Specific Irreducible Polynomials with Linearly Independent Roots over Finite Fields*

December 8, 1993

Ian F. Blake, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada. E-mail: ifblake@claude.uwaterloo.ca

Shuhong Gao, Department of Computer Science, University of Toronto, Toronto, Ontario, M5S 1A4, Canada. E-mail: sgao@cs.toronto.edu

Ronald C. Mullin, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada. E-mail: rcmullin@math.uwaterloo.ca

Abstract. In this paper we give several families of specific irreducible polynomials with the following property: if $f(x)$ is one of the given polynomials of degree n over a finite field F_q and α is a root of it, then $\alpha \in F_{q^n}$ is normal over every intermediate field between F_{q^n} and F_q. Here by $\alpha \in F_{q^n}$ being normal over a subfield F_q we mean that the algebraic conjugates $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over F_q. The degrees of the given polynomials are of the form 2^k or $\prod_{i=1}^{u} r_i^{l_i}$ where $r_1, r_2, \ldots, r_u$ are distinct odd prime factors of $q-1$ and $k, l_1, \ldots, l_u$ are arbitrary positive integers. For example, we prove that, for a prime $p \equiv 3 \bmod 4$, if $x^2 - bx - 1 \in F_p[x]$ is irreducible with $b \neq 2$ then the polynomial

$$(x-1)^{2^{k+1}} - b(x-1)^{2^k} x^{2^k} - x^{2^{k+1}}$$

has the described property over F_p for every integer $k \geq 0$. We will also show how to efficiently compute the required $b \in F_p$.

*This work was supported by grant OGP0003071.

1 Introduction and Main Results

Let q be a prime power and n a positive integer. Let F_q be the field of q elements and F_{q^n} the extension over F_q of degree n, a field of q^n elements. An element $\alpha \in F_{q^n}$ is said to be *normal* over F_q if its algebraic conjugates $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over F_q. When α is normal, the basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is called a *normal basis* for F_{q^n} over F_q. In 1888, Hensel [9] proved the normal basis theorem (for finite fields) which guarantees that there is always a normal basis for F_{q^n} over F_q for every prime power q and positive integer n. In 1986, Blessenohl and Johnsen [5] proved a stronger theorem, that is, for any prime power q and positive integer n, there is an element $\alpha \in F_{q^n}$ that is normal over every intermediate field between F_{q^n} and F_q. In this case, we say that α is *completely normal* over F_q, and the basis generated by α for F_{q^n} is called a *completely normal basis* over F_q. For simpler proofs of Blessenohl and Johnsen's theorem, see [4, 8]. The present paper is interested in the constructive aspect of the two theorems.

Another way to describe a normal or completely normal element in F_{q^n} over F_q is via its minimal polynomial over F_q. For any element $\alpha \in F_{q^n}$ of degree n, it is easily seen that its minimal polynomial over F_q is $\prod_{i=0}^{n-1}(x - \alpha^{q^i})$ which is in $F_q[x]$ and is irreducible over F_q. Let f be an irreducible polynomial of degree n in $F_q[x]$. We say that f is normal (resp. completely normal) over F_q if any of its roots in F_{q^n} is normal (resp. completely normal) over F_q. Obviously, if $\alpha \in F_{q^n}$ is normal (resp. completely normal) over F_q, then its minimal polynomial is normal (resp. completely normal) over F_q.

The problem in general is, for any given F_q and integer n, to efficiently construct a normal (resp. completely normal) basis in F_{q^n} over F_q, or equivalently a normal (resp. completely normal) polynomial in $F_q[x]$ of degree n. There are considerable amount of work on construction of normal bases over finite fields. In some special cases, normal bases are explicitly constructed in [1, 3, 6, 15, 23]. In [7, 21, 22] some general algorithms for normal bases are given, but none of them runs (deterministically) in time polynomial in n and $\log q$. However, if an irreducible polynomial of degree n in $F_q[x]$ is given then polynomial-time algorithms are known [11, 13, 24]. Also if the extended Riemann hypothesis is true, then one can construct in polynomial time a normal basis for F_{p^n} over F_p for any prime p and positive integer n, by Theorem 5.5 in [14, page 101]. For construction of completely normal bases, not much is known.

We show in this paper that completely normal polynomials over F_q can be constructed explicitly when the degree n is of the form 2^k or $\prod_{i=1}^{u} r_i^{l_i}$ where $r_1, r_2, \ldots, r_u$ are distinct odd prime factors of $q-1$ and $k, l_1, \ldots, l_u$ are arbitrary positive integers. More specifically, we will prove the following two theorems.

Theorem 1.1 *Let $a \in F_q$ be such that $x^n - a$ is irreducible in $F_q[x]$. Then*

$$ax^n - (x-1)^n \tag{1}$$

is a completely normal polynomial over F_q.

Theorem 1.2 *Let $p \equiv 3 \bmod 4$ be a prime. Assume that $x^2 - bx - c \in F_p[x]$ is irreducible with $b \neq 2$ and c a quadratic residue in F_p. Then*

$$(x-1)^{2^{k+1}} - b(x-1)^{2^k} x^{2^k} - cx^{2^{k+1}} \tag{2}$$

is a completely normal polynomial over F_{p^m} for every integer $k \geq 0$ and odd integer m.

Some comments on the theorems follow. In Theorem 1.1, to see for which n there is an element $a \in F_q$ such that $x^n - a$ is irreducible, we quote the following result.

Lemma 1.3 *[12, Thm 3.75] Let $a \in F_q^*$ with multiplicative order e. Then the binomial $x^n - a$ is irreducible in $F_q[x]$ if and only if the integer $n \geq 2$ satisfies the following conditions:*

(i) each prime factor of n divides e but not $(q-1)/e$, and

(ii) if $4|n$ then $4|(q-1)$.

As the the multiplicative order of an element in F_q is a divisor of $q-1$, we see that each prime divisor of n has to divide $q-1$. Assume that n satisfies this condition. Then the condition (i) in the lemma is satisfied if we take a to be a primitive element in F_q. This leads to the following corollary.

Corollary 1.4 *Let a be a primitive element in F_q and $n = \prod_{i=1}^{u} r_i^{l_i}$ where $r_1, r_2, \ldots, r_u$ are distinct prime factors of $q-1$. We assume that $q \equiv 1 \pmod 4$ if some $r_i = 2$. Then (1) is a completely normal polynomial over F_q for all integers $l_1, l_2, \ldots, l_u \geq 0$.*

Another interesting case is when $n = 2^k$. By Lemma 1.3, when $q \equiv 1 \bmod 4$, $x^{2^k} - a$ is irreducible for every k if and only if a is a quadratic nonresidue in F_q. Thus we have the next corollary.

Corollary 1.5 *Let $q \equiv 1 \bmod 4$ and let a be a quadratic nonresidue in F_q. Then*

$$ax^{2^k} - (x-1)^{2^k}$$

is a completely normal polynomial over F_q for every integer $k \geq 0$.

When $q \equiv 3 \bmod 4$, Lemma 1.3 implies that $x^{2^k} - a$ is reducible for all $a \in F_q$ if $k > 1$. So we cannot get normal polynomials of degree a power of 2 from irreducible binomials. However, this case is covered by Theorem 1.2.

