, $d_1 < \cdots < d_k < n$ divisors of n, and $a_j \in \mathbb{F}_{q^{d_i}}$, we discuss the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that, for each $1 \le j \le k$,

$$\mathrm{Tr}_{q^n/q^{d_j}}(\alpha) = \sum_{i=0}^{n/d_j-1} \alpha^{q^{id_j}} = a_j.$$

Our main result, Theorem 2.4, provides an inequality-like condition to ensure the existence of such elements. This condition might easily yield asymptotic existence results. We then present a special instance where we can obtain effective results. In particular, we prove that, up to a few critical cases, there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ with arbitrary prescribed traces in any two intermediate $\mathbb{F}_q$-extensions of $\mathbb{F}_{q^n}$: see Theorem 5.1 for more details.

The structure of the paper is as follows. In Section 2 we introduce some useful notation and present our main result. Section 3 provides background material that is used along the way and some auxiliary results. In Section 4 we prove our main result. Finally, in Section 5, we restrict our problem to a special class of intermediate extensions, where our results are sharpened.

2. Main results

Before we state our main result, we introduce some notation and discuss a natural condition that we have to impose in the problem. Throughout this paper, q is a prime power and $\mathbb{F}_q$ is the finite field with q elements.

DEFINITION 2.1. For $n > 1$, d a divisor of n and $\alpha \in \mathbb{F}_{q^n}$, we set

$$\mathrm{Tr}_{n/d}(\alpha) = \sum_{i=0}^{n/d-1} \alpha^{q^{di}},$$

the *trace* of α over $\mathbb{F}_{q^d}$.

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

Recall that the trace is transitive, that is, if e divides d and d divides n, then for any $\alpha \in \mathbb{F}_{q^n}$ we have that $\mathrm{Tr}_{n/e}(\alpha) = \mathrm{Tr}_{n/d}(\mathrm{Tr}_{d/e}(\alpha))$. In particular, if $d_1 < \cdots < d_k < n$ are divisors of n and we pick $a_i \in \mathbb{F}_{q^{d_i}}$, $1 \le i \le k$, then the existence of an element $\alpha \in \mathbb{F}_{q^n}$ with $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ is necessarily conditional on the following identities:

$$\mathrm{Tr}_{d_i/\gcd(d_i,d_j)}(a_i) = \mathrm{Tr}_{n/\gcd(d_i,d_j)}(\alpha) = \mathrm{Tr}_{d_j/\gcd(d_i,d_j)}(a_j), \ 1 \le i,j \le k. \tag{2-1}$$

REMARK 2.2. As recently shown by the first author in [7], the equations in (2-1) are also sufficient and, in this case, there exist exactly $q^{n-\lambda}$ elements in $\mathbb{F}_{q^n}$ with $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ for $1 \le i \le k$, where

$$\begin{aligned}\lambda &= \deg(\mathrm{lcm}(x^{d_1}-1,\dots,x^{d_k}-1)) \\ &= d_1 + \cdots + d_k + \sum_{i=2}^{k}(-1)^{i+1} \sum_{1\le \ell_1<\cdots<\ell_i\le k} \gcd(d_{\ell_1},\dots,d_{\ell_i}).\end{aligned}$$

The proof of this result is a simple application of the Chinese remainder theorem for the ring $\mathbb{F}_q[x]$. For more details, see Theorem 4.1 in [7].

The equations in (2-1) imply that if d_i divides some d_j, then the equality $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ is already implied by $\mathrm{Tr}_{n/d_j}(\alpha) = a_j$. Therefore, we may restrict ourselves to divisors $d_1 < \cdots < d_k$ of n such that $d_i \nmid d_j$ for any $1 \le i < j \le k$. In addition, the case $k = 1$ was completely settled by Cohen [1], so we assume that $k > 1$, that is, n is not a prime power. We introduce some useful notation.

DEFINITION 2.3. Let $n > 1$ be an integer that is not a prime power and $1 < k < \sigma_0(n)$, where $\sigma_0(n)$ denotes the number of positive divisors of n.

(i) $\Lambda_k(n)$ stands for the set of k-tuples $\mathbf{d} = (d_1,\dots,d_k)$, where $d_1 < \cdots < d_k < n$ are divisors of n such that d_i does not divide d_j for every $1 \le i,j \le k$ with $i \ne j$.

