Rose-
Hulman
Undergraduate
Mathematics
Journal

Subfield-Compatible Polynomials over Finite Fields

John J. Hull[a]

Volume 14, no. 2, Fall 2013

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Georgia State University

Rose-Hulman Undergraduate Mathematics Journal
Volume 14, no. 2, Fall 2013

Subfield-Compatible Polynomials over Finite Fields

John J. Hull

Abstract. Polynomial functions over finite fields are important in computer science and electrical engineering in that they present a mathematical representation of arithmetic circuits. This paper establishes necessary and sufficient conditions for polynomial functions with coefficients in a finite field and naturally restricted degrees to be compatible with given subfields. Most importantly, this is done for the case where the domain and codomain fields have differing cardinalities. These conditions, which are presented for polynomial rings in one and several variables, are developed via a universal permutation that depends only on the cardinalities of the given fields.

Acknowledgements: The author would like to thank Florian Enescu, whose skill as an instructor is surpassed only by his dedication to the development of his students. The author would also like to thank the anonymous referee for providing excellent guidance toward improving this paper. This project was undertaken as a part of the Research Initiations in Mathematics, Mathematics Education, and Statistics (RIMMES) program at Georgia State University.

1 Introduction

Let E be a finite field of characteristic p and let K and L be subfields of E. Let $g : E \to E$ be any function on E. This paper presents conditions that characterize when the restriction of g to the subfield K maps entirely into L, i.e. $g(K) \subseteq L$. When this occurs, we say that g is *K to L compatible*. When we say that a polynomial $f \in E[x]$ is K to L compatible, we mean that $f(\alpha) \in L$ for all $\alpha \in K$. It is well known that every such function g has a polynomial representation $f \in E[x]$ (c.f. Theorem 2.2). Our characterization will be expressed in terms of conditions on the coefficients of f that can be verified in practice. We will also formulate an answer to the multivariate case of this problem.

The questions handled by this paper are driven by the observation that arithmetic circuits, in whole or in part, can be represented by functions between finite fields of characteristic 2 [6]. The theory of finite fields and the functions between them therefore finds broad application in areas such as cryptography, error correction codes, and signal processing ([5], pg. 1). Interpolating polynomials representing arithmetic circuits can be used to validate hardware designs, but it is often the case that the fields over which these polynomials are being interpolated are too large to obtain a result. It may, however, be possible to examine the whole circuit as multiple functions between smaller finite fields of characteristic 2, reducing the problem of interpolating a representative polynomial to smaller, more achievable parts. Because these fields may or may not be of the same cardinality, additional efficiency may be gained by describing the form of polynomial functions that, when evaluated at elements of a specific finite field, map entirely into a target field of the same characteristic. While this is immediately applicable in the aforementioned context of characteristic 2, this paper handles the above question for finite fields of any characteristic. This is accomplished by establishing necessary and sufficient conditions on the coefficients of polynomials that satisfy the stated criteria through the development of a permutation that depends only on the cardinality of the domain field.

In Section 2 we present the terminology, definitions, and preliminary theory necessary for the development of our results. In Section 3, we develop the aforementioned permutation and present the main result of the paper in terms of the single-variable case. In Section 4, we discuss some properties that arise from the main result and in Section 5, we present a matrix test for subfield compatibility. In Section 6, we present a brief argument for the extension of all of these results to the multi-variable case.

2 Background

Where E is a field, let $E[x]$ denote the ring of polynomials in x with coefficients in E. Similarly, $E[x_1, \ldots, x_d]$ denotes the polynomial ring in d variables with coefficients in E. For any nonzero polynomial $f \in E[x]$, $deg(f)$ denotes the *degree of f*. The ideal in $E[x_1, \ldots, x_d]$ generated by the polynomials $f_1, \ldots, f_m$ is denoted by $\langle f_1, \ldots, f_m \rangle$.

Where q is some positive integer, $\mathbb{F}_q$ denotes a field of cardinality q. For a prime integer p, we will denote the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ with the symbol $\overline{\mathbb{F}_p}$. For a field E, we will

at times denote the set of non-zero elements (i.e. the multiplicative group) of E with the symbol $E^\times$. For positive integers m and n, let (m, n) denote the *greatest common divisor* of m and n and let $[m, n]$ denote the *least common multiple* of m and n. Throughout this paper, when we write $m \equiv k(mod\ n)$ for integers m, k, and n, we mean that $0 \leq k < n$.

Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields of characteristic $p > 0$. The *composite field* of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ is defined to be the smallest field containing both $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$. Recall that for k a positive integer, $\mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if k divides n ([1], pg. 310-315). Note that the above implies that for any two finite fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, the composite field of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ is $\mathbb{F}_{p^{[n,m]}}$. The following definition recalls an important endomorphism on fields of positive characteristic:

Definition 2.1. Define the endomorphism $F : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ such that for $\alpha \in \overline{\mathbb{F}_p}$, $F(\alpha) = \alpha^p$. We call F the *Frobenius endomorphism*.

It is well known that when restricted to $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$, F is an automorphism on $\mathbb{F}_{p^n}$ and F^n is the identity function. Recall also that F is an endomorphism on $\overline{\mathbb{F}_p}[x]$.

We now state an important result that follows directly from the multivariate interpolation formula found in [2]. The interpolation formula itself will not factor into our discussions, rather this result grants us the freedom to consider all functions defined on finite fields of the same characteristic as polynomial functions.

Theorem 2.2. *([2], pg. 3) Let E be a finite field. Every function $f : E^d \to E$ can be represented by a polynomial function in d variables with coefficients in E.*

Remark 2.3. Let K and L be finite fields and let E be the composite field of K and L. Consider a function $g : K \to L$. Extend the function g to $g' : E \to E$ by setting the image for all elements in $E \backslash K$ to 0 (assuming that $E \backslash K$ is nonempty). By Theorem 2.2, we can construct a polynomial $f \in E[x]$ such that $f(\alpha) = g'(\alpha) = g(\alpha) \in L$ for all $\alpha \in K$. Now had we chosen to map all the elements in $E \backslash K$ to 1 instead of 0, we would have obtained a different polynomial that when evaluated at elements of K gives the function g. With this, we can see that the polynomial f representing g on E is not unique when $E \backslash K$ is nonempty. In fact, it is not hard to see that there are exactly $|E|^{|E \backslash K|}$ ways to extend the function g to E and therefore *at least* $|E|^{|E \backslash K|}$ polynomials in $E[x]$ that give g when evaluated at elements of K. This number could be very large in relatively simple cases; for example, take $K = \mathbb{F}_8$ and $L = \mathbb{F}_4$ so that $E = \mathbb{F}_{64}$. Then by the reasoning above, for any function $g : \mathbb{F}_8 \to \mathbb{F}_4$, there are *at least* 64^{56} distinct polynomials that when evaluated at elements of $\mathbb{F}_8$ give g.

Uniqueness is therefore essential to our discussion, otherwise there would be no meaningful way to examine the relationships between subfield-compatible functions and the coefficients of polynomials representing them. We obtain this uniqueness by considering all of the polynomial functions representing a given function $g : K \to L$ as elements in a coset of a specific quotient ring. We may then choose a representative element of that coset which in turn provides us with a unique polynomial that when evaluated at K gives the function g.

Definition 2.4. Let E^d be an affine d-space and let $A \subseteq E^d$. Define the set $\mathcal{I}(A) = \{f \in E[x_1, \ldots, x_d] \mid f(a_1, \ldots, a_d) = 0 \text{ for all } (a_1, \ldots, a_d) \in A\}$. Then $\mathcal{I}(A)$ is an ideal of

$E[x_1, \ldots, x_d]$. We will refer to this ideal as *the ideal of polynomials that vanish on* A or the *ideal of vanishing.*

It is a widely known fact that the ideal of polynomials that vanish on a set also identifies polynomials that are equivalent as functions on that set by shared coset membership. This is usually taken for granted, however we prove the statement here for the benefit of the reader and list it as a lemma for ease of future reference.

Lemma 2.5. *Let* E *be a field,* $f, g \in E[x_1, \ldots, x_d]$ *and* $A \subseteq E^d$*. Then for the coset* $f + \mathcal{I}(A)$ *in the quotient ring* $E[x_1, \ldots, x_d]/\mathcal{I}(A)$*,* $g \in f + \mathcal{I}(A)$ *if and only if* $g(\alpha) = f(\alpha)$ *for all* $\alpha \in A$*.*

Proof. The polynomial g is in the coset $f + \mathcal{I}(A)$ if and only if $g - f \in \mathcal{I}(A)$ if and only if $g(\alpha) - f(\alpha) = 0$ for all $\alpha \in A$ if and only if $g(\alpha) = f(\alpha)$ for all $\alpha \in A$. □

The above shows that choosing a unique representative of a coset in $E[x_1, \ldots, x_d]/\mathcal{I}(A)$ is equivalent to choosing a unique polynomial representation of all functions that are equivalent when restricted to A. As we wish to handle the multivariate case of our problem, we turn to Gröbner bases to obtain unique representatives of polynomials that are equivalent on a set.