In Theorem 1.2, we can take $c = 1$, and compute b as follows. Let v be the largest integer such that $2^v | (p+1)$. Then $v \geq 2$ as $p \equiv 3 \pmod 4$. Define b_v recursively by the formula

$$b_i = \begin{cases} \pm(\frac{b_{i-1}+1}{2})^{(p+1)/4}, & \text{for } 2 \leq i \leq v-1 \\ \pm(\frac{b_{i-1}-1}{2})^{(p+1)/4}, & \text{for } i = v, \end{cases}$$

with $b_1 = 0$, and at each step one can choose freely either $+$ or $-$ sign. Then it is shown by the authors [2] that

$$x^{2^k} - 2b_v x^{2^{k-1}} - 1$$

is irreducible over F_p for every integer $k \geq 1$. Hence the required quadratic irreducible polynomial in Theorem 1.2 can be found quickly.

For completeness, we mention the following construction of completely normal polynomials with degree a power of the characteristic.

Theorem 1.6 *Let p be a prime. Define $f_0(x) = x^p + x^{p-1} + \cdots + x - 1$, $f_1(x) = f_0(x^p - x - 1)$ and $f_k(x) = f_{k-1}^*(x^p - x - 1)$ for $k \geq 2$, where $f^*(x) = x^n f(1/x)$ denotes the reciprocal polynomial of $f(x)$ with n being its degree. Then $f_k^*(x)$ is a completely normal polynomial of degree p^{k+1} over F_p for every $k \geq 0$.*

The construction in Theorem 1.6 is due to Varshamov [25] where no proof is given; here we just provided an initial polynomial. The proof of the irreducibility of the polynomials in Theorem 1.6 can be found in [14, Section 3.4]. To prove that these polynomials

are completely normal, we just need to check that the second highest coefficient for each polynomial is not zero by Corollary 2.3 in the next section. We will leave the details to the reader.

We learned recently that Scheerhorn [20] independently constructed several families of normal polynomials over F_q of degree r^k where k is an arbitrary integer and r is a prime divisor of $q(q-1)(q+1)$. For the case $r|(q-1)$, since Scheerhorn's construction is similar to that in Theorem 1.1, we think that his polynomials are also completely normal. However, the case $r = 2$ and $q \equiv 3 \bmod 4$ is not covered by his constructions, while our theorem 1.2 deals exclusively with this case. It turns out that the proof of Theorem 1.1 is quite straightforward, but the proof of Theorem 1.2 is very lengthy. It is interesting to see if there is any simple proof of Theorem 1.2.

We point out that linear algebra plays a central role in the proofs of Theorems 1.1 and 1.2, which are given in section 3. In the next section, we will first review some basic results on normal elements in finite fields, a tailored version for that of cyclic vectors in vector spaces.

2 Preliminaries

Recall that the Frobenius map:

$$\sigma : \quad \eta \mapsto \eta^q, \quad \eta \in F_{q^n}$$

is an automorphism of F_{q^n} that fixes F_q. In particular, σ is a linear transformation of F_{q^n} viewed as a vector space of dimension n over F_q. By definition, $\alpha \in F_{q^n}$ is a normal element over F_q if and only if $\alpha, \sigma\alpha, \ldots, \sigma^{n-1}\alpha$ are linearly independent over F_q. In terms of linear algebra, this is equivalent to saying that α is a cyclic vector of F_{q^n} over F_q for σ. To characterize all the normal elements, we first determine the minimal and characteristic polynomials of σ.

Lemma 2.1 *The minimal and characteristic polynomials for σ are both $x^n - 1$.*

Proof. Note that $\sigma^n\eta = \eta^{q^n} = \eta$ for every $\eta \in F_{q^n}$, we have $\sigma^n - I = 0$. We prove that $x^n - 1$ is the minimal polynomial of σ.

Assume that there is a polynomial $f(x) = \sum_{i=0}^{n-1} f_i x^i \in F_q[x]$ of degree less than n that annihilates σ, that is,

$$\sum_{i=0}^{n-1} f_i \sigma^i \;=\; 0.$$

Then, for any $\eta \in F_{q^n}$,

$$\left(\sum_{i=0}^{n-1} f_i \sigma^i\right)\eta \;=\; \sum_{i=0}^{n-1} f_i \eta^{q^i} = 0,$$

i.e., η is a root of the polynomial $F(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$. This is impossible, since $F(x)$ has degree at most q^{n-1} and cannot have $q^n > q^{n-1}$ roots in F_{q^n}. Hence the minimal polynomial for σ is $x^n - 1$.

Since the characteristic polynomial of σ is monic of degree n and is divisible by the minimal polynomial for σ, it must also be equal to $x^n - 1$. □

As the minimal and characteristic polynomial of σ are equal, we know from linear algebra that there exists a normal element in F_{q^n} over F_q. We can actually give a more precise description of how normal elements are distributed in the whole space (Theorem 2.4) and then count them easily (Corollary 2.5). For this purpose, we first introduce some notations and give a trivial but useful characterization of normal elements.

For any polynomial $g(x) \in F_q[x]$, $g(\sigma)$ is also a linear transformation on F_{q^n}. The *null space* (or kernel) of $g(\sigma)$ is defined to be the set of all elements $\alpha \in F_{q^n}$ such that $g(\sigma)\alpha = 0$; we also call it the null space of $g(x)$. On the other hand, for any element $\alpha \in F_{q^n}$, the monic polynomial $g(x) \in F_q[x]$ of smallest degree such that $g(\sigma)\alpha = 0$ is called the *σ-Order* of α (some authors call it the σ-annihilator, the minimal polynomial, or the additive order of α). We denote this polynomial by $\mathrm{Ord}_\alpha(x)$. Note that $\mathrm{Ord}_\alpha(x)$ divides any polynomial $h(x)$ annihilating α (i.e., $h(\sigma)\alpha = 0$). In particular, for every $\alpha \in F_{q^n}$, $\mathrm{Ord}_\alpha(x)$ divides $x^n - 1$, the minimal or characteristic polynomial for σ.

Let p denote the characteristic of F_q and let $n = n_1 p^e$ where $\gcd(p, n_1) = 1$ and $e \geq 0$. For convenience we denote p^e by t. Then

$$x^n - 1 \;=\; (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^t, \tag{3}$$

where $\varphi_i(x) \in F_q[x]$, $1 \leq i \leq r$, are all the distinct irreducible factors of $x^{n_1} - 1$. For $1 \leq i \leq r$, let

$$\Phi_i(x) \;=\; (x^n - 1)/\varphi_i(x). \tag{4}$$

Then we have a useful characterization of normal elements in F_{q^n}.