(ii) For $\mathbf{d} = (d_1,\dots,d_k) \in \Lambda_k(n)$, set $\mathbb{F}(\mathbf{d}) = \prod_{i=1}^{k} \mathbb{F}_{q^{d_i}}$ and

$$\lambda(\mathbf{d}) = d_1 + \cdots + d_k + \sum_{i=2}^{k}(-1)^{i+1} \sum_{1\le \ell_1<\cdots<\ell_i\le k} \gcd(d_{\ell_1},\dots,d_{\ell_i}).$$

Moreover, for $\mathbf{d} = (d_1,\dots,d_k) \in \Lambda_k(n)$ and $\mathbf{a} = (a_1,\dots,a_k) \in \mathbb{F}(\mathbf{d})$, the k-tuple $\mathbf{a}$ is $\mathbf{d}$-*admissible* if, for any $1 \le i < j \le k$,

$$\mathrm{Tr}_{d_i/\gcd(d_i,d_j)}(a_i) = \mathrm{Tr}_{d_j/\gcd(d_i,d_j)}(a_j).$$

From previous observation, we only need to consider $\mathbf{d}$-admissible k-tuples. Our main result can be stated as follows.

THEOREM 2.4. *Let $n > 1$ be an integer that is not a prime power, $1 < k < \sigma_0(n)$, $\mathbf{d} = (d_1,\dots,d_k) \in \Lambda_k(n)$ and $\mathbf{a} = (a_1,\dots,a_k) \in \mathbb{F}(\mathbf{d})$ a $\mathbf{d}$-admissible k-tuple. Then there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ with prescribed traces $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ for every*

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

$1 \le i \le k$ *provided that*

$$q^{n/2-\lambda(\mathbf{d})} \ge W(q^n - 1), \tag{2-2}$$

where $W(t)$ *denotes the number of squarefree divisors of* t.

In the context of Theorem 2.4, we also obtain the following minor result.

THEOREM 2.5. *We have that Theorem 2.4 also holds if the condition* $q^{n/2-\lambda(\mathbf{d})} \ge W(q^n - 1)$ *is replaced by the inequality* $\operatorname{lcm}(d_1, \dots, d_k) < n$.

While the proof of Theorem 2.5 is a straightforward combination of Theorem 4.1 in [7] and Theorem 1.1, the proof of Theorem 2.4 relies on character sum methods to count elements in finite fields with specified properties. We follow the traditional approach that is presented in [1, 2, 6]. In this approach, we frequently need to simplify character sums by detecting trivial Gauss sums; in our case, we employ a result from [7] concerning special zero sums in finite fields.

3. Preliminaries

This section provides background material that is used throughout the paper and some auxiliary results.

3.1. Characters and characteristic functions. Here we provide character sum expressions for the characteristic functions of elements in finite fields with specified properties. We start by recalling some basics on characters over finite fields.

Fix a primitive element $\alpha \in \mathbb{F}_{q^n}$. A typical multiplicative character of $\mathbb{F}_{q^n}$ is a function $\eta : \mathbb{F}_{q^n}^* \to \mathbb{C}$ given by $\eta(\alpha^k) = e^{2\pi i k t/(q^n-1)}$ for some positive integer $t \le q^n - 1$. The character $\eta_1 \equiv 1$ is the trivial multiplicative character. The set of multiplicative characters of $\mathbb{F}_{q^n}$ forms a (multiplicative) cyclic group of order $q^n - 1$. In particular, for each divisor t of $q^n - 1$, there exist exactly $\varphi(t)$ multiplicative characters of order t; we denote the set of such characters by $\Gamma(t)$. We extend the evaluation of multiplicative characters to the element $0 \in \mathbb{F}_{q^n}$ by letting $\eta(0) = 0$.

If p is the characteristic of $\mathbb{F}_q$, say $q = p^s$, and m is any divisor of n, the canonical additive character of $\mathbb{F}_{q^m}$ is the function $\chi : \mathbb{F}_{q^m} \to \mathbb{C}$ given by

$$\chi(\beta) = e^{\frac{2\pi i \mathcal{T}_m(\beta)}{p}},$$

where $\mathcal{T}_m(\beta) = \sum_{i=1}^{ms-1} \beta^{p^i} \in \mathbb{F}_p$ is the absolute trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_p$. For each $c \in \mathbb{F}_{q^m}$, we set $\chi_c(\beta) = \chi(c \cdot \beta)$, which is another additive character of $\mathbb{F}_{q^m}$. In fact, the set of additive characters of $\mathbb{F}_{q^m}$ is a (multiplicative) group isomorphic to the additive group $\mathbb{F}_{q^m}$ and comprises the characters $\{\chi_c \mid c \in \mathbb{F}_{q^m}\}$. The identity of such group is the trivial additive character χ_0. We introduce some useful notation.