Definition 2.6. A *Gröbner basis* for an ideal I in the polynomial ring $E[x_1, \ldots, x_d]$ is a finite set of generators $\{g_1, \ldots, g_m\}$ for I whose leading terms generate the ideal of all leading terms in I.

Theorem 2.7. *([3], pg. 321-322) Fix a monomial ordering on* $R = E[x_1, \ldots, x_d]$ *and suppose* $\{g_1, \ldots, g_m\}$ *is a Gröbner basis for the nonzero ideal* I *in* R*. Then*

1. *Every polynomial* $f \in R$ *can be written uniquely in the form* $f = f_I + r$ *for some* $f_I \in I$ *so that no nonzero term of* r *is divisible by the leading term of* g_i *for any* $i = 1, \ldots, m$*.*

2. *The remainder* r *provides a unique representative for the coset of* f *in the quotient ring* $E[x_1, \ldots, x_d]/I$*.*

We note here that the remainder term remains the same regardless of choice of Gröbner basis for I. We have now collected enough information to define the unique polynomial representative of a function on particular set.

Definition 2.8. (Minimal Representations) Let E be a field, $f \in E[x_1, \ldots, x_d]$ and $A \subseteq E^d$. Let $G = \{g_1, \ldots, g_m\} \subset E[x_1, \ldots, x_d]$ be a Gröbner basis for $\mathcal{I}(A)$, and let f_r be the unique remainder term such that $f = f_{\mathcal{I}(A)} + f_r$ for $f_{\mathcal{I}(A)} \in \mathcal{I}(A)$ and no nonzero term of f_r is divisible by any leading term of the polynomials in G. We call f_r the *minimal representation of* f *with respect to* A. If $f = f_r$, we say that f is *minimally represented.*

Now we return to finite fields and give an explicit set of generators for the ideal of vanishing with respect to a specific field.

Theorem 2.9. *([7], pg. 35) Let $q = p^n$. The ideal of polynomials that vanish on $\mathbb{F}_q^d$ is generated by the set $\{x_1^q - x_1, \ldots, x_d^q - x_d\}$ in $\overline{\mathbb{F}_p}[x_1, \ldots, x_d]$.*

For a polynomial $g \in K[x_1, \ldots, x_d]$, let $LT(g)$ denote the leading term of g with respect to a chosen monomial ordering. For two polynomials $f_1, f_2 \in K[x_1, \ldots, x_d]$, define $S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2$ where M is the monic least common multiple of monomial terms $LT(f_1)$ and $LT(f_1)$.

Proposition 2.10. *(Buchberger's Criterion) ([3], pg 324) Let $R = E[x_1, \ldots, x_d]$ and fix a monomial ordering on R. If $I = \langle g_1, \ldots, g_m \rangle$ is a nonzero ideal in R, then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j) \equiv 0$ mod G for $1 \leq i < j \leq m$.*

We now state a well known result regarding the set of generators in Theorem 2.9.

Proposition 2.11. *Let $q = p^n$ and $G = \{x_1^q - x_1, \ldots, x_d^q - x_d\} \subset \overline{\mathbb{F}_p}[x_1, \ldots, x_d]$. Then G is a Gröbner basis for the ideal $\mathcal{I}(\mathbb{F}_q^d)$.*

Proof. By Theorem 2.9, the set G generates the ideal $\mathcal{I}(\mathbb{F}_q^d)$. For any $i, j \in \{1, \ldots, d\}$, $S(x_i^q - x_i, x_j^q - x_j) = x_j^q(x_i^q - x_i) - x_i^q(x_j^q - x_j)$, hence $S(x_i^q - x_i, x_j^q - x_j) \equiv 0$ mod G for every $i, j \in \{1, \ldots, d\}$. Therefore by Buchberger's criterion, G is a Gröbner basis for $\mathcal{I}(\mathbb{F}_q^d)$. □

3 Single Variable Case

Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields of characteristic $p > 0$. We restate here that our goal is to present necessary and sufficient conditions on the coefficients of a polynomial $f \in \overline{\mathbb{F}_p}[x]$ so that $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$. Note that we have chosen to examine polynomials in $\overline{\mathbb{F}_p}[x]$ as opposed to the polynomial ring over any particular finite field containing both $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$. This provides sufficient generality for our problem; however, it will be shown in Proposition 2.3 that if $f \in \overline{\mathbb{F}_p}[x]$ is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible *and* minimally represented with respect to $\mathbb{F}_{p^n}$, then f necessarily has coefficients in $\mathbb{F}_{p^{[n,m]}}$.

In the following proposition, we exhibit a method for deriving minimal representations with respect to a particular finite field that escapes the use of the Euclidian algorithm. Note that if $f \in \mathcal{I}(\mathbb{F}_{p^n})$, then $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$ trivially and by definition we must have that $f_r = 0$. For this reason, it is enough to discuss the minimal representations of polynomials that do not vanish on $\mathbb{F}_{p^n}$.

Proposition 3.1. *Let $f \in \overline{\mathbb{F}_p}[x] \backslash \mathcal{I}(\mathbb{F}_{p^n})$. Then the minimal representation of f with respect to $\mathbb{F}_{p^n}$ is the nonzero polynomial $f_r \in \overline{\mathbb{F}_p}[x]$ such that $deg\,(f_r) < p^n$ and $f(\alpha) = f_r(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$. Furthermore, each coefficient of f_r is a sum of coefficients of f.*

Proof. By definition and the special case of Theorem 2.9 where $d = 1$, the minimal representation of f with respect to $\mathbb{F}_{p^n}$ is the polynomial $f_r \in \overline{\mathbb{F}_p}[x]$ such that $f = c(x^{p^n} - x) + f_r$ for some $c \in \overline{\mathbb{F}_p}[x]$ so that no nonzero term of f_r is divisible x^{p^n}. It is clear then that

$deg\,(f_r) < p^n$ and as $f - f_r \in \mathcal{I}(\mathbb{F}_{p^n})$, we have that $f \in f_r + \mathcal{I}(\mathbb{F}_{p^n})$ which implies that $f(\alpha) = f_r(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$.

Furthermore, suppose that $deg\,(f) \geq p^n$. As $\alpha^{p^n} = \alpha$ for each $\alpha \in \mathbb{F}_{p^n}$, we can form a polynomial g such that $deg\,(g) < p^n$ and the coefficients of g are sums of coefficients of terms in f that have degree greater than or equal to p^n and coefficients of terms in f that have degree strictly less than p^n under the assumption that $x^{p^n} = x$. By construction, $deg\,(g) < p^n$ and $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$, hence by the uniqueness of minimal representations, $g = f_r$. □

We emphasize here that the only requirement for a nonzero polynomial $f \in \overline{\mathbb{F}_p}[x]$ to be minimally represented with respect to $\mathbb{F}_{p^n}$ is that it has degree strictly less than p^n. Due to the fact that the minimal representation of a function defined on $\mathbb{F}_{p^n}$ is essentially the polynomial of minimal degree representing that function, our problem may be reduced entirely to the consideration of minimally represented polynomials. We now prove the claim made at the beginning of this section regarding the coefficients of $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials that are minimally represented with respect to $\mathbb{F}_{p^n}$.

Proposition 3.2. *If $f \in \overline{\mathbb{F}_p}[x]$ is an $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial that is minimally represented with respect to $\mathbb{F}_{p^n}$, then f has coefficients in $\mathbb{F}_{p^{[n,m]}}$.*

Proof. Define the function $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ by $\alpha \mapsto f(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$. Extend g to $g' : \mathbb{F}_{p^{[n,m]}} \to \mathbb{F}_{p^{[n,m]}}$ by $\beta \mapsto g(\beta)$ if $\beta \in \mathbb{F}_{p^n}$ and $\beta \mapsto 0$ otherwise. By Theorem 2.2, there exists a polynomial $h \in \mathbb{F}_{p^{[n,m]}}[x]$ so that $h(\beta) = g'(\beta) = g(\beta) = f(\beta)$ for all $\beta \in \mathbb{F}_{p^n}$. Let h_r be the minimal representation of h with respect to $\mathbb{F}_{p^n}$. By Proposition 3.1, each coefficient of h_r is a sum of coefficients of h, so it follows that h_r has coefficients in $\mathbb{F}_{p^{[n,m]}}$. By the uniqueness of minimal representations, $h_r = f$, hence f has coefficients in $\mathbb{F}_{p^{[n,m]}}$. □

Now we present an important function based on the Frobenius endomorphism. We will later show that this function gives rigid structure to minimally represented subfield-compatible polynomials over finite fields.