Theorem 2.2 *[21] An element $\alpha \in F_{q^n}$ is normal over F_q if and only if*

$$\Phi_i(\sigma)\alpha \neq 0, \quad \text{for } i = 1, 2, \ldots, r. \tag{5}$$

Proof. By definition, an element $\alpha \in F_{q^n}$ is normal over F_q if and only if $\alpha, \sigma\alpha, \ldots, \sigma^{n-1}\alpha$ are linearly independent over F_q. This is true if and only if there is no polynomial $f(x) \in F_q[x]$ of degree less than n that annihilates α with respect to σ (i.e., $f(\sigma)\alpha = 0$), i.e., $\mathrm{Ord}_\alpha(x) = x^n - 1$. The latter holds if and only if no proper factor of $x^n - 1$ annihilates α, that is, (5) holds. □

Corollary 2.3 *[18, 8] Let $n = p^e$ and $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over F_q where p is the characteristic of F_q. Then $f(x)$ is a completely normal polynomial if and only if $a_1 \neq 0$.*

Proof. Let $\alpha \in F_{q^n}$ be a root of $f(x)$. We first determine when α is normal over F_q. As $n = p^e$, we have $x^n - 1 = (x-1)^n$. So, in (3), $r = 1$, $\varphi_1(x) = x - 1$ and $\Phi_1(x) = x^{n-1} + \cdots + x + 1$. By Theorem 2.2, $\alpha \in F_{q^n}$ is normal over F_q if and only if

$$\Phi_1(\sigma)\alpha = \sum_{i=0}^{n-1} \alpha^{q^i} = \mathrm{Tr}_{q^n|q}(\alpha) \neq 0.$$

Similarly, α is normal over an intermediate field F_{q^d}, where $d|n$, if and only if $\mathrm{Tr}_{q^n|q^d}(\alpha)$ (the trace from F_{q^n} to F_{q^d}) is not zero. Since $\mathrm{Tr}_{q^n|q}(\alpha) = \mathrm{Tr}_{q^d|q}(\mathrm{Tr}_{q^n|q^d}(\alpha))$, if $\mathrm{Tr}_{q^n|q}(\alpha) \neq 0$ then $\mathrm{Tr}_{q^n|q^d}(\alpha) \neq 0$ for every $d|n$. The proof is finished by noting that $\mathrm{Tr}_{q^n|q}(\alpha) = -a_1$. □

By Corollary 2.3, one can easily prove that the polynomials in Theorem 1.6 are indeed completely normal. We will not get into any detail here, the interested reader is referred to [14].

The following theorem enables us to see the structure of normal elements.

Theorem 2.4 (Decomposition Theorem) *Let W_i be the null space of $\varphi_i^t(x)$ and $\widetilde{W_i}$ the null space of $\varphi_i^{t-1}(x)$. Let $\overline{W_i}$ be any subspace of W_i such that $W_i = \overline{W_i} \oplus \widetilde{W_i}$. Then*

$$F_{q^n} = \sum_{i=1}^{r} \overline{W_i} \oplus \widetilde{W_i}$$

is a direct sum where $\overline{W_i}$ *has dimension* d_i *and* $\widetilde{W_i}$ *has dimension* $(t-1)d_i$ *where* d_i *is the degree of* $\varphi_i(x)$*. Furthermore, an element* $\alpha \in F_{q^n}$ *with* $\alpha = \sum_{i=1}^{r}(\overline{\alpha}_i + \widetilde{\alpha}_i)$*,* $\overline{\alpha}_i \in \overline{W_i}$*,* $\widetilde{\alpha}_i \in \widetilde{W_i}$*, is a normal element over* F_q *if and only if* $\overline{\alpha}_i \neq 0$ *for* $i = 1, 2, \ldots, r$*.*

Proof. The first part of the theorem is just the primary decomposition theorem in linear algebra [10, page 220]. We only need to prove the second part. Note that if $i \neq j$ then $\varphi_j^t(x)|\Phi_i(x)$, and $\Phi_i(\sigma)\alpha_j = 0$ for any $\alpha_j \in W_j$. So

$$\Phi_i(\sigma)\alpha \;=\; \Phi_i(\sigma)(\overline{\alpha}_i + \widetilde{\alpha}_i) \;=\; \Phi_i(\sigma)\overline{\alpha}_i + \Phi_i(\sigma)\widetilde{\alpha_i} \;=\; \Phi_i(\sigma)\overline{\alpha}_i,$$

as $\Phi_i(x)$ is divisible by $\varphi_i^{t-1}(x)$. Therefore, by Theorem 2.2, α is a normal element over F_q if and only if $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ for $i = 1, 2, \ldots, r$.

We prove that $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ if and only if $\overline{\alpha}_i \neq 0$. Obviously, if $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ then $\overline{\alpha}_i \neq 0$. Conversely, let $\overline{\alpha}_i \neq 0$. Then $\overline{\alpha}_i \in W_i \setminus \widetilde{W_i}$, which means that

$$\varphi_i^t(\sigma)\overline{\alpha}_i \;=\; 0, \quad \varphi_i^{t-1}(\sigma)\overline{\alpha}_i \;\neq\; 0.$$

So the σ-Order of $\overline{\alpha}_i$ is $\varphi_i^t(x)$. If $\Phi_i(\sigma)\overline{\alpha}_i = 0$ then $\Phi_i(x)$ would be divisible by $\varphi_i^t(x)$. This is impossible from the definition for $\Phi_i(x)$. □

If we have a basis for each of the subspaces $\overline{W_i}$ and $\widetilde{W_i}$, then by putting them together we have a basis for F_{q^n} over F_q with the property that an element in F_{q^n} represented in this basis generates a normal basis if and only if its coordinates corresponding to the subspace $\overline{W_i}$ are not simultaneously zero for each i. Note that $\overline{W_i}$ has $q^{d_i} - 1$ nonzero elements and $\widetilde{W_i}$ has $q^{(t-1)d_i}$ elements, we see that the total number of normal elements in F_{q^n} over F_q is $\prod_{i=1}^{r} q^{d_i(t-1)}(q^{d_i} - 1) = q^n \prod_{i=1}^{r}(1 - q^{-d_i})$. We state this as a corollary.

Corollary 2.5 *[9, 16] The total number of normal elements in* F_{q^n} *over* F_q *is*

$$v(n, q) \;=\; q^n \prod_{\varphi|(x^n-1)} (1 - q^{-\deg\varphi}),$$

where the product ranges over the irreducible monic factors of $x^n - 1$ *in* $F_q[x]$ *and* $\deg\varphi$ *denotes the degree of* φ*.*

In the special case that n and q are relatively prime, we have $t = 1$, $\widetilde{W_i} = \{0\}$ and $\overline{W_i} = W_i$ in Theorem 2.4. We restate this as a corollary.

Corollary 2.6 *[19, 22] Suppose that* $\gcd(n, q) = 1$. *Then*

$$x^n - 1 \;=\; \varphi_1(x)\varphi_2(x)\cdots\varphi_r(x),$$

where $\varphi_1(x), \ldots, \varphi_r(x)$ *are distinct irreducible polynomials in* $F_q[x]$. *Let* W_i *be the null space of* $\varphi_i(x)$. *Then*

$$F_{q^n} \;=\; W_1 \oplus W_2 \oplus \cdots \oplus W_r \tag{6}$$

is a direct sum of σ*-invariant subspaces; the dimension of* W_i *equals the degree of* $\varphi_i(x)$. *Furthermore* $\alpha = \sum_{i=1}^{r} \alpha_i \in F_{q^n}$, $\alpha_i \in W_i$, *is a normal element of* F_{q^n} *over* F_q *if and only if* $\alpha_i \neq 0$ *for each* i.

Assume now that $\gcd(n, q) = 1$. Note that each W_i in the decomposition (6) in Corollary 2.6 is a σ-invariant subspace and every element in W_i is annihilated by $\varphi_i(\sigma)$. As $\varphi_i(x)$ is irreducible, W_i has no proper σ-invariant subspaces. In this case, we say that W_i is an *irreducible* σ-invariant subspace. The decomposition (6) is unique in the sense that if F_{q^n} is decomposed into a direct sum of irreducible σ-invariant subspaces

$$F_{q^n} \;=\; V_1 \oplus V_2 \oplus \cdots \oplus V_s,$$

then $s = r$ and, after rearranging the order of V_i's if necessary, $V_i = W_i$ for $i = 1, 2, \ldots, r$. As an application of this observation, we look at the special case of the degree n when there exists an element $a \in F_q$ such that $x^n - a$ is irreducible over F_q.