DEFINITION 3.1. Fix a positive integer n, d a divisor of n and $a \in \mathbb{F}_{q^d}$. Let $I_{n,d,a}$ be the characteristic function for elements in $\mathbb{F}_{q^n}$ with trace a over $\mathbb{F}_{q^d}$, and let Ω_n be the

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

characteristic function for primitive elements in $\mathbb{F}_{q^n}$, that is, for $\alpha \in \mathbb{F}_{q^n}$,

$$I_{n,d,a}(\alpha) = \begin{cases} 1 & \text{if } \operatorname{Tr}_{n/d}(\alpha) = a, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \Omega_n(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is primitive,} \\ 0 & \text{otherwise.} \end{cases}$$

In addition, set $\theta(q) = (\varphi(q^n - 1)/(q^n - 1))$.

The following results provide expressions for the functions Ω_n and $I_{n,d,a}$ by means of characters.

LEMMA 3.2. *For every $\beta \in \mathbb{F}_{q^n}$,*

$$\Omega_n(\beta) = \theta(q) \sum_{t \mid q^n - 1} \frac{\mu(t)}{\varphi(t)} \sum_{\eta \in \Gamma(t)} \eta(\beta),$$

where μ is the Möbius function over the integers.

For the proof of the previous lemma, see Theorem 2.8 of [5] and the comments thereafter.

LEMMA 3.3. *Let m be a divisor of n and $\gamma \in \mathbb{F}_{q^n}$ be such that $\operatorname{Tr}_{n/m}(\gamma) = a \in \mathbb{F}_{q^m}$. If χ denotes the canonical additive character of $\mathbb{F}_{q^n}$, then, for any $\beta \in \mathbb{F}_{q^n}$,*

$$I_{n,d,a}(\beta) = \frac{1}{q^m} \sum_{c \in \mathbb{F}_{q^m}} \chi_c(\beta - \gamma) = \frac{1}{q^m} \sum_{c \in \mathbb{F}_{q^m}} \chi_c(\beta) \chi_c(\gamma)^{-1}.$$

For the proof of the previous lemma, see Subsection 2.3.1 of [5].

3.2. Auxiliary lemmas. From Corollary 1.2 in [7], we have the following result.

LEMMA 3.4. *Let $n > 1$ be an integer that is not a prime power, $1 < k < \sigma_0(n)$ and let $\mathbf{d} = (d_1, \ldots, d_k) \in \Lambda_k(n)$. Then the number of k-tuples $(x_1, \ldots, x_k) \in \mathbb{F}(\mathbf{d})$ such that $x_1 + \cdots + x_k = 0$ equals*

$$q^{d_1 + \cdots + d_k - \lambda(\mathbf{d})}.$$

We further require effective upper bounds on the functions W and $\lambda(\mathbf{d})$. We have the following results.

LEMMA 3.5.

(i) *If $W(t)$ is the number of squarefree divisors of t, then, for all $t \geq 3$,*

$$W(t - 1) < t^{(0.96/\log\log t)}.$$

(ii) *If $n > 1$ is an integer that is not a prime power, $1 < k < \sigma_0(n)$ and $\mathbf{d} \in \Lambda_k(n)$, then*

$$\lambda(\mathbf{d}) \leq n - \varphi(n),$$

where $\varphi(n)$ is the Euler totient function.

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

PROOF. Item (i) is a straightforward consequence of inequality (4.1) in [3]. For item (ii), observe that, as stated in Remark 2.2, $\lambda(\mathbf{d})$ equals the degree of the least common multiple of the polynomials $x^{d_1}-1,\dots,x^{d_k}-1$. Since $d_1<\cdots<d_k<n$, if $p_1,\dots,p_t$ are the distinct prime divisors of n, we have that the polynomials $x^{d_1}-1,\dots,x^{d_k}-1$ divide the polynomial

$$\operatorname{lcm}(x^{n/p_1}-1,\dots,x^{n/p_t}-1).$$

An inclusion–exclusion argument shows that the previous polynomial has degree $n-\varphi(n)$ and the result follows. □