Definition 3.3. (The Frobenius Permutation) Let β be a generator for the multiplicative group of $\mathbb{F}_{p^n}$. Define the function $\varphi : \{0, \ldots, p^n - 1\} \to \{0, \ldots, p^n - 1\}$ so that for $i \in \{1, \ldots, p^n - 1\}$, $F(\beta^i) = \beta^{\varphi(i)}$ where $\varphi(i) \in \{1, \ldots, p^n - 1\}$ and $\varphi(0) = 0$.

The following proposition shows that the above function is a permutation and gives some of its other properties. We will refer to φ as the *Frobenius permutation of order n* in later discussions and we will at times write φ_n to distinguish that the order of φ is n. Note that the proposition below shows that φ does not depend on the choice of the generator β for $\mathbb{F}_{p^n}^{\times}$. The permutation φ *does* depend on the characteristic p, therefore the characteristic will be made known when it is not clear from context.

Proposition 3.4. *Let φ be as defined above. Then φ is a permutation of order n on the set $\{0, \ldots, p^n - 1\}$ (i.e. $\varphi^n = \varepsilon$). Furthermore, for $i \in \{0, \ldots, p^n - 1\}$, $\varphi(i) = q + r$ where $pi = p^n q + r$, $0 \leq r < p^n$.*

Proof. Let $i, j \in \{1, \ldots, p^n - 1\}$ and suppose that $\varphi(i) = \varphi(j)$. Then $\beta^{\varphi(i)} = \beta^{\varphi(j)}$ and $F(\beta^i) = F(\beta^j)$. As F is an automorphism on $\mathbb{F}_{p^n}$ and therefore injection on $\mathbb{F}_{p^n}$, $\beta^i = \beta^j$. As β^k is unique for $k \in \{1, \ldots, p^n - 1\}$, $i = j$, hence φ injects into the set $\{1, \ldots, p^n - 1\}$. As the set $\{1, \ldots, p^n - 1\}$ is finite, φ is a bijection and hence a permutation on $\{1, \ldots, p^n - 1\}$.

Now let $i \in \{1, \ldots, p^n - 1\}$ and note that $F^k(\beta^i) = \beta^{\varphi^k(i)}$ for all k. Since $F^n(\beta^i) = \beta^i$, we have that $\varphi^n(i) = i$. As $F^k(\beta) \neq \beta$ for any $k = 1, \ldots, n-1$, it follows that the order of φ is n on $\{1, \ldots, p^n - 1\}$. $\varphi(0) = 0$ by definition, so 0 is a fixed point of φ. Because we can adjoin any arbitrary fixed point to a permutation and it remains a permutation of the same order, it follows that φ is a permutation of order n on the set $\{0, \ldots, p^n - 1\}$.

Let $i \in \{1, \ldots, p^n - 1\}$ and assume that $pi = p^n q + r$ with $0 \leq r < p^n$. As $i \in \{1, \ldots, p^n - 1\}$, clearly $q + r > 0$. We claim that $q \leq p - 1$. Otherwise, $q \geq p$ and $pi = p^n q + r \geq p^n p$ which implies that $p(i - p^n) \geq 0$, contradicting $i \in \{0, \ldots, p^n - 1\}$. We also claim that $r \leq p^n - p$. As $pi = p^n q + r$, we see that $r \equiv 0 (mod\ p)$. This implies that p divides r and consequently that $r = pm$ for some nonnegative integer m. If $m \geq p^{n-1}$, then $r \geq p^n$ which contradicts $0 \leq r < p^n$. Conclude that $m \leq p^{n-1} - 1$ and hence $r \leq p^n - p$. Consequently, for any $i \in \{1, \ldots, p^n - 1\}$ where $pi = p^n q + r$ and $0 \leq r < p^n$, we have that $0 < q + r \leq p - 1 + p^n - p = p^n - 1$, so $q + r \in \{1, \ldots, p^n - 1\}$. By definition, $\beta^{\varphi(i)} = F(\beta^i) = \beta^{pi} = \beta^{p^n q + r} = \beta^{p^n q} \beta^r = \beta^q \beta^r = \beta^{q+r}$. As β^k is distinct for $k \in \{1, \ldots, p^n - 1\}$, $\beta^{\varphi(i)} = \beta^{q+r}$ implies that $\varphi(i) = q + r$. Since $p0 = p^n 0 + 0 = \varphi(0)$, conclude that for all $i \in \{0, \ldots, p^n - 1\}$, $\varphi(i) = q + r$ where $pi = p^n q + r$, $0 \leq r < p^n$. □

Remark 3.5. It should be noted here that the Frobenius permutation is a permutation defined on the set of indices of coefficients a_i corresponding to terms $a_i x^i$ of degree strictly less than p^n. This is also to say that the Frobenius permutation is defined on the indices of the coefficients of any polynomial that is minimally represented with respect to $\mathbb{F}_{p^n}$.

The following proposition shows that the Frobenius permutation can be applied not only to powers of a generator of $\mathbb{F}_{p^n}^{\times}$ but to powers of any element of $\mathbb{F}_{p^n}$ as well.

Proposition 3.6. *Let $i \in \{0, \ldots, p^n - 1\}$. Then for all $\alpha \in \mathbb{F}_{p^n}$, $F(\alpha^i) = \alpha^{\varphi(i)}$ where φ is the Frobenius permutation of order n.*

Proof. For all $\alpha \in \mathbb{F}_{p^n}$, $\alpha^{p^n} = \alpha$. If $pi = p^n q + r$ with $0 \leq r < p^n$, then $F(\alpha^i) = (\alpha^i)^p = \alpha^{pi} = \alpha^{p^n q + r} = \alpha^{q+r} = \alpha^{\varphi(i)}$. □

Next, we show that the Frobenius permutation of order n can be applied to obtain the minimal representation (with respect to $\mathbb{F}_{p^n}$) of $F^k(f)$ when f is any minimally represented polynomial in $\overline{\mathbb{F}_p}[x]$.

Proposition 3.7. *Let $f \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$ (i.e. $deg(f) < p^n$). If $f = \sum_{i=0}^{p^n - 1} a_i x^i$, then for all nonnegative integers k, the minimal representation of the k^{th} power of the Frobenius endomorphism applied to f $\left(i.e.\ F^k(f)_r\right)$ is given by the polynomial $\sum_{i=0}^{p^n - 1} a_i^{p^k} x^{\varphi^k(i)}$ where φ is the Frobenius permutation of order n.*

Proof. We proceed by induction on k. For $k = 0$, f is minimally represented and there is nothing to show. Assume that the statement is true for $k \geq 0$. As φ is a permutation on the set $\{0, \ldots, p^n - 1\}$, the degree of $\sum_{i=0}^{p^n-1} a_i^{p^{k+1}} x^{\varphi^{k+1}(i)}$ is strictly less than p^n, so by Proposition 3.1 it is sufficient to show function equality on $\mathbb{F}_{p^n}$. By our inductive hypothesis, $F^k(f)_r = \sum_{i=0}^{p^n-1} a_i^{p^k} x^{\varphi^k(i)}$, which is also to say that $F^k(f)_r(\alpha) = F^k(f)(\alpha) = \sum_{i=0}^{p^n-1} a_i^{p^k} \alpha^{\varphi^k(i)}$ for all $\alpha \in \mathbb{F}_{p^n}$. Thus for all $\alpha \in \mathbb{F}_{p^n}$:

$$\begin{aligned} F^{k+1}(f)(\alpha) &= F(F^k(f)(\alpha)) \\ &= F\left(\sum_{i=0}^{p^n-1} a_i^{p^k} \alpha^{\varphi^k(i)}\right) \\ &= \sum_{i=0}^{p^n-1} F(a_i^{p^k} \alpha^{\varphi^k(i)}) \\ &= \sum_{i=0}^{p^n-1} (a_i^{p^k})^p \alpha^{\varphi(\varphi^k(i))} \\ &= \sum_{i=0}^{p^n-1} a_i^{p^{k+1}} \alpha^{\varphi^{k+1}(i)} \end{aligned}$$

Therefore $F^{k+1}(f)_r = \sum_{i=0}^{p^n-1} a_i^{p^{k+1}} x^{\varphi^{k+1}(i)}$ and the statement is true for all nonnegative integers.