We need some notation. A *cyclotomic coset* mod n with respect to q that contains an integer ℓ is the subset of $\{0, 1, \ldots, n-1\}$:

$$M_\ell \;=\; \{\ell, \ell q, \ldots, \ell q^{m-1}\} \mod n$$

where m is the smallest positive integer such that $\ell q^m \equiv \ell \pmod{n}$. Let S be a subset of $\{0, 1, \ldots, n-1\}$ such that M_{ℓ_1} and M_{ℓ_2} are disjoint for any ℓ_1, $\ell_2 \in S$, $\ell_1 \neq \ell_2$, and

$$\{0, 1, \ldots, n-1\} \;=\; \bigcup_{\ell \in S} M_\ell.$$

Any subset S satisfying this property is called a *complete set of representatives* of the cyclotomic cosets mod n.

Theorem 2.7 *[22] Assume that* $\gcd(n,q)=1$ *and that* $x^n-a \in F_q[x]$ *is irreducible. Let* θ *be a root of* x^n-a *and* S *a complete set of representatives of the cyclotomic cosets mod* n *with respect to* q*. For* $\ell \in S$*, let* V_ℓ *be the subspace of* F_{q^n} *spanned over* F_q *by the elements of the set* $\{\theta^m \mid m \in M_\ell\}$*. Then*

$$F_{q^n} \;=\; \sum_{\ell \in S} V_\ell \tag{7}$$

is a direct sum of irreducible σ*-invariant subspaces. Therefore an element* $\alpha = \sum_{\ell \in S} \alpha_\ell$*,* $\alpha_\ell \in V_\ell$*, is a normal element if and only if* $\alpha_\ell \neq 0$ *for* $\ell \in S$*.*

Proof. As $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of F_{q^n} over F_q, (7) is a direct sum. Obviously, each V_ℓ is σ-invariant. We just need to prove that V_ℓ is irreducible. Denote by $f_\ell(x)$ the characteristic polynomial of σ on V_ℓ. Then the degree of $f_\ell(x)$ is equal to $\dim V_\ell = |M_\ell|$, and

$$x^n - 1 \;=\; \prod_{\ell \in S} f_\ell(x). \tag{8}$$

Since for every integer $m \geq 1$ the number of irreducible factors of degree m of x^n-1 is equal to the number of $\ell \in S$ such that $|M_\ell| = m$, which is the same as the number of $f_\ell(x), \ell \in S$, such that $\deg f_\ell(x) = m$, we see that $f_\ell(x)$ is irreducible for all $\ell \in S$. So (7) is an irreducible σ-invariant decomposition. □

We are now ready to prove Theorems 1.1 and 1.2.

3 Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. We use the notation in Theorem 2.7. The irreducibility of x^n-a implies that (1) is irreducible over F_q. Let α be root of (1) in F_{q^n}. Then $\theta = (\alpha-1)/\alpha$ is a root of x^n-a. As

$$\alpha = \frac{1}{1-\theta} \;=\; \frac{1}{1-a}(1+\theta+\cdots+\theta^{n-1}) = \sum_{\ell \in S} \alpha_\ell,$$

where

$$\alpha_\ell = \frac{1}{1-a} \sum_{m \in M_\ell} \theta^m \in V_\ell \setminus \{0\}, \quad \ell \in S.$$

It follows from Theorem 2.7 that α is normal over F_q. To see that α is normal over F_{q^d} for any divisor d of n, note that $\theta^{n/d} \in F_{q^d}$ and, by Lemma 1.3, $x^{n/d} - \theta^{n/d}$ is irreducible over

F_{q^d}, which has θ as a root. Similar argument shows that $\alpha = 1/(1-\theta)$ is normal over F_{q^d} for any $d|n$. Therefore α is completely normal over F_q. □

Proof of Theorem 1.2. Note that a completely normal polynomial of degree n in $F_q[x]$ is a completely normal polynomial in $F_{q^m}[x]$ if and only if $\gcd(n,m) = 1$ [14, Lemma 4.2]. It is enough to prove that the polynomial in (2) is a completely normal polynomial over F_p, as it will remains as a completely normal polynomial over F_{p^m} for every odd integer m.

For any fixed $k \geq 0$, let α be a root of (2). Then $\alpha = 1/(1-\theta)$ where θ is a root of

$$x^{2^{k+1}} - bx^{2^k} - c. \tag{9}$$

The polynomial (2) is irreducible over F_p if and only if the polynomial (9) is irreducible over F_p. To see that (9) is irreducible, let γ be a root of $x^2 - bx - c$ in F_{p^2}. As $x^2 - bx - c$ is irreducible over F_p, we have $\gamma^p + \gamma = b$ and $\gamma^p\gamma = \gamma^{p+1} = -c$. The second equation implies that γ, and thus γ^p is a quadratic nonresidue in F_{p^2}, since $-c$ is a quadratic nonresidue in F_p. It follows from Lemma 1.3 that $x^{2^k} - \gamma$ and $x^{2^k} - \gamma^p$ are irreducible over F_{p^2} for every integer $k \geq 0$. Consequently

$$(x^{2^k} - \gamma)(x^{2^k} - \gamma^p) = x^{2^{k+1}} - bx^{2^k} - c,$$

is irreducible over F_p. So θ, and thus α has degree 2^{k+1} over F_p.

To show that α is completely normal over F_p, we need to prove that $\alpha = 1/(1-\theta)$ is normal over $F_{p^{2^i}}$ for $0 \leq i \leq k+1$. If $i \geq 1$ then the proof of Theorem 1.1 applies here for $n = 2^{k+1-i}$, $q = p^{2^i}$ and $a = \theta^{2^{k+1-i}}$, as $x^{2^{k+1-i}} - \theta^{2^{k+1-i}} \in F_{p^{2^i}}[x]$ is irreducible over $F_{p^{2^i}}$ when $i \geq 1$. It remains to prove that α is normal over F_p.

To establish this, we shall use Corollary 2.6. We first factor $x^{2^{k+1}} - 1$ over F_p, then we decompose $F_{p^{2^{k+1}}}$ into the direct sum of irreducible invariant subspaces under the Frobenius map $\sigma : \beta \mapsto \beta^p$, $\beta \in F_{p^{2^{k+1}}}$, and at the same time we prove that the projection of α in each of the subspaces is not zero. Our approach is motivated by Semaev [22, §3].

First some notations are in order. We fix that

$$p^2 - 1 = 2^{a+1}h_1, \quad p + 1 = 2^a h_2, \quad p - 1 = 2h_3, \tag{10}$$

where h_1, h_2, h_3 are odd integers. Obviously,

$$h_1 = h_2 h_3, \quad (1 + h_3) = h_2 2^{a-1} = (p+1)/2. \tag{11}$$

Let E be the multiplicative subgroup of order 2^{a+1} in F_{p^2} and let $E_i \subset E$ be the set of elements in F_{p^2} with multiplicative order exactly 2^i for $i = 0, 1, 2, \ldots, a+1$. Then $E = E_0 \cup E_1 \cup \cdots \cup E_{a+1}$. For an integer ℓ, we use $v(\ell)$ to denote the largest integer v such that $2^v | \ell$. When $\ell = 0$ we define $v(\ell) = \infty$.