LEMMA 3.6 (see Lemma 4.1 of [5]). *If a is a positive integer and $p_1,\dots,p_j$ are the distinct prime divisors of t such that $p_i\le 2^a$, then*

$$W(t)\le c_{t,a}t^{1/a},\qquad \text{where}\quad c_{t,a}:=\frac{2^j}{(p_1\cdots p_j)^{1/a}}.$$

In particular,

$$c_{t,4}<\begin{cases}4.9 & \text{for } t \text{ even},\\ 2.9 & \text{for } t \text{ odd}\end{cases}\qquad \text{and}\qquad c_{t,8}<4514.7.$$

4. Proof of the main result

Let $N(n,\mathbf{d},\mathbf{a})$ be the number of primitive elements $\alpha\in\mathbb{F}_{q^n}$ such that $\operatorname{Tr}_{n/d_i}(\alpha)=a_i$. In particular,

$$N(n,\mathbf{d},\mathbf{a})=\sum_{w\in\mathbb{F}_{q^n}}\Omega_n(\omega)\cdot\prod_{i=1}^{k}I_{n,d_i,a_i}(w).$$

Since the k-tuple $(a_1,\dots,a_k)$ is $\mathbf{d}$-admissible, we have seen that there exists $\beta\in\mathbb{F}_{q^n}$ such that $\operatorname{Tr}_{(n/t)/d_i}(\beta)=a_i$ for $1\le i\le k$. Write $D=d_1+\cdots+d_k$ and, for a generic $\mathbf{c}=(c_1,\dots,c_k)\in\mathbb{F}(\mathbf{d})$, write $s(\mathbf{c})=\sum_{i=1}^{k}c_i$. From Lemmas 3.2 and 3.3,

$$\begin{aligned}\frac{q^DN(n,\mathbf{d},\mathbf{a})}{\theta(q)}&=\sum_{w\in\mathbb{F}_{q^n}}\sum_{t\mid q^n-1}\frac{\mu(t)}{\varphi(t)}\sum_{\eta\in\Gamma(t)}\eta(w)\cdot\prod_{i=1}^{k}\Bigg(\sum_{c_i\in\mathbb{F}_{q^{d_i}}}\chi_{c_i}(w)\cdot\chi_{c_i}(\beta)^{-1}\Bigg)\\&=\sum_{w\in\mathbb{F}_{q^n}}\sum_{\mathbf{c}\in\mathbb{F}(\mathbf{d})}\sum_{t\mid q^n-1}\frac{\mu(t)}{\varphi(t)}\sum_{\eta\in\Gamma(t)}\eta(w)\cdot\chi_{s(\mathbf{c})}(w)\cdot\chi_{s(\mathbf{c})}(-\beta)\\&=\sum_{\mathbf{c}\in\mathbb{F}(\mathbf{d})}\sum_{t\mid q^n-1}\frac{\mu(t)}{\varphi(t)}\sum_{\eta\in\Gamma(t)}\chi_{s(\mathbf{c})}(-\beta)\cdot G_n(\eta,\chi_{s(\mathbf{c})}),\end{aligned}$$

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

where $G_n(\eta,\chi_{s(\mathbf{c})}) = \sum_{w\in\mathbb{F}_{q^n}} \eta(w)\cdot\chi_{s(\mathbf{c})}(w)$ denotes a Gauss sum. We use the orthogonality relations to obtain

$$G_n(\eta,\chi_{s(\mathbf{c})}) = \begin{cases} q^n & \text{if } \eta\in\Gamma(1) \text{ and } s(\mathbf{c})=0,\\ 0 & \text{if } \eta\in\Gamma(1) \text{ and } s(\mathbf{c})\neq 0,\\ 0 & \text{if } \eta\notin\Gamma(1) \text{ and } s(\mathbf{c})=0,\end{cases}$$

and in the remaining cases we have the well-known identity $|G_n(\eta,\chi_{s(\mathbf{c})})| = q^{n/2}$. In addition, if $s(\mathbf{c})=0$, then $\chi_{s(\mathbf{c})}(-\beta)=\chi_0(-\beta)=1$. In particular, we may rewrite

$$\frac{q^D N(n,\mathbf{d},\mathbf{a})}{\theta(q)} = \sum_{\substack{\mathbf{c}\in\mathbb{F}(\mathbf{d})\\ s(\mathbf{c})=0}} q^n + \underbrace{\sum_{\substack{\mathbf{c}\in\mathbb{F}(\mathbf{d})\\ s(\mathbf{c})\neq 0}} \sum_{\substack{t\mid q^n-1\\ t\neq 1}} \frac{\mu(t)}{\varphi(t)} \sum_{\eta\in\Gamma(t)} \chi_{s(\mathbf{c})}(-\beta)\cdot G_n(\eta,\chi_{s(\mathbf{c})})}_{S}.$$