□

We now collect the preceding arguments to provide the main result. In summary, the following theorem shows that given any two finite fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, the minimally represented polynomials that map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ have a very specific form in terms of their coefficients. This form depends essentially on the Frobenius permutation of order n.

Theorem 3.8. *Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields. Let $f \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$, $f = \sum_{i=0}^{p^n-1} a_i x^i$. Then $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$ if and only if $a_i^{p^m} = a_{\varphi^k(i)}$ for each $i \in \{0, \ldots, p^n - 1\}$ where φ is the Frobenius permutation of order n and $m \equiv k (mod\ n)$.*

Proof. It is clear that $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$ if and only if the image of f evaluated at every element of $\mathbb{F}_{p^n}$ is fixed by the m^{th} power of the Frobenius endomorphism, which is to say that $F^m(f(\alpha)) = F^m(f)(\alpha) = f(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$. Since the minimal representation of $F^m(f)$ with respect to $\mathbb{F}_{p^n}$ and $F^m(f)$ are equivalent as functions when evaluated at elements of $\mathbb{F}_{p^n}$, $F^m(f)(\alpha) = f(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$ if and only if $F^m(f)_r(\alpha) = f(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$, and the preceding is true if and only if $F^m(f)_r \in f + \mathcal{I}(\mathbb{F}_{p^n})$ by Lemma 2.5. As we took f to be minimally represented and minimal representations are unique, we have that

$F^m(f)_r = f \in \overline{\mathbb{F}_p}[x]$. As $F^m(f)_r = \sum_{i=0}^{p^n-1} a_i^{p^m} x^{\varphi^m(i)}$ (by Proposition 3.7) and $f = \sum_{i=0}^{p^n-1} a_i x^i$, it follows that $a_i^{p^m} x^{\varphi^m(i)} = a_{\varphi^m(i)} x^{\varphi^m(i)}$ for each $i \in \{0, \ldots, p^n - 1\}$ which in turn implies that $a_i^{p^m} = a_{\varphi^m(i)}$ for each $i \in \{0, \ldots, p^n - 1\}$. Since the order of φ is n and $m \equiv k(mod\ n)$, $\varphi^m(i) = \varphi^k(i)$ for each i and the result follows. □

4 Consequences of the Main Result

We will now examine the Frobenius permutation in order to deduce some of the properties that it imposes on subfield-compatible polynomials. For a group G and an element a of G, let $|a|$ denote the order of a. For a positive integer l, let S_l denote the group of all permutations on the set $\{1, \ldots, l\}$. The following facts and terminology related to the permutation group S_l can be found in [8]. If $\sigma \in S_l$ and $i \in \{1, \ldots, l\}$, then σ *fixes* i if $\sigma(i) = i$, and σ *moves* i if $\sigma(i) \neq i$. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, \ldots, l\}$. If $\sigma \in S_l$ fixes all the other integers (if any) and if $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$, then we say σ is a *cycle* and that it has (or is of) *length* r. Two permutations $\sigma, \mu \in S_l$ are called *disjoint* if every i moved by one is fixed by the other. Note that if σ and μ are disjoint, $\sigma\mu = \mu\sigma$, that is, the multiplication (composition) of disjoint permutations commutes. This is also to say that for disjoint permutations $\sigma_1, \sigma_2, \ldots, \sigma_q$, $(\sigma_1\sigma_2 \cdots \sigma_q)^k = \sigma_1^k\sigma_2^k \cdots \sigma_q^k$ for any integer k.

For now we will examine the Frobenius permutation φ_n as an element of S_{p^n-1}, that is, we will ignore that φ_n is defined on $\{0, \ldots, p^n - 1\}$ and consider it only as it acts on the set $\{1, \ldots, p^n - 1\}$. This is reasonable as 0 is always a fixed point of φ_n and does not factor into its behavior under the group operation of function composition. It is also the case that $p^n - 1$ is always a fixed point of φ_n, however we choose to retain its consideration for convenience.

Proposition 4.1. *([8], pg. 113) Every permutation $\sigma \in S_l$ is either a cycle or the product of disjoint cycles.*

Definition 4.2. A *complete factorization* of a permutation σ is a factorization of σ into disjoint cycles that contains a cycle of length one for every i fixed by σ.

Theorem 4.3. *([8], pg. 114-115) Let $\sigma \in S_l$ and let $\sigma = \tau_1 \cdots \tau_q$ be a complete factorization into disjoint cycles. This factorization is unique up to the order in which the cycles occur.*

Proposition 4.4. *([4], pg. 48-49) For any $\sigma \in S_l$, the order of σ is the least common multiple of the lengths of the disjoint cycles in the complete factorization of σ.*

Note that since the length and order of a cycle are equal, we will use these terms interchangeably when acceptable.

Definition 4.5. A permutation $\mu \in S_l$ is a *regular permutation* if μ is the product of disjoint cycles of equal length.

Proposition 4.6. *([3], 57) Let G be a group and let $a \in G$, $j \in \mathbb{Z}^+$. If $|a| = k < \infty$, then $|a^j| = \frac{k}{(j,k)}$.*

Proposition 4.7. *Let $\sigma \in S_l$ be a cycle of length $n > 1$. Then for each positive integer k, σ^k is either a cycle of length n or a regular permutation that is the product of disjoint cycles of length $\frac{n}{(k,n)}$.*

Proof. Let k be any positive integer. Suppose that σ^k is a nontrivial cycle of length $r > 1$. Let A be the set of elements $i_1, \ldots, i_n$ moved by σ so that $\sigma(i_j) = i_{j+1}$ and $\sigma(i_n) = i_1$. Let B denote the set of elements moved by σ^k. If $\sigma(i) = i$, then $\sigma^k(i) = i$, so by contraposition, $B \subseteq A$. If B is a proper subset of A, then there exists some i_j in A such that $\sigma^k(i_j) = i_j$. But then since $\sigma(i_j) = i_{j+1}$, we have that $\sigma^k(i_j) = \sigma^{k-1}(i_{j+1}) = i_j$, hence $\sigma^k(i_{j+1}) = i_{j+1}$. This implies that $B = \emptyset$, which is false by the hypothesis that σ^k is a nontrivial cycle. Conclude that $B = A$ and that $r = n$.

Suppose now that $\sigma^k = \tau_1\tau_2\cdots\tau_q$ for disjoint cycles $\tau_1, \tau_2, \ldots, \tau_q$. Suppose that i_j is an element moved by σ^k such that i_j is moved by a disjoint cycle τ_j and $|\tau_j| = r$. As $|\sigma^k| = \frac{n}{(k,n)}$, r must divide $\frac{n}{(k,n)}$ (by Propsition 4.4), therefore $r \leq \frac{n}{(k,n)}$. If $r < \frac{n}{(k,n)}$, then $kr < k\frac{n}{(k,n)} = [k,n]$. Since kr is a multiple of k and $kr < [k,n]$, we see that kr is not a multiple of n. But then $(\sigma^k)^r(i_j) = \sigma^{kr}(i_j) = i_j$ and as before, if σ^{kr} fixes one element moved by σ, it must fix all, and since n is the order of σ, n must divide kr, a contradiction. Conclude that $r = \frac{n}{(k,n)}$. Since our choice of τ_j was arbitrary, it follows that σ^k is a regular permutation that is the product of disjoint cycles of length $\frac{n}{(k,n)}$. □

Proposition 4.8. *Let $\sigma \in S_l$ where $|\sigma| = n$. Assume that the complete factorization of σ contains a disjoint cycle of length n. Then for every positive integer k, the complete factorization of the permutation σ^k contains a cycle of length $\frac{n}{(k,n)}$.*

Proof. Suppose that the complete factorization of σ is given by $\sigma = \tau_1 \cdots \tau_q$ for disjoint cycles $\tau_1, \ldots, \tau_q$. Suppose that one of those cycles, say τ_s, has length n. Note that $\sigma^k = \tau_1^k \cdots \tau_q^k$. By Proposition 4.7, τ_s^k is either a cycle of length n or τ_s^k is a regular permutation that is the product of cycles of length $\frac{n}{(k,n)}$. If τ_s^k is a cycle of length n, then $|\tau_s^k| = \frac{n}{(k,n)} = n$, i.e. $(k,n) = 1$. It follows then that in either case, the complete factorization of $\sigma^k = \tau_1^k \cdots \tau_q^k = \mu_1 \cdots \mu_m$ for disjoint cycles $\mu_1, \ldots, \mu_m$ contains at least one cycle μ_i of length $\frac{n}{(k,n)}$. □