The irreducible factors of $x^{2^{k+1}} - 1$ over F_p have the following forms:

(a) $x - 1$, $x + 1$;

(b) $x^2 + 1$;

(c) $x^2 - (\omega + \omega^{-1})x + 1$, for $\omega \in E_3 \cup E_4 \cup \cdots \cup E_{\min\{a,k+1\}}$;

(d) $x^2 - (\omega - \omega^{-1})x - 1$ for $\omega \in E_{a+1}$, if $k \geq a$;

(e) $x^{2^{r+1}} - (\omega - \omega^{-1})x^{2^r} - 1$ for $\omega \in E_{a+1}$ and $1 \leq r \leq k - a$.

This could be seen as follows. Let β be a root of $x^{2^{k+1}} - 1$. Then β has multiplicative order 2^i for some i with $0 \leq i \leq k+1$. The minimal polynomial $m_\beta(x)$ of β over F_p is an irreducible factor of $x^{2^{k+1}} - 1$. If $i \leq 1$ then $m_\beta(x)$ is either $x - 1$ or $x + 1$. If $2 \leq i \leq a$, then $\beta \in E \setminus E_{a+1}$ and $\beta^{2^a} = 1$. As $2^a | (p+1)$, we have $\beta^{p+1} = 1$, hence $\beta^p = \beta^{-1} \neq \beta$. So $m_\beta(x)$ is of the form (b) or (c). If $i > a$, then $\omega = \beta^{2^{i-a-1}} \in E_{a+1}$. In this case, $\omega^{2^a} = -1$, and $\omega^{p+1} = \omega^{2^a h_2} = (-1)^{h_2} = -1$, as h_2 is odd. Hence $\omega^p = -\omega^{-1}$. Since $x^{2^{i-a-1}} - \omega$ and $x^{2^{i-a-1}} - \omega^p$ are irreducible over F_{p^2} by Lemma 1.3, the polynomial

$$(x^{2^{i-a-1}} - \omega)(x^{2^{i-a-1}} - \omega^p) = x^{2^{i-a}} - (\omega - \omega^{-1})x^{2^{i-a-1}} - 1$$

is irreducible over F_p. However since this polynomial has β as a zero, we see that $m_\beta(x)$ is of the form (d) or (e).

Now we proceed to decompose $F_{p^{2^{k+1}}}$ into the direct sum of irreducible σ-invariant subspaces. For convenience, we denote $t = 2^k$. We use t and 2^k interchangeably. Thus $2t = 2^{k+1}$. Let

$$\gamma = \theta^t = \theta^{2^k}. \tag{12}$$

Then γ is a root of $x^2 - bx - c$ and

$$\sigma(\gamma) = \gamma^p = -c/\gamma, \quad \gamma^2 = b\gamma + c, \quad \gamma^{p+1} = -c. \tag{13}$$

Since $-c$ is a quadratic nonresidue in F_p, γ is a quadratic nonresidue in F_{p^2}. Thus

$$\gamma^{h_1 u} \in E_{a+1} \text{ for any odd integer } u.$$

We also have

$$\alpha = \frac{1}{1-\theta} = \frac{1}{1-\gamma^2}(1 + \theta + \cdots + \theta^{t-1} + \gamma + \gamma\theta + \cdots + \gamma\theta^{t-1}). \tag{14}$$

Since θ has degree $2t$ over F_p, the $2t$ elements

$$1, \theta, \ldots, \theta^{t-1}, \gamma, \gamma\theta, \ldots, \gamma\theta^{t-1} \tag{15}$$

form a basis for $F_{p^{2t}}$ over F_p.

For $0 \le \ell \le t-1 = 2^k - 1$, let

$$M_\ell = \{\ell p^i \bmod t : \ i = 0, 1, 2, \ldots\}$$

be the cyclotomic coset mod t with respect to p that contains ℓ. Note that $M_0 = \{0\}$, and for $\ell \neq 0$, the size of M_ℓ is equal to the smallest positive integer i such that $\ell \equiv \ell p^i \bmod 2^k$, i.e., $1 \equiv p^i \bmod 2^{k-v(\ell)}$. As 2 and 2^{a+1} divide exactly $p-1$ and p^2-1, respectively, we see that

$$|M_\ell| = \begin{cases} 1, & \text{if } \ell = 0, \\ 1, & \text{if } v(\ell) = k-1, \text{ i.e., } \ell = 2^{k-1}, \\ 2, & \text{if } k-a \le v(\ell) \le k-2, \\ 2^{k-v(\ell)-a}, & \text{if } v(\ell) < k-a. \end{cases} \tag{16}$$

Let V_ℓ be the subspace of $F_{p^{2t}}$ spanned over F_p by the elements of the set

$$\{\theta^r, \gamma\theta^r : \ r \in M_\ell\}.$$

Then V_ℓ is of dimension $2|M_\ell|$ over F_p, and V_ℓ is also a linear subspace over F_{p^2} of dimension $|M_\ell|$. Let S be a complete set of representatives of cyclotomic cosets mod t with respect to p. Then

$$F_{p^{2t}} = \sum_{\ell \in S} V_\ell$$

is a direct sum. Let

$$\alpha_\ell = \frac{1}{1-\gamma^2}(\sum_{r \in M_\ell} \theta^r + \gamma\theta^r).$$

Then $\alpha_\ell \in V_\ell$ and

$$\alpha = \sum_{\ell \in S} \alpha_\ell.$$

For each $\ell \in S$, we shall prove that V_ℓ is either an irreducible σ-invariant subspace or a direct sum of two irreducible σ-invariant subspaces. Thus we obtained all the irreducible σ-invariant subspaces of $F_{p^{2t}}$ over F_p. To prove that α is a normal element, it suffices to check that the projection of α in each of the subspaces is not zero. In the first case, the projection of α in V_ℓ is $\alpha_\ell \neq 0$, nothing to check. In the latter case, we need to find the projection of α_ℓ in each of the two irreducible subspaces of V_ℓ and verify that it is not zero. We proceed by cases of ℓ, in accordance with the types of polynomials (a)–(e):

(A) $\ell = 0$;

(B) $v(\ell) = k-1$, i.e., $\ell = 2^{k-1}$;

(C) $k-a+1 \leq v(\ell) \leq k-2$;

(D) $v(\ell) = k-a$;

(E) $v(\ell) < k-a$.

We follow the order A,B,E,C,D, since the cases (C) and (D) are more complicated to handle.

Case (A). $M_0 = \{0\}$ and $V_0 = F_p \oplus \gamma F_p = F_{p^2}$. Hence V_0 is a σ-invariant subspace with x^2-1 as annihilating polynomial. As $x^2-1 = (x-1)(x+1)$, V_0 splits into two irreducible σ-invariant subspaces. One is evidently F_p with $x-1$ as annihilating polynomial. Since $\sigma(\gamma+c/\gamma) = -(\gamma+c/\gamma)$, the other must be $(\gamma+c/\gamma)F_p$ with $x+1$ as annihilating polynomial. Therefore

$$V_0 = F_p \oplus (2\gamma - b)F_p.$$

(Note that $2\gamma - b = \gamma + c/\gamma$.) It can be checked that

$$\alpha_0 = \frac{1}{1-\gamma^2}(1+\gamma) = \frac{b-2}{2(b+c-1)} + \left(-\frac{1}{2(b+c-1)}\right)(2\gamma - b).$$

As $b \neq 2$ by assumption, the projections of α_0 (or α) into the irreducible σ-invariant subspaces with annihilating polynomials $x-1$ and $x+1$ do not vanish.