From Lemma 3.4, we obtain the following equality:

$$\frac{q^D N(n,\mathbf{d},\mathbf{a})}{\theta(q)} = q^{n+D-\lambda(\mathbf{d})} + S.$$

We observe that $|\chi_{s(\mathbf{c})}(-\beta)|=1$ and $|G_n(\eta,\chi_{s(\mathbf{c})})| = q^{n/2}$ in every term of the sum S. Recall that there exist exactly $\varphi(t)$ elements in $\Gamma(t)$ and the function μ has absolute value 1 at squarefree integers and vanishes everywhere else. In particular, we obtain the following inequality:

$$|S| < \sum_{\substack{\mathbf{c}\in\mathbb{F}(\mathbf{d})\\ s(\mathbf{c})\neq 0}} \sum_{\substack{t\mid q^n-1\\ t \text{ squarefree}}} q^{n/2} = q^{n/2+D}\cdot W(q^n-1).$$

Hence,

$$\frac{q^D N(n,\mathbf{d},\mathbf{a})}{\theta(q)} > q^{n+D-\lambda(\mathbf{d})} - q^{n/2+D}\cdot W(q^n-1) \geq 0$$

provided that $q^{n/2-\lambda(\mathbf{d})} \geq W(q^n-1)$.

4.1. Proof of Theorem 2.5. Set $\operatorname{lcm}(d_1,\ldots,d_k) = n/t$, where $t>1$ is a divisor of n. Since there do not exist $1\leq i,j\leq k$ such that d_i divides d_j, we have that $d_i < n/t$ for any $1\leq i\leq k$ and then, from Lemma 3.5, we have that $\lambda(\mathbf{d}) \leq n/t - \varphi(n/t)$. From hypothesis, the k-tuple $(a_1,\ldots,a_k)$ is $\mathbf{d}$-admissible and then, as stated in Remark 2.2, Theorem 4.1 of [7] implies that there exist $q^{n/t-\lambda(\mathbf{d})} \geq q^{\varphi(n/t)} > 1$ elements $\theta\in\mathbb{F}_{q^{n/t}}$ such that $\operatorname{Tr}_{(n/t)/d_i}(\theta) = a_i$ for $1\leq i\leq k$. In particular, there exists a nonzero element $\theta_0\in\mathbb{F}_{q^{n/t}}$ with such traces in a way that $\theta_0\neq 0$. Since $\theta_0\neq 0$, Theorem 1.1 implies that there exists a primitive element $\alpha\in\mathbb{F}_{q^n}$ such that $\operatorname{Tr}_{n/(n/t)}(\alpha)=\theta_0$ and then, by the transitivity of the trace,

$$\operatorname{Tr}_{n/d_i}(\alpha) = \operatorname{Tr}_{\frac{n}{t}/d_i}(\theta_0) = a_i,\ 1\leq i\leq k.$$

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

5. Theorem 2.4 under the condition $\gcd(d_i, d_j) = 1$

In this section we discuss the existence of primitive elements of $\mathbb{F}_{q^n}$ with arbitrary prescribed traces over extensions $\mathbb{F}_{q^{d_i}}$ under the following condition:

$$\boxed{\gcd(d_i, d_j) = 1 \text{ for } 1 \le i < j \le k}.$$

We observe that the above condition is not restrictive when $k = 2$. In fact, if $d_1 < d_2$ are divisors of n and $d = \gcd(d_1, d_2)$, we have that $\mathbb{F}_{q^{d_i}} = \mathbb{F}_{Q^{e_i}}$, for $Q = q^d$, where $e_i = d_i/d$ satisfy $\gcd(e_1, e_2) = 1$. We obtain asymptotic and concrete results that are displayed in the following theorem.