Proposition 4.9. *For every positive integer k dividing n, there is a cycle of length k in the complete factorization of φ_n, the Frobenius permutation of order n.*

Proof. Let k be some positive integer dividing n and let β be a generator for $\mathbb{F}_{p^n}^\times$. As k divides n, $\mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^n}$. This implies that there exists some element $\alpha = \beta^j \in \mathbb{F}_{p^n}^\times$, $j \in \{1, \ldots, p^n - 1\}$, such that α is a generator for $\mathbb{F}_{p^k}^\times$. Thus $F^k(\alpha) = \alpha$ and $F^l(\alpha) \neq \alpha$ for any $l = 1, \ldots, k-1$. This is also to say that $F^k(\beta^j) = \beta^{\varphi_n^k(j)} = \beta^j$ and $F^l(\beta^j) = \beta^{\varphi_n^l(j)} \neq \beta^j$ for any $l = 1, \ldots, k-1$, hence $\varphi_n^k(j) = j$ and $\varphi_n^l(j) \neq j$ for any $l = 1, \ldots, k-1$. It follows then that j is moved by some cycle in the complete factorization of φ_n which has order k, hence for every k dividing n, there is a cycle of length k in the complete factorization of φ_n. □

By Proposition 3.2, the set of available coefficients for minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials is a subset of the composite field $\mathbb{F}_{p^{[n,m]}}$. Because the form of such polynomials is restricted by the Frobenius permutation, it would be a reasonable intuition that the reverse inclusion might not hold; however, the following theorem shows that this is not the case. That is, we show that the set of available coefficients for minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials is the entire field $\mathbb{F}_{p^{[n,m]}}$.

Theorem 4.10. *If $\alpha \in \mathbb{F}_{p^{[n,m]}}$ then α is a coefficient in a minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial.*

Proof. Choose any element $\alpha \in \mathbb{F}_{p^{[n,m]}}$ and suppose also that $m \equiv k(mod\ n)$. By Proposition 4.9, the complete factorization of $\varphi_n \in S_{p^n-1}$ contains a disjoint cycle of length n, and by Proposition 4.8, the complete factorization of φ_n^k contains a disjoint cycle of length $l = \frac{n}{(n,k)}$. Choose some $j \in \{1, \ldots, p^n - 1\}$ such that j is moved by a cycle of length l in the complete factorization of φ_n^k.

Construct the polynomial $f = \alpha x^j + \alpha^{p^m} x^{\varphi_n^k(j)} + \alpha^{p^{2m}} x^{\varphi_n^{2k}(j)} + \cdots + \alpha^{p^{(l-1)m}} x^{\varphi_n^{(l-1)k}(j)}$. Note that since $m \equiv k(mod\ n)$, $(n,k) = (n,m)$, hence $l = \frac{n}{(n,m)}$. It follows then that $(\alpha^{p^{(l-1)m}})^{p^m} = \alpha^{p^{lm}} = \alpha^{p^{[n,m]}} = \alpha$ by $\alpha \in \mathbb{F}_{p^{[n,m]}}$. Also note that $(\varphi_n^{(l-1)k})^k(j) = \varphi_n^{lk}(j) = j$. As φ_n^k permutes the set $\{1, \ldots, p^n - 1\}$, $deg\,(f) < p^n$, so applying Theorem 3.8, we have that $f\,(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$. □

The construction of the arbitrary polynomial in the proof of Theorem 4.10 motivates the following definition.

Definition 4.11. Let E be a field. A *cycle polynomial* is a polynomial $f \in E[x]$ such that there exists a cycle σ of length r, a term $a_i x^i$ in f, and a positive integer k such that $a_i^{k^r} = a_i$ so that we can write:

$$f = a_i x^i + a_i^k x^{\sigma(i)} + a_i^{k^2} x^{\sigma^2(i)} + \cdots + a_i^{k^{r-1}} x^{\sigma^{r-1}(i)}$$

In the above case, we say that f is *a cycle polynomial corresponding to* σ and that $a_i x^i$ is *a generating term* for f.

For a permutation $\sigma \in S_l$ and $i \in \{1, \ldots, l\}$, let the notation $\mathcal{O}_\sigma(i)$ denote the orbit of i under the action of σ, i.e. $\mathcal{O}_\sigma(i) = \{\sigma^k(i) | k \in \mathbb{Z}^+\}$. If σ is a permutation on the set A, the relation $i \sim j$ for $i, j \in A$ if and only if $j \in \mathcal{O}_\sigma(i)$ is an equivalence relation and therefore partitions the set A. Consequently, if σ factors completely into disjoint cycles $\tau_1, \ldots, \tau_q$, we have that $i_s \sim j$ if and only if $\sigma^k(i_s) = \tau_s^k(i_s) = j$ for some $k \in \mathbb{Z}^+$, where τ_s is the cycle moving (or fixing) i_s. This allows us to identify each orbit partitioning A as the collection of elements moved (or fixed) by the same cycle in the complete factorization of σ.

The following theorem shows that every minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial can be decomposed into a sum of cycle polynomials. For a polynomial f, $f(\mathbb{F}_{p^n}) \subset \mathbb{F}_{p^m}$ implies that $f(0) = a_0 \in \mathbb{F}_{p^m}$. For this reason, it is enough to show that all minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials without constant terms can be decomposed

into a sum of cycle polynomials. The result then naturally extends to polynomials with constant terms.

Theorem 4.12. *Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be finite fields and assume that $m \equiv k(mod\ n)$. Every minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial f such that $f(0) = 0$ is a sum of cycle polynomials corresponding to the disjoint cycles in the complete factorization of $\varphi_n^k \in S_{p^n-1}$. Furthermore, each of the cycle polynomials that sum to f are independent of choice of generating term and a cycle polynomial corresponding to a cycle τ of length l in the complete factorization of φ_n^k has coefficients in $\mathbb{F}_{p^{lm}} \subseteq \mathbb{F}_{p^{[n,m]}}$.*

Proof. Let $f = \sum_{i=1}^{p^n-1} a_i x^i$ be any minimally represented polynomial that is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible and vanishes at 0. Suppose that the complete factorization of φ_n^k in S_{p^n-1} is given by $\varphi_n^k = \tau_1 \cdots \tau_q$ for disjoint cycles $\tau_1, \ldots, \tau_q$. Choose elements $i_1, \ldots, i_q$ so that i_s is moved (or fixed if i_s is fixed by φ_n^k) by τ_s for $s = 1, \ldots, q$. It follows that $\{\mathcal{O}_{\varphi_n^k}(i_s)\}_{s=1}^q$ is a partition of $\{1, \ldots, p^n - 1\}$ and we may write:

$$f = \sum_{i=1}^{p^n-1} a_i x^i = \sum_{i \in \mathcal{O}_{\varphi_n^k}(i_1)} a_i x^i + \cdots + \sum_{i \in \mathcal{O}_{\varphi_n^k}(i_q)} a_i x^i$$

Fix $s \in \{1, \ldots, q\}$, let l_s be the length of τ_s, and consider the sum $\sum_{i \in \mathcal{O}_{\varphi_n^k}(i_s)} a_i x^i$. If $j \in \mathcal{O}_{\varphi_n^k}(i_s)$, then $j = \varphi_n^{ak}(i_s)$ for a unique $a \in \{0, \ldots, l_s - 1\}$. By Theorem 3.8 and recursion, we have that $a_{i_s}^{p^{am}} x^{\varphi_n^{ak}(i_s)} = a_j x^j$ for a unique $a \in \{0, \ldots, l_s - 1\}$. Define $g_{i_s} = a_{i_s} x^{i_s} + a_{i_s}^{p^m} x^{\varphi_n(i_s)} + \cdots + a_{i_s}^{p^{(l_s-1)m}} x^{\varphi_n^{(l_s-1)k}(i_s)} = \sum_{j=0}^{l_s-1} a_{i_s}^{p^{jm}} x^{\varphi_n^{jk}(i_s)}$. Thus g_{i_s} is a cycle polynomial corresponding to τ_s with $a_{i_s} x^{i_s}$ as a generating term. Since for each $j \in \mathcal{O}_{\varphi_n^k}(i_s)$ we have that $a_j x^j = a_{i_s}^{p^{am}} x^{\varphi_n^{ak}(i_s)}$ for a unique $a \in \{0, \ldots, l_s - 1\}$, we can write:

$$\sum_{i \in \mathcal{O}_{\varphi_n^k}(i_s)} a_i x^i = \sum_{j=0}^{l_s-1} a_{i_s}^{p^{jm}} x^{\varphi_n^{jk}(i_s)} = g_{i_s}$$