Case (B). $M_{2^{k-1}} = \{2^{k-1}\}$ and $V_{2^{k-1}} = \theta^{2^{k-1}}F_p + \gamma\theta^{2^{k-1}}F_p$. Note that $\theta^{2^k} = \gamma \in F_{p^2}$, we have $\left(\theta^{2^{k-1}(p^2-1)}\right)^2 = \left(\theta^{2^k}\right)^{p^2-1} = 1$. It follows that $\theta^{2^{k-1}(p^2-1)} = -1$, as $\theta^{2^{k-1}} \notin F_{p^2}$. Hence

$$(\sigma^2+1)(\theta^{2^{k-1}}) = \theta^{2^{k-1}}\left(\theta^{2^{k-1}(p^2-1)}+1\right) = 0,$$
$$(\sigma^2+1)(\gamma\theta^{2^{k-1}}) = \gamma\theta^{2^{k-1}}\left(\theta^{2^{k-1}(p^2-1)}+1\right) = 0.$$

Therefore $V_{2^{k-1}}$ is annihilated by x^2+1. As the dimension of $V_{2^{k-1}}$ over F_p is 2, the same as the degree of x^2+1, $V_{2^{k-1}}$ is the irreducible invariant subspace for x^2+1. The projection of α in $V_{2^{k-1}}$ is $\alpha_{2^{k-1}} \neq 0$.

Case (E). By (16), $|M_\ell| = 2^{k-v(\ell)-a}$, so the dimension of V_ℓ over F_p is $2^{k-v(\ell)-a+1}$. We prove that V_ℓ is σ-irreducible (the projection α_ℓ of α in V_ℓ is nonzero). Let $\ell = 2^{v(\ell)}\ell_1$ for ℓ_1 odd and let $p_1 = p^{2^{k-v(\ell)-a}}$. Since $k-v(\ell)-a \geq 1$, we have $p_1 = 1+2^{k-v(\ell)}w$ for w odd and

$$p_1^2 = 1 + 2^{k-v(\ell)+1}(w + 2^{k-v(\ell)-1}w^2).$$

Note that $(p^2-1)|(p_1-1)$, we have $h_1|w$ and $\gamma^{2^{k-v(\ell)}w} = 1$, as $k-v(\ell) \geq a+1$. Define $b_\ell = \gamma^{w\ell_1}$. Then

$$b_\ell \in E_{a+1}, \quad b_\ell - b_\ell^{-1} \in F_p.$$

Now let

$$\psi_\ell(x) = x^{2^{k-v(\ell)-a+1}} - (b_\ell - b_\ell^{-1})x^{2^{k-v(\ell)-a}} - 1.$$

Then $\psi_\ell(x)$ is irreducible over F_p. We show that V_ℓ is annihilated by $\psi_\ell(x)$, then V_ℓ is σ-irreducible, as its dimension is equal to the degree of $\psi_\ell(x)$.

By definition, V_ℓ is spanned over F_p by the $2^{k-v(\ell)-a+1}$ elements in

$$\{\theta^{\ell p^v}, \gamma\theta^{\ell p^v} : \quad 0 \leq v \leq 2^{k-v(\ell)-a}-1\}. \tag{17}$$

For any integer v, we have

$$\begin{aligned}
\psi_\ell(\sigma)\theta^{\ell p^v} &= \theta^{\ell p^v}\left(\theta^{\ell p^v(p_1^2-1)} - (b_\ell - b_\ell^{-1})\theta^{\ell p^v(p_1-1)} - 1\right) \\
&= \theta^{\ell p^v}\left(\theta^{2^{k+1}(w+2^{k-v(\ell)-1}w^2)\ell_1} - (b_\ell - b_\ell^{-1})\theta^{2^k w\ell_1} - 1\right)^{p^v} \\
&= \theta^{\ell p^v}\left(\gamma^{2w\ell_1} - (b_\ell - b_\ell^{-1})\gamma^{w\ell_1} - 1\right)^{p^v} = \theta^{\ell p^v}\left(b_\ell^2 - (b_\ell - b_\ell^{-1})b_\ell - 1\right)^{p^v} = 0.
\end{aligned}$$

Since $k-v(\ell)-a \geq 1$, $\psi_\ell(x)$ is a polynomial in x^2 and $\psi_\ell(\sigma)$ is actually a linear transform over F_{p^2}. So all the elements in (17) are annihilated by $\psi_\ell(x)$, and thus V_ℓ is annihilated by $\psi_\ell(x)$.

Common Arguments for Cases (C) and (D). In both cases, we shall show that V_ℓ splits into two irreducible σ-invariant subspaces of dimension 2. Let $\ell = 2^{v(\ell)}\ell_1$ for ℓ_1 odd. By assumption, $k-a \leq v(\ell) \leq k-2$. So

$$2 \leq k - v(\ell) \leq a.$$

Note that $\ell(p+1) = 2^{v(\ell)+a}\ell_1 h_2 \equiv 2^k \pmod{t}$, as $v(\ell)+a \geq k$. We see that $\ell p \equiv 2^k - \ell \pmod{t}$. Thus

$$M_\ell = \{\ell, 2^k - \ell\}.$$

The basis for V_ℓ over F_p is

$$\{\theta^\ell, \theta^{2^k-\ell}, \gamma\theta^\ell, \gamma\theta^{2^k-\ell}\} = \{\theta^\ell, \gamma\theta^{-\ell}, \gamma\theta^\ell, \gamma^2\theta^{-\ell}\}.$$

So

$$\alpha_\ell = \frac{1}{1-\gamma^2}(\theta^\ell + \gamma\theta^{-\ell} + \gamma\theta^\ell + \gamma^2\theta^{-\ell}) = \frac{1}{1-\gamma}(\theta^\ell + \gamma\theta^{-\ell}),$$

and

$$V_\ell = \theta^\ell F_{p^2} \oplus \theta^{-\ell} F_{p^2},$$

since $F_{p^2} = F_p(\gamma) = F_p \oplus \gamma F_p$. Define

$$b_\ell = \gamma^{2^{a-k}h_1\ell} = \gamma^{2^{a-k+v(\ell)}h_1\ell_1}, \quad c_\ell = \gamma^{2^{a-k}h_2\ell}. \tag{18}$$

Then

$$\sigma^2(\theta^\ell) = \theta^{p^2\ell} = \theta^\ell\theta^{\ell(p^2-1)} = \theta^\ell\theta^{2^{a+1}h_1\ell} = \theta^\ell((\theta^{2^k})^{2^{a-k}h_1\ell})^2 = \theta^\ell(\gamma^{2^{a-k}h_1\ell})^2 = \theta^\ell b_\ell^2, \tag{19}$$

and

$$\sigma(\theta^\ell) = \theta^{p\ell} = \theta^{-\ell}\theta^{\ell(p+1)} = \theta^{-\ell}\theta^{2^a h_2\ell} = \theta^{-\ell}(\theta^{2^k})^{2^{a-k}h_2\ell} = \theta^{-\ell}\gamma^{2^{a-k}h_2\ell} = \theta^{-\ell}c_\ell. \tag{20}$$

Define $d_\ell = b_\ell c_\ell$. Then

$$d_\ell = \gamma^{2^{a-k}(h_1+h_2)\ell} = \gamma^{2^{a-k}h_2(1+h_3)\ell} = (\gamma^{(p+1)/2})^{2^{a-k+v(\ell)}h_2\ell_1}. \tag{21}$$