THEOREM 5.1. *Let $n > 1$ be an integer that is not a prime power, $1 < k < \sigma_0(n)$ and $\mathbf{d} = (d_1, \dots, d_k) \in \Lambda_k(n)$ be such that $\gcd(d_i, d_j) = 1$ for every $1 \le i < j \le k$. Furthermore, let $\mathbf{a} = (a_1, \dots, a_k) \in \mathbb{F}(\mathbf{d})$ be a $\mathbf{d}$-admissible k-tuple. Then there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ with prescribed traces $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ provided that one of the following holds:*

(a) $k \ge 3$;
(b) $k = 2$ *and*

(b.1) $d_1 \ge 5$ *and* $q \ge 5$ *if* $(d_1, d_2) = (5, 6)$;
(b.2) $d_1 = 4$ *and* $d_2 \ge 11$, *or* $d_2 \ge 9$ *and* $q \ge 3$, *or* $d_2 = 5, 7$ *and* $q \ge e^{e^{6.7}}$;
(b.3) $d_1 = 3$ *and either* $d_2 \ge 38$, *or* $d_2 \ge 5$ *and* $q \ge e^{e^{26.1}}$.

PROOF. We may assume that $\mathrm{lcm}(d_1, \dots, d_k) = n$ since otherwise the result is directly implied by Theorem 2.5. For $k \ge 2$, the condition $\gcd(d_i, d_j) = 1$ implies that

$$\lambda(\mathbf{d}) = d_1 + \cdots + d_k - k + 1.$$

From Lemma 3.6, Theorem 2.4 and the equation above, it suffices to verify that

$$\frac{n}{2} - \sum_{i=1}^{k} d_i + k - 1 \ge \frac{n}{a} + \log_q(c_{q^n,a}) \tag{5-1}$$

for some $a \ge 3$. We always take $a = 4$ or $a = 8$. Since

$$\mathrm{lcm}(d_1, \dots, d_k) = n, \quad 2 \le d_1 < \cdots < d_k$$

and $\gcd(d_i, d_j) = 1$,

$$d_1 \cdots d_k = n.$$

We provide the proofs of items (a) and (b) separately.

5.1. The case $k \ge 3$. We split the proof into cases.
(i) $k \ge 4$: Let $2 = p_1 < p_2 < \cdots$ be the increasing sequence of the prime numbers. We have that $p_\ell \le d_\ell$ and then

$$p_\ell \le d_\ell \le \left(\frac{n}{p_1 \cdots p_{\ell-1}}\right)^{1/(k+1-\ell)}$$

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

for $1 \le \ell \le k$, where the empty product equals 1. Furthermore,

$$\frac{n}{2} - \left[\log_7\left(\frac{n}{30}\right) + 2\right]\sqrt{\frac{n}{2}} - \frac{n}{30} + 3 \ge \frac{n}{4} + 2 \tag{5-2}$$

for $n \ge 39$. Since $(n/(p_1 \cdots p_{\ell-1}))^{1/(k+1-\ell)} < \sqrt{n/2}$ for every $1 \le \ell \le k-1$ and also $n \ge 2 \cdot 3 \cdot 5 \cdot 7^{k-3} \ge 210$, the left-hand side of inequality (5-1) is greater than the left-hand side of inequality (5-2). Taking $a = 4$, the right-hand side of inequality (5-2) is greater than the right-hand side of inequality (5-1). This concludes the case $k \ge 4$.
(ii) $k = 3$: In the same way, we have that the inequality

$$\frac{n}{2} - \sqrt[3]{n} - \sqrt{\frac{n}{2}} - \frac{n}{6} + 2 \ge \frac{n}{8} + 12.2 \tag{5-3}$$

holds true for $n \ge 107$. Since the left-hand side of inequality (5-1) is greater than the left-hand side of inequality (5-3), and the right-hand side of inequality (5-3) is greater than the right-hand side of inequality (5-1) with $a = 8$, we are done unless $n \in \{30 = 2 \cdot 3 \cdot 5,\ 42 = 2 \cdot 3 \cdot 7,\ 60 = 3 \cdot 4 \cdot 5,\ 66 = 2 \cdot 3 \cdot 11,\ 70 = 2 \cdot 5 \cdot 7,\ 78 = 2 \cdot 3 \cdot 13,\ 84 = 3 \cdot 4 \cdot 7,\ 90 = 2 \cdot 5 \cdot 9,\ 102 = 2 \cdot 3 \cdot 17,\ 105 = 3 \cdot 5 \cdot 7\}$, which are the numbers smaller than 107 that split into at least three nontrivial relatively prime factors. We now consider the following cases.