Next, constructing g_{i_s} in the same manner for each $s \in \{1, \ldots, q\}$, we can rewrite f:

$$\begin{aligned} f &= \sum_{i=1}^{p^n-1} a_i x^i \\ &= \sum_{i \in \mathcal{O}_{\varphi_n^k}(i_1)} a_i x^i + \cdots + \sum_{i \in \mathcal{O}_{\varphi_n^k}(i_q)} a_i x^i \\ &= \sum_{j=0}^{l_1-1} a_{i_1}^{p^{jm}} x^{\varphi_n^{jk}(i_1)} + \cdots + \sum_{j=0}^{l_q-1} a_{i_q}^{p^{jm}} x^{\varphi_n^{jk}(i_q)} \\ &= g_{i_1} + \cdots + g_{i_q} \end{aligned}$$

Therefore f is a sum of cycle polynomials corresponding to the disjoint cycles in the complete factorization of φ_n^k. If j is another element moved by τ_s moving i_s, then $\mathcal{O}_{\varphi_n^k}(i_s) = \mathcal{O}_{\varphi_n^k}(j)$. If g_j is constructed in the same manner as g_{i_s}, it is clear that $g_j = g_{i_s}$, hence the cycle polynomials summing to f are independent of choice of generating term.

Finally, let τ_s be a cycle of length l_s in the complete factorization of φ_n^k and consider $g_{i_s} = \sum_{j=0}^{l_s-1} a_{i_s}^{p^{jm}} x^{\varphi_n^{jk}(i_s)}$ as before. We must have that $a_{i_s}^{p^{l_s m}} = a_{i_s}$, so $a_{i_s} \in \mathbb{F}_{p^{l_s m}}$ and therefore all of the coefficients of g_{i_s} are in $\mathbb{F}_{p^{l_s m}}$. As l_s divides $|\varphi_n^k| = \frac{n}{(k,n)} = \frac{n}{(m,n)}$, we have that $l_s m$ divides $\frac{n}{(m,n)} m = [n,m]$, so $\mathbb{F}_{p^{l_s m}} \subseteq \mathbb{F}_{p^{[n,m]}}$. □

Corollary 4.13. *Every minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ compatible polynomial f is the sum of the function value $f(0)$ and cycle polynomials corresponding to the disjoint cycles in the complete factorization of $\varphi_n^k \in S_{p^n-1}$.*

Proof. We see that $f - f(0)$ vanishes at 0, so by Theorem 4.12, $f - f(0) = g_1 + \cdots + g_q$ for cycle polynomials g_i. □

Definition 4.14. The sum $f(0) + g_1 + \cdots + g_q$ is called a *cycle polynomial decomposition* of f.

It should be noted that if f has the cycle polynomial decomposition $f = f(0)+g_1+\cdots+g_q$, then each of the cycle polynomials g_i are independently $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible. In fact, cycle polynomials corresponding to cycles of φ_n^k can be seen as the "smallest" $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials in that they cannot be decomposed further into smaller $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials.

Theorem 4.15. *Cycle polynomial decompositions are unique.*

Proof. Every distinct function $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ has a distinct minimally represented polynomial $f \in \overline{\mathbb{F}_p}[x]$ such that $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$, and every minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial f has a cycle polynomial decomposition. It is enough then to show that the number of distinct cycle polynomial decompositions is equal to the number of distinct functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$.

Let $\tau_1, \ldots, \tau_q$ be the disjoint cycles in the complete factorization of $\varphi_n^k \in S_{p^n-1}$. Choose τ_s of length l_s and choose some i_s moved by τ_s. Let $\alpha, \beta \in \mathbb{F}_{p^{l_s m}}$. If $\alpha \neq \beta$ then $\alpha x^{i_s} \neq \beta x^{i_s}$ and it is clear that the cycle polynomials corresponding to τ_s generated by αx^{i_s} and βx^{i_s} are distinct. It follows that there are $p^{l_s m}$ distinct cycle polynomials corresponding to τ_s.

Let N be the number of distinct cycle polynomial decompositions for $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomials. As there are p^m choices for $f(0)$, and $p^{l_s m}$ choices for each g_s corresponding to τ_s (where l_s is the length of each cycle τ_s), we see that $N = p^m \cdot p^{l_1 m} \cdots p^{l_q m} = p^m \cdot p^{l_1 m + \cdots + l_q m} = p^m \cdot p^{(m \sum_{s=1}^q l_s)} = p^m \cdot (p^m)^{\sum_{s=1}^q l_s}$. Since the lengths of the cycles $\tau_1, \ldots, \tau_q$ must sum to $p^n - 1$, we have that $N = p^m \cdot (p^m)^{p^n-1} = (p^m)^{p^n}$, which is the number of distinct functions mapping $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ (see [1], pg. 15). □

We now provide two additional corollaries to Theorem 4.12 that may prove useful in interpolation scenarios.

Corollary 4.16. *Suppose that $m \equiv k(mod\ n)$ and the complete factorization of φ_n^k in S_{p^n-1} is $\varphi_n^k = \tau_1 \cdots \tau_q$. Choose any elements $i_1, \ldots, i_q \in \{0, \ldots, p^n - 1\}$ such that each i_s is moved by a distinct disjoint cycle τ_s. Then in order to know the minimally represented polynomial f representing a function $h : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, it is enough to know the terms $a_{i_s}x^{i_s}$ of f for each $s = 1, \ldots, q$ and $h(0)$.*

Proof. This follows immediately from the algorithm for constructing each cycle polynomial $g_{i_s} = \sum_{j=0}^{l_s-1} a_{i_s}^{p^{jm}} x^{\varphi_n^{jk}(i_s)}$ (where l_s is the length of each τ_s) in the proof of Theorem 4.12 so that $f = h(0) + g_{i_1} + \cdots + g_{i_q}$. □

Corollary 4.17. *For $m \equiv k(mod\ n)$, let $\varphi_n^k = \tau_1 \cdots \tau_q$ be the complete factorization of φ_n^k into disjoint cycles $\tau_1, \ldots, \tau_q$. Choose a representative element i_s moved or fixed by each $\tau_s \in \{\tau_1, \ldots, \tau_q\}$. Then the set of possible degrees for any nonzero minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial is given by $\{0\} \cup \{max[\mathcal{O}_{\varphi_n^k}(i_s)]\}_{s=1}^q$.*

Proof. Let f be a minimally represented polynomial that is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible. By Corollary 4.13, we may write $f = f(0) + g_{i_1} + \cdots + g_{i_q}$ where each g_{i_s} is the cycle polynomial corresponding to the disjoint cycle τ_s moving i_s with generating term $a_{i_s}x^{i_s}$. Note that g_{i_s} is nonzero if and only if $a_{i_s}x^{i_s}$ is nonzero. Assume that $a_{i_s}x^{i_s}$ is nonzero. By construction, the degrees of terms in g_{i_s} correspond to elements in $\mathcal{O}_{\varphi_n^k}(i_s)$, hence $deg\,(g_{i_s}) = max[\mathcal{O}_{\varphi_n^k}(i_s)]$. If $a_{i_s}x^{i_s} = 0$, then $g_{i_s} = 0$. It follows then that for any minimally represented polynomial f that is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible, the degree of $f = f(0) + g_{i_1} + \cdots + g_{i_q}$ is determined by the degree of g_{i_s} where g_{i_s} is the largest degree cycle polynomial summing to f. It follows then that the possible degrees for any minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial are given by $\{0\} \cup \{max[\mathcal{O}_{\varphi_n^k}(i_s)]\}_{s=1}^q$. □

Note that the set $\{max[\mathcal{O}_{\varphi_n^k}(i_s)]\}_{s=1}^q$ is equivalent to the set of the largest integers moved by each disjoint cycle τ_s, $s = 1, \ldots, q$. Consequently, to see the possible nonzero degrees of any minimally represented $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial, it is enough to write φ_n^k in its complete factorization and choose the largest integer moved by each cycle. For instance, the permutation (in characteristic 2) $\varphi_4^3 = (1, 8, 4, 2)(3, 9, 12, 6)(5, 10)(7, 11, 13, 14)(15)$ in S_{15}. It follows from Corollary 4.17 that all minimally represented polynomials that are $\mathbb{F}_{16}$ to $\mathbb{F}_{2^k}$ compatible where $k \equiv 3(mod\ 4)$ are of degree 0, 8, 10, 12, 14, or 15.