Case (C). Assume that we are in case (C). Then $v(\ell)+a-k \geq 1$. It follows from (18) and (21) that $b_\ell \in E \setminus E_{a+1}, b_\ell + b_\ell^{-1} \in F_p$ and

$$d_\ell = (\gamma^{p+1})^{2^{a-k+v(\ell)-1}h_2\ell_1} = c^{2^{a-k+v(\ell)-1}h_2\ell_1} \in F_p.$$

For $\delta = 1, 2$, let

$$\psi_{\ell\delta}(x) = x^2 + (-1)^\delta(b_\ell + b_\ell^{-1})x + 1.$$

Then $\psi_{\ell\delta}(x)$ is irreducible in $F_p[x]$. For $\delta = 1, 2$, let $V_{\ell\delta} \subseteq V_\ell$ be the subspace spanned over F_p by

$$\alpha_{\ell\delta}^{(1)} = \theta^\ell - (-1)^\delta d_\ell\theta^{-\ell}, \text{ and } \alpha_{\ell\delta}^{(2)} = c\gamma^{-1}\theta^\ell + (-1)^\delta d_\ell\gamma\theta^{-\ell}.$$

Then $V_\ell = V_{\ell 1} \oplus V_{\ell 2}$. Since $\sigma(\theta^{-\ell}) = (\sigma(\theta^\ell))^{-1}$ and $\sigma(\gamma) = -c\gamma^{-1}$, from (19) and (20) we have

$$\begin{aligned}
\psi_{\ell\delta}(\sigma)\alpha_{\ell\delta}^{(1)} &= \theta^\ell b_\ell^2 + (-1)^\delta (b_\ell + b_\ell^{-1})\theta^{-\ell} c_\ell + \theta^\ell \\
&\quad -(-1)^\delta d_\ell \Big(\theta^{-\ell} b_\ell^{-2} + (-1)^\delta (b_\ell + b_\ell^{-1}) \theta^\ell c_\ell^{-1} + \theta^{-\ell} \Big) \\
&= \theta^\ell b_\ell (b_\ell + b_\ell^{-1})(1 - d_\ell c_\ell^{-1} b_\ell^{-1}) - (-1)^\delta \theta^{-\ell} b_\ell^{-1} (b_\ell + b_\ell^{-1})(d_\ell - c_\ell b_\ell) \\
&= 0,
\end{aligned}$$

and

$$\begin{aligned}
\psi_{\ell\delta}(\sigma)\alpha_{\ell\delta}^{(2)} &= c\Big(\gamma^{-1}\theta^\ell b_\ell^2 + (-1)^\delta (b_\ell + b_\ell^{-1})(-\gamma/c)\theta^{-\ell} c_\ell + \gamma^{-1}\theta^\ell \Big) \\
&\quad +(-1)^\delta d_\ell \Big(\gamma\theta^{-\ell} b_\ell^{-2} + (-1)^\delta (b_\ell + b_\ell^{-1})(-c\gamma^{-1})\theta^\ell c_\ell^{-1} + \gamma\theta^{-\ell} \Big) \\
&= c\gamma^{-1} b_\ell (b_\ell + b_\ell^{-1})(1 - d_\ell c_\ell^{-1} b_\ell^{-1})\theta^\ell + (-1)^\delta \gamma b_\ell^{-1} (b_\ell + b_\ell^{-1})(d_\ell - c_\ell b_\ell)\theta^{-\ell} \\
&= 0.
\end{aligned}$$

We see that $V_{\ell\delta}$ is annihilated by $\psi_{\ell\delta}(\sigma)$. As the dimension of $V_{\ell\delta}$ equals the degree of $\psi_{\ell\delta}(x)$, it follows that $V_{\ell\delta}$ is the irreducible σ-invariant subspace of $\psi_{\ell\delta}(\sigma)$ for $\delta = 1, 2$.

By using the identity $\gamma^2 = b\gamma + c$, it is easy to check that

$$\alpha_\ell = x_1\alpha_{\ell 1}^{(1)} + x_2\alpha_{\ell 1}^{(2)} + y_1\alpha_{\ell 2}^{(1)} + y_2\alpha_{\ell 2}^{(2)},$$

where

$$\begin{aligned}
x_1 &= \frac{d_\ell + c}{2d_\ell(1 - b - c)}, \qquad x_2 = \frac{d_\ell - 1}{2d_\ell(1 - b - c)}, \\
y_1 &= \frac{d_\ell - c}{2d_\ell(1 - b - c)}, \qquad y_2 = \frac{d_\ell + 1}{2d_\ell(1 - b - c)}.
\end{aligned}$$

Since $c \neq -1$ (as -1 is a quadratic nonresidue in F_p),

$$x_1 - x_2 = y_2 - y_1 = \frac{c + 1}{2d_\ell(1 - b - c)} \neq 0.$$

Therefore

$$(x_1, x_2) \neq (0, 0), \quad (y_1, y_2) \neq (0, 0),$$

that is, the projections of α_ℓ (or α) in $V_{\ell 1}$ and $V_{\ell 2}$ do not vanish.

Case (D). Finally, assume that we are in case (D), that is, $v(\ell) = k - a$. Then $b_\ell = \gamma^{h_1\ell_1} \in E_{a+1}$ and $d_\ell = (\gamma^{(p+1)/2})^{2^{a-1}h_2\ell_1}$, by (18) and (21). We have

$$(d_\ell)^{p-1} = \left(\gamma^{(p^2-1)/2}\right)^{h_2\ell_1} = (-1)^{h_2\ell_1} = -1,$$

since γ is a quadratic nonresidue in F_{p^2} and $h_2\ell_1$ is odd. Thus

$$\sigma(d_\ell) = (d_\ell)^p = -d_\ell.$$

Define $\epsilon = d_\ell/(\gamma + c\gamma^{-1})$. Since $\sigma(\gamma + c\gamma^{-1}) = -(\gamma + c\gamma^{-1})$, we have $\sigma(\epsilon) = \epsilon$. So $\epsilon \in F_p$. For $\delta = 1, 2$, let

$$\psi_{\ell\delta}(x) = x^2 + (-1)^\delta(b_\ell - b_\ell^{-1})x - 1.$$

Then $\psi_{\ell\delta}(x)$ is irreducible in $F_p[x]$. Let $V_{\ell\delta} \subseteq V_\ell$ be the subspace spanned over F_p by the two elements:

$$\begin{aligned}
\alpha_{\ell\delta}^{(1)} &= \theta^\ell + (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\theta^{-\ell}, \\
\alpha_{\ell\delta}^{(2)} &= c\gamma^{-1}\theta^\ell - (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell}.
\end{aligned}$$