(ii.1) $(d_1, d_2) = (3, 5)$: If $n \ge 60$, then $(n/2) - 3 - 5 - (n/15) + 2 \ge (n/4) + 2$ and we argue as above with $a = 4$.
(ii.2) $(d_1, d_2) = (3, 4)$: If $n \ge 42$, then $(n/2) - 3 - 4 - (n/12) + 2 \ge (n/4) + 2$ and we argue as above with $a = 4$.
(ii.3) $(d_1, d_2) = (2, 5)$: If $n \ge 47$, then $(n/2) - 2 - 5 - (n/10) + 2 \ge (n/4) + 2$ and we argue as above with $a = 4$.
(ii.4) $(d_1, d_2) = (2, 3)$: If $n \ge 60$, then $(n/2) - 2 - 3 - (n/6) + 2 \ge (n/4) + 2$ and we argue as above with $a = 4$. Hence, there only remains $n \in \{30, 42\}$.

For $n = 30$, the inequality

$$\frac{30}{2} - 2 - 3 - 5 + 2 \ge (30/8) + \log_q(4514.7)$$

holds true if $q \ge 14$ and we argue as above with $a = 8$. Therefore, there only remain the cases $q \in \{2, 3, 4, 5, 7, 8, 9, 11, 13\}$, for which the inequality $q^{n/2-\lambda(\mathbf{d})} \ge W(q^n - 1)$ can be directly verified.

For $n = 42$, the inequality

$$\frac{42}{2} - 2 - 3 - 7 + 2 \ge \frac{42}{8} + \log_q(4514.7)$$

holds true if $q \ge 5$ and we argue as above with $a = 8$. Therefore, there only remain the cases $q \in \{2, 3, 4\}$, for which the inequality $q^{n/2-\lambda(\mathbf{d})} \ge W(q^n - 1)$ can be directly verified.

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

5.2. The case $k = 2$. As in previous cases, it suffices to prove that

$$\frac{n}{2} - d_1 - d_2 + 1 \geq \frac{n}{a} + \log_q(c_{q^n,a}) \tag{5-4}$$

for $a \in \{4, 8\}$. Notice that if $d_1 \geq 8$, then $d_2 \geq 9$ and $(d_1 - 4)(d_2 - 4) \geq 20 \geq 12 + 4\log_q(c_{q^n,4})$. Therefore, inequality (5-4) holds true with $a = 4$. Table 1 provides the ranges of q, d_1, d_2 where inequality (5-4) holds and the value of a that is used.

Table 1 compiles exceptions (q, d_1, d_2) for inequality (5-4), assuming that $d_1 \geq 5$, or $d_1 = 4$ and $d_2 \geq 7$, or $d_1 = 3$ and $d_2 \geq 38$. With respect to these ranges, the exceptional triples have reasonably small parameters. Using the software SageMath we verify that such triples (q, d_1, d_2) satisfy inequality (2-2) with the exception of $(q, d_1, d_2) = (q, 5, 6)$ with $q < 5$ and $(q, d_1, d_2) = (2, 4, 9)$.

For $(q, d_1, d_2) = (q, 3, 4)$, inequality (2-2) does not hold for any prime power q. For the remaining cases, that is, $(q, d_1, d_2) = (q, 4, 5)$ and $(q, d_1, d_2) = (q, 3, d_2)$ with $5 \leq d_2 \leq 37$, Lemma 3.5(i) (or inequality (5-4) with $a = 8$ provided that $d_1 = 3$ and $17 \leq d_2 \leq 37$) ensures that there exists a computable constant q_0 depending only on d_1 and d_2 such that inequality (2-2) holds for every $q \geq q_0$. □

REMARK 5.2. For $k = 2$, $d_1 = 2$ and $n = \mathrm{lcm}(2, d_2)$, we have that $q^{n/2-\lambda(\mathbf{d})} < 1 < W(q^n - 1)$ and so Theorem 2.4 is inconclusive. Moreover, in this setting we can

TABLE 1. Ranges of q, d_1, d_2 where inequality (5-4) holds true and the value of a that is used.