We close this section with an example illustrating Theorem 4.12 with a minimally represented polynomial known to be $\mathbb{F}_8$ to $\mathbb{F}_4$ compatible. The polynomial in this example was taken from some preliminary work on a method of interpolating polynomials representing circuits using Gröbner bases. For more on this topic, see [5].

Example 4.18. Let α be a root of the irreducible polynomial $x^6 + x + 1 \in \mathbb{F}_2[x]$ so that $\mathbb{F}_{2^6} \cong \{a_0 + a_1\alpha + \ldots + a_5\alpha^5 | a_i \in \mathbb{F}_2\}$. Consider the following polynomial:

$$f(x) = (\alpha^2+\alpha)x^6+(\alpha^4+\alpha^3+\alpha)x^5+(\alpha^2+\alpha)x^4+(\alpha^4+\alpha^3+\alpha^2)x^3+(\alpha^4+\alpha^3+\alpha^2)x^2+(\alpha^4+\alpha^3+\alpha)x$$

As a function, we have that $f : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ and $f(\mathbb{F}_{2^3}) \subseteq \mathbb{F}_{2^2}$. Noting that f is minimally represented, Theorem 3.8 applies. This implies that for each term $a_i x^i$ in f, we must have that $a_i^4 = a_{\varphi_3^2(i)}$. The applicable Frobenius permutation is $\varphi_3^2 = (1,4,2)(3,5,6)(7)$. We see that we may rewrite f according to the complete factorization of φ_3^2:

$$f(x) = \underbrace{0x^0}_{f(0)} + \underbrace{(\alpha^4+\alpha^3+\alpha)x + (\alpha^2+\alpha)x^4 + (\alpha^4+\alpha^3+\alpha^2)x^2}_{(1,4,2)} + \underbrace{(\alpha^4+\alpha^3+\alpha^2)x^3 + (\alpha^4+\alpha^3+\alpha)x^5 + (\alpha^2+\alpha)x^6}_{(3,5,6)} + \underbrace{0x^7}_{(7)}$$

$$f(x) = \sum_{i=0}^{2} (\alpha^4+\alpha^3+\alpha)^{2^{2i}} x^{(\varphi_3^2)^i(1)} + \sum_{i=0}^{2} (\alpha^4+\alpha^3+\alpha^2)^{2^{2i}} x^{(\varphi_3^2)^i(3)}$$

5 Matrix Test for Subfield Compatibility

In this section, we present a test that is simpler than image by image verification of a minimally represented polynomial's subfield compatibility. Note that we are now considering φ_n as it is defined on $\{0, \ldots, p^n - 1\}$. For this reason, we will index the rows and columns of an $n \times n$ matrix from 0 to $n-1$ as opposed to the usual 1 to n.

Definition 5.1. Let $B = \{0, \ldots, n-1\}$ and let σ be a permutation on the set B. For $i \in B$, let e_i be the n-entry column vector with a 1 in the i^{th} row and 0 elsewhere. Let $e_{\sigma(i)} = e_j$ where $\sigma(i) = j$. The *permutation matrix representing* σ is defined to be the $n \times n$ matrix

$$M_\sigma = \begin{bmatrix} e_{\sigma(0)} & e_{\sigma(1)} & \cdots & e_{\sigma(n-1)} \end{bmatrix}$$

Defined as such, the permutation matrices for permutations σ and λ on $B = \{b_1, \ldots, b_n\}$ have the following well known properties which we state here without proof:

1. When applied to the ordered vector $[0, 1, \ldots, n-1]^T$,

$$M_\sigma \cdot \begin{bmatrix} 0 \\ 1 \\ \vdots \\ n-1 \end{bmatrix} = \begin{bmatrix} \sigma(0) \\ \sigma(1) \\ \vdots \\ \sigma(n-1) \end{bmatrix}$$

2. The permutation matrix $M_{\lambda\circ\sigma}$ for the permutation $\lambda \circ \sigma$ is given by the product $M_\lambda M_\sigma$ under the normal operation of matrix multiplication. In particular, the permutation matrix for the permutation σ^k is given by M_σ^k, the k^{th} power under matrix multiplication of M_σ.

3. Let $A = \{a_0, \ldots, a_{n-1}\}$ and suppose that μ is a permutation on A such that $\mu(a_i) = a_{\sigma(i)}$ for $i = 0, \ldots, n-1$. Then if N_μ is the permutation matrix for μ, $N_\mu = M_\sigma$. In other words, permutation matrices act on set vectors equivalently so that in the above case,

$$M_\sigma \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} \mu(a_0) \\ \mu(a_1) \\ \vdots \\ \mu(a_{n-1}) \end{bmatrix}$$

Definition 5.2. Fix a characteristic $p > 0$. M_{φ_n} denotes the $p^n \times p^n$ permutation matrix representing the Frobenius permutation of order n in characteristic p.

We now present a natural analog of Theorem 3.8.

Proposition 5.3. *Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields where $m \equiv k(mod\ n)$. Let $f \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$, $f = \sum_{i=0}^{p^n-1} a_i x^i$. Then $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$ if and only if the following vector equation is satisfied:*

$$\begin{bmatrix} a_0^{p^m} \\ a_1^{p^m} \\ \vdots \\ a_{p^n-1}^{p^m} \end{bmatrix} - (M_{\varphi_n})^k \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p^n-1} \end{bmatrix} = \hat{0}$$

Proof. The above equation is simply a restatement in terms of vectors of the necessary and sufficient condition in Theorem 3.8 that $a_i^{p^m} = a_{\varphi_n^k(i)}$ for $i = 0, 1, \ldots, p^n - 1$. □

For sufficiently small fields $\mathbb{F}_{p^n}$, conducting the above test is reasonable, and in fact quite simple due to the ease of construction of the matrix M_{φ_n}. To construct the matrix M_{φ_n}, start at the top left corner of an empty $p^n \times p^n$ matrix and enter a 1. Move p columns to the right on the next row and enter another 1. Repeat this process until there are $0 \leq k < p$ columns to the right of the last 1. Then advance to the row below and place a 1 in the $(p-k)^{th}$ column. Continue in this manner until the process terminates in the last entry of the matrix. Fill in the remaining entries of the matrix with 0's. Note that there will be one and only one 1 in each row and column of the matrix. This completes the construction of M_{φ_n}. Examples are provided below.

Example 5.4. The matrix for the Frobenius permutation (in characteristic 2) of order 3:

$$M_{\varphi_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Note that this matrix would be used to test whether or not a minimally represented polynomial in $\overline{\mathbb{F}_2}[x]$ maps from $\mathbb{F}_8$ into $\mathbb{F}_2$. The matrix $M^2_{\varphi_3}$ would be used to test if a minimally represented polynomial maps from $\mathbb{F}_8$ into $\mathbb{F}_4$, and the same matrix would be used to test whether a polynomial maps from $\mathbb{F}_8$ into $\mathbb{F}_{32}$ (as $5 \equiv 2 \ (mod\ 3)$).

Example 5.5. The matrix for the Frobenius permutation (in characteristic 3) of order 2:

$$M_{\varphi_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Note that this matrix would be used to test whether or not a minimally represented polynomial in $\overline{\mathbb{F}_3}[x]$ maps from $\mathbb{F}_9$ into $\mathbb{F}_3$ (or into $\mathbb{F}_{3^k}$ where k is any odd positive integer).

6 Multi-Variable Case

We now provide an abridged extension of all of the preceding results to the multi-variable case. In the interest of clarity, we will restate the original problem in this new context. Let E be a finite field of characteristic p and let K and L be subfields of E. Let f be a function that maps E^d into E. We now wish to present conditions that characterize when the restriction of $f : E^d \to E$ to the subspace K^d maps entirely into L, i.e. $f\left(K^d\right) \subseteq L$.

Let E now be any field and $E[x_1, \ldots, x_d]$ the polynomial ring in d variables over E. Throughout this section, when considering polynomials in the ring $E[x_1, \ldots, x_d]$, we will use the lexicographic monomial ordering $x_1 > x_2 > \ldots > x_d$. For a term $bx_1^{i_1}x_2^{i_2}\cdots x_d^{i_d}$ with each $i_j \in \mathbb{Z}_{\geq 0}$, the multi-degree of that term is the d-tuple $(i_1, i_2, \ldots, i_d)$. For a polynomial $f \in E[x_1, \ldots, x_d]$, the multi-degree of f is the multi-degree of the term of highest order according to the fixed monomial ordering. Let $\alpha \in A \subset \mathbb{Z}^d_{\geq 0}$. If $\alpha = (i_1, i_2, \ldots, i_d)$, then $\mathbf{x}^\alpha = x_1^{i_1}x_2^{i_2}\cdots x_d^{i_d}$. When we write $a_\alpha \mathbf{x}^\alpha$, we mean the term $a_\alpha x_1^{i_1}x_2^{i_2}\cdots x_d^{i_d}$ where $a_\alpha \in E$ is the coefficient of the term of multi-degree α.

We begin by describing minimal representations in this new context, and note that again it is enough to consider polynomials that do not vanish on $\mathbb{F}^d_{p^n}$.

Proposition 6.1. *Let $f \in \overline{\mathbb{F}_p}[x_1, \ldots, x_d] \backslash \mathcal{I}(\mathbb{F}^d_{p^n})$. Then the minimal representation of f with respect to $\mathbb{F}^d_{p^n}$ is the polynomial $f_r \in \overline{\mathbb{F}_p}[x_1, \ldots, x_d]$ such that the multi-degree of f is $\alpha = (i_1, \ldots, i_d)$ and each $i_j < p^n$, and $f(\beta) = f_r(\beta)$ for all $\beta \in \mathbb{F}^d_{p^n}$. Furthermore, each coefficient of f_r is a sum of coefficients of f.*

Proof. Recall that by definition, the minimal representation of f with respect to $\mathbb{F}_{p^n}^d$ is the polynomial f_r such that $f = c_1(x_1^{p^n} - x_1) + \cdots + c_d(x_d^{p^n} - x_d) + f_r$ and no nonzero term of f_r is divisible by $x_i^{p^n}$ for any $i = 1, \ldots, d$. The rest of the proof is straightforward, and the second part is similar to the single-variable case. □

We now extend Frobenius permutation to handle the d-variable case.

Definition 6.2. Let $H = \{0, \ldots, p^n - 1\}$. Define the function $\Phi_{n,d} : H^d \to H^d$ so that for $\alpha = (i_1, \ldots, i_d) \in H^d$, $\alpha \mapsto (\varphi_n(i_1), \ldots, \varphi_n(i_d))$ where φ_n is the Frobenius permutation of order n.

Proposition 6.3. *$\Phi_{n,d}$ is a permutation of order n on the finite set H^d.*

Proof. As φ_n permutes the set H, it is straightforward to show that $\Phi_{n,d}$ is an injection and therefore a bijection. It is also immediate that the order of $\Phi_{n,d}$ is equal to the order of φ_n. □

We will refer to $\Phi_{n,d}$ as the *d-space Frobenius permutation of order n*. Note that $\varphi_n = \Phi_{n,1}$. We now extend Proposition 3.7 to suit the multi-variable case.

Proposition 6.4. *Let $f \in \overline{\mathbb{F}_p}[x_1, \ldots, x_d]$ be minimally represented with respect to $\mathbb{F}_{p^n}^d$. Let $\Lambda = \{0, \ldots, p^n - 1\}^d$. If $f = \sum_{\alpha \in \Lambda} a_\alpha \mathbf{x}^\alpha$, then for all positive integers k, the minimal representation of the k^{th} power of the Frobenius endomorphism applied to f $\left(\text{i.e. } F^k(f)_r\right)$ is given by the polynomial $f = \sum_{\alpha \in \Lambda} a_\alpha^{p^k} \mathbf{x}^{\Phi_{n,d}(\alpha)}$ where $\Phi_{n,d}$ is the d-space Frobenius permutation of order n.*

Proof. The proof is similar to that of Propositions 3.6 and 3.7. □

The following is a restatement of Theorem 3.8 for the d-variable case.

Theorem 6.5. *Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields where $m \equiv k (mod\ n)$. Let $f \in \overline{\mathbb{F}_p}[x_1, \ldots, x_d]$ be minimally represented with respect to $\mathbb{F}_{p^n}^d$, $f = \sum_{\alpha \in \Lambda} a_\alpha \mathbf{x}^\alpha$ where $\Lambda = \{0, \ldots, p^n - 1\}^d$. Then $f\left(\mathbb{F}_{p^n}^d\right) \subseteq \mathbb{F}_{p^m}$ if and only if $a_\alpha^{p^m} = a_{\Phi_{n,d}^k(\alpha)}$ for each $\alpha \in \Lambda$ where $\Phi_{n,d}$ is the d-space Frobenius permutation of order n.*

Proof. The proof is similar to that of Theorem 3.8. □

Theorem 6.5 clearly implies that Theorem 4.10 and Theorem 4.12 still hold in the d-variable case. A matrix test for multi-variable polynomials can also be easily derived using a "nested" permutation matrix. The matrix $M_{\Phi_{n,d}}$ is a matrix constructed of block matrices that contain the matrix $M_{\Phi_{n,d-1}}$ in the position where the matrix M_{φ_n} contains a 1 and $p^{n(d-1)} \times p^{n(d-1)}$ zero blocks in all other positions. As an example, we will construct the matrix for $\Phi_{2,3}$ in characteristic 2.

We start with the matrix $M_{\varphi_2} = M_{\Phi_{2,1}}$:

$$M_{\Phi_{2,1}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The matrix $M_{\Phi_{2,2}}$ is given by:

$$M_{\Phi_{2,2}} = \begin{bmatrix} M_{\Phi_{2,1}} & \mathbf{0}_4 & \mathbf{0}_4 & \mathbf{0}_4 \\ \mathbf{0}_4 & \mathbf{0}_4 & M_{\Phi_{2,1}} & \mathbf{0}_4 \\ \mathbf{0}_4 & M_{\Phi_{2,1}} & \mathbf{0}_4 & \mathbf{0}_4 \\ \mathbf{0}_4 & \mathbf{0}_4 & \mathbf{0}_4 & M_{\Phi_{2,1}} \end{bmatrix}$$

where each $\mathbf{0}_4$ represents a 4×4 zero block matrix. Finally, we have the matrix $M_{\Phi_{2,3}}$:

$$M_{\Phi_{2,3}} = \begin{bmatrix} M_{\Phi_{2,2}} & \mathbf{0}_{16} & \mathbf{0}_{16} & \mathbf{0}_{16} \\ \mathbf{0}_{16} & \mathbf{0}_{16} & M_{\Phi_{2,2}} & \mathbf{0}_{16} \\ \mathbf{0}_{16} & M_{\Phi_{2,2}} & \mathbf{0}_{16} & \mathbf{0}_{16} \\ \mathbf{0}_{16} & \mathbf{0}_{16} & \mathbf{0}_{16} & M_{\Phi_{2,2}} \end{bmatrix}$$

where each $\mathbf{0}_{16}$ represents a 16×16 zero block matrix.

Constructed in this way, we can use the matrix $M_{\Phi_{n,d}}$ to implement the analog of the single-variable test for subfield compatibility. Index each $\alpha \in \Lambda = \{0, \ldots, p^n - 1\}^d$ according to the lexicographic monomial order on $\overline{\mathbb{F}_p}[x_1, \ldots, x_d]$ so that for $\alpha_j, \alpha_k \in \Lambda$, $\alpha_j > \alpha_k$ if and only if $\mathbf{x}^{\alpha_j} >_{lex} x^{\alpha_k}$. Then for $\Lambda = \{\alpha_1, \ldots, \alpha_{p^{nd}}\}$, a minimally represented polynomial $f \in \overline{\mathbb{F}_p}[x_1, \ldots, x_d]$ is $\mathbb{F}_{p^n}^d$ to $\mathbb{F}_{p^m}$ compatible *if and only if* for $f = \sum_{i=1}^{p^{nd}} a_{\alpha_i} \mathbf{x}^{\alpha_i}$:

$$\begin{bmatrix} a_{\alpha_1}^{p^m} \\ a_{\alpha_2}^{p^m} \\ \vdots \\ a_{\alpha_{p^{nd}}}^{p^m} \end{bmatrix} - M_{\Phi_{n,d}}^k \cdot \begin{bmatrix} a_{\alpha_1} \\ a_{\alpha_2} \\ \vdots \\ a_{\alpha_{p^{nd}}} \end{bmatrix} = \hat{0}$$

Of course these matrices will become prohibitively large when constructed for polynomial rings of many variables, but in rings of a small number of variables this method of testing may still prove more efficient than image by image verification of subfield compatibility. The matrix $M_{\Phi_{2,3}}$ that we previously constructed would be used to test whether or not a polynomial f that is minimally represented with respect to $\mathbb{F}_4^3$ maps into $\mathbb{F}_{2^k}$ for any odd positive integer k.

References

[1] P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul. *Basic Abstract Algebra* (2nd ed.