Then $V_\ell = V_{\ell 1} \oplus V_{\ell 2}$. Note that

$$\begin{aligned}
\psi_{\ell\delta}(\sigma)\alpha_{\ell\delta}^{(1)} &= \theta^\ell b_\ell^2 + (-1)^\delta(b_\ell - b_\ell^{-1})\theta^{-\ell}c_\ell - \theta^\ell + (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\theta^{-\ell}b_\ell^{-2} \\
&\quad + (-1)^\delta(b_\ell - b_\ell^{-1})(-1)^\delta\epsilon(-\gamma - c\gamma^{-1})\theta^\ell c_\ell^{-1} - (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\theta^{-\ell} \\
&= b_\ell(b_\ell - b_\ell^{-1})(1 - \epsilon(\gamma + c\gamma^{-1})c_\ell^{-1}b_\ell^{-1})\theta^\ell \\
&\quad - (-1)^\delta b_\ell^{-1}(b_\ell - b_\ell^{-1})(\epsilon(\gamma + c\gamma^{-1}) - c_\ell b_\ell)\theta^{-\ell} \\
&= 0,
\end{aligned}$$

and

$$\begin{aligned}
\psi_{\ell\delta}(\sigma)\alpha_{\ell\delta}^{(2)} &= c\gamma^{-1}\theta^\ell b_\ell^2 - (-1)^\delta(b_\ell - b_\ell^{-1})\gamma\theta^{-\ell}c_\ell - c\gamma^{-1}\theta^\ell - (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell}b_\ell^{-2} \\
&\quad - (b_\ell - b_\ell^{-1})\epsilon(\gamma + c\gamma^{-1})c\gamma^{-1}\theta^\ell c_\ell^{-1} + (-1)^\delta\epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell} \\
&= c\gamma^{-1}\theta^\ell b_\ell(b_\ell - b_\ell^{-1})(1 - \epsilon(\gamma + c\gamma^{-1})c_\ell^{-1}b_\ell^{-1}) \\
&\quad + (-1)^\delta\gamma\theta^{-\ell}b_\ell^{-1}(b_\ell - b_\ell^{-1})(\epsilon(\gamma + c\gamma^{-1}) - c_\ell b_\ell) \\
&= 0.
\end{aligned}$$

We see that $V_{\ell\delta}$ is annihilated by $\psi_{\ell\delta}(\sigma)$. As the dimension of $V_{\ell\delta}$ equals the degree of $\psi_{\ell\delta}(x)$, it follows that $V_{\ell\delta}$ is the irreducible σ-invariant subspace of $\psi_{\ell\delta}(\sigma)$ for $\delta = 1, 2$.

By using the identity $\gamma^2 = b\gamma + c$, it is straightforward to check that

$$\alpha_\ell \;=\; x_1\alpha_{\ell 1}^{(1)} + x_2\alpha_{\ell 1}^{(2)} + y_1\alpha_{\ell 2}^{(1)} + y_2\alpha_{\ell 2}^{(2)},$$

where

$$\begin{aligned}
x_1 &= \frac{1}{2}\left(\frac{1}{1-b-c} + \frac{c(b-2)}{\epsilon(1-b-c)(b^2+4c)}\right),\\
x_2 &= \frac{1}{2}\left(\frac{1}{1-b-c} + \frac{2c+b}{\epsilon(1-b-c)(b^2+4c)}\right),\\
y_1 &= \frac{1}{2}\left(\frac{1}{1-b-c} - \frac{c(b-2)}{\epsilon(1-b-c)(b^2+4c)}\right),\\
y_2 &= \frac{1}{2}\left(\frac{1}{1-b-c} - \frac{2c+b}{\epsilon(1-b-c)(b^2+4c)}\right).
\end{aligned}$$

Note that

$$x_1 - x_2 = y_2 - y_1 = \frac{(c-1)b - 4c}{2\epsilon(1-b-c)(b^2+4c)}.$$

We claim that $(c-1)b - 4c \neq 0$. Suppose on the contrary that $(c-1)b - 4c = 0$. Then $c \neq 1$ and thus $b = 4c/(c-1)$. Hence the discriminant $b^2 + 4c = 4c(c+1)^2/(c-1)^2$. The irreducibility of $x^2 - bx - c$ would imply that c were a quadratic nonresidue in F_p, contradicting the assumption that c is a quadratic residue in F_p. Therefore

$$(x_1, x_2) \neq (0,0), \quad (y_1, y_2) \neq (0,0),$$

that is, the projections of α_ℓ (or α) in $V_{\ell 1}$ and $V_{\ell 2}$ do not vanish.

This completes the proof of Theorem 1.2. □

References

[1] D.W. Ash, I.F. Blake and S.A. Vanstone, "Low complexity normal bases", *Discrete Applied Math.*, **25** (1989), 191-210.

[2] I.F. Blake, S. Gao and R.C. Mullin, "Explicit factorization of $x^{2^k} + 1$ over F_p with prime $p \equiv 3 \pmod 4$", *App. Alg. in Eng., Comm. and Comp.*, **4** (1993), 89–94.

[3] I.F. Blake, S. Gao and R.C. Mullin, "Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$", to appear in *SIAM J. Discrete Mathematics.*

[4] D. Blessenohl, "Supplement zu "Eine Verschärfung des Satzes von der Normalbasis" ", *J. Algebra*, **132** (1990), 154-159.

[5] D. Blessenohl and K. Johnsen, "Eine Verschärfung des Satzes von der Normalbasis", *J. Algebra*, **103** (1986), 141-159.

[6] S. Gao and H.W. Lenstra, Jr., "Optimal normal bases", *Designs, Codes and Cryptography*, **2** (1992), 315-323.

[7] J. von zur Gathen and M. Giesbrecht, "Constructing normal bases in finite fields", *J. Symbolic Computation*, **10** (1990), 547-570.

[8] D. Hachenberger, "On completely free elements in finite fields", preprint.

[9] K. Hensel, "Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor", *J. Reine Angew. Math.*, **103** (1888), 230-237.

[10] K. Hoffman and R. Kunze, *Linear Algebra*, 2nd ed., Prentice-Hall, Englewood Cliffs, N.J., 1971.

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

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge University Press.)

[13] H. Lüneburg, "On a little but useful algorithm", *Proc. AAECC-3, Lecture Notes in Computer Science* **229**, Springer-Verlag, Berlin, 1985, 296-301.

[14] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, Boston-Dordrecht-Lancaster, 1993.

[15] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Math.*, **22** (1988/1989), 149-161.

[16] O. Ore, "Contributions to the theory of finite fields", *Trans. Amer. Math. Soc.*, **36** (1934), 243-274.

[17] D. Pei, C.C. Wang and J.K. Omura, "Normal bases of finite field $GF(2^m)$", *IEEE Trans. Info. Th.*, **32** (1986), 285-287.

[18] S. Perlis, "Normal bases of cyclic fields of prime-power degree", *Duke Math. J.*, **9** (1942), 507-517.

[19] A. Pincin, "Bases for finite fields and a canonical decomposition for a normal basis generator", *Communications in Algebra*, **17** (1989), 1337-1352.

[20] A. Scheerhorn, "Iterated constructions of normal bases over finite fields", to appear in *Finite Fields: Theory, Applications and Algorithms* (G. L. Mullen and P. J.-S. Shiue, eds.), Contemporary Mathematics, Amer. Math. Soc., 1994.

[21] Š. Schwarz, "Irreducible polynomials over finite fields with linearly independent roots", *Math. Slovaca*, **38** (1988), 147-158.

[22] I.A. Semaev, "Construction of polynomials irreducible over a finite field with linearly independent roots", *Math. USSR Sbornik*, **63** (1989), 507-519.

[23] V.M. Sidel'nikov, "On normal bases of a finite field", *Math. USSR Sbornik* **61**(1988), 485–494.

[24] S.A. Stepanov and I.E. Shparlinskiy, "On the construction of a normal basis for a finite field", *Acta Arith.* **49** (1987), 189–192.

[25] R.R. Varshamov, "A general method of synthesizing irreducible polynomials over Galois fields", *Soviet Math. Dokl.*, **29** (1984), 334-336.