d_1	d_2	q	a	d_1	d_2	q	a
7	≥ 11	for all q	4	4	≥ 19	≥ 4	8
7	10	≥ 5	4	4	17	≥ 5	8
7	9	≥ 8	4	4	15	≥ 7	8
7	8	≥ 37	8	4	13	≥ 13	8
6	≥ 15	for all q	4	4	11	≥ 29	8
6	13	≥ 3	4	4	9	≥ 274	8
6	11	≥ 3	8	4	7	$\geq 2.039 \cdot 10^7$	8
6	7	≥ 11	8	3	≥ 114	for all q	8
5	≥ 19	for all q	8	3	≥ 78	≥ 3	8
5	≥ 14	≥ 3	8	3	≥ 65	≥ 4	8
5	≥ 12	≥ 4	8	3	≥ 58	≥ 5	8
5	11	≥ 5	8	3	≥ 52	≥ 7	8
5	9	≥ 9	8	3	≥ 49	≥ 8	8
5	8	≥ 17	8	3	47	≥ 9	8
5	7	≥ 53	8	3	46	≥ 11	8
5	6	≥ 839	8	3	≥ 43	≥ 13	8
4	≥ 31	for all q	8	3	≥ 40	≥ 17	8
4	≥ 23	≥ 3	8	3	38	≥ 23	8

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

actually provide genuine exceptions. In fact, let $n = 2 \cdot N$, $N > 1$ odd, and choose $b \in \mathbb{F}_{q^2}$ in such a way that $\mathrm{Tr}_{N/1}(b) = 0$. In particular, the pair $(b, 0) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^N}$ is $(2, N)$-admissible. However, there is no primitive element $\alpha \in \mathbb{F}_{q^n}$ with zero trace over $\mathbb{F}_{q^N}$. In fact, any element $\alpha \in \mathbb{F}_{q^n}$ with zero trace over $\mathbb{F}_{q^N}$ satisfies $\alpha^{q^N} = -\alpha$ and, consequently, $\alpha^{2(q^N-1)} = 1$. But such an α cannot be primitive since $2(q^N - 1) < q^n - 1$ for every $q \geq 2$.

6. Conclusion

In this paper we discuss the existence of primitive elements of finite fields with prescribed traces in intermediate extensions. Our main result provides a sufficient condition for the existence of such elements. This condition is encoded in an inequality that is further explored in order to obtain concrete results on the existence of these elements; this is presented in Theorem 5.1.

It would be desirable to explore the validity of Theorem 5.1 without the restriction $\gcd(d_i, d_j) = 1$ or at least complete this theorem, exploring the remaining cases under this restriction. For instance, by using a sieving method that is traditional in this kind of problem (see [2, 3]), one can remove the restrictions $q \geq 5$ and $q \geq 3$ in items (b.1) and (b.2) of Theorem 5.1. Within the approach of this paper, we believe that any such improvement would have to go through sharper estimates on the character sums appearing in the proof of Theorem 2.4.

Acknowledgement

We thank the anonymous referee for suggestions that substantially improved the presentation of this work.

References

[1] S. D. Cohen, 'Primitive elements and polynomials with arbitrary trace', *Discrete Math.* **83**(1) (1990), 1–7.
[2] S. D. Cohen and S. Huczynska, 'The primitive normal basis theorem—without a computer', *J. Lond. Math. Soc.* **67**(1) (2003), 41–56.
[3] S. D. Cohen, T. Oliveira e Silva and T. Trudgian, 'On consecutive primitive elements in a finite field', *Bull. Lond. Math. Soc.* **47**(3) (2015), 418–426.
[4] W. Diffie and M. Hellman, 'New directions in cryptography', *IEEE Trans. Inform. Theory* **22**(6) (1976), 644–654.
[5] G. Kapetanakis and L. Reis, 'Variations of the primitive normal basis theorem', *Des. Codes Cryptogr.* **87**(7) (2019), 1459–1480.
[6] H. W. Lenstra Jr and R. J. Schoof, 'Primitive normal bases for finite fields', *Math. Comp.* **48**(177) (1987), 217–231.
[7] L. Reis, 'Counting solutions of special linear equations over finite fields', *Finite Fields Appl.* **68** (2020), 101759.

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press

LUCAS REIS, Departamento de Matemática,
Universidade Federal de Minas Gerais (UFMG),
Belo Horizonte, MG 30270-901, Brazil
e-mail: lucasreismat@mat.ufmg.br

SÁVIO RIBAS, Departamento de Matemática,
Universidade Federal de Ouro Preto (UFOP),
Ouro Preto, MG 35400-000, Brazil
e-mail: savio.ribas@ufop.edu.br

https://doi.org/10.1017/S1446788721000094 Published online by Cambridge University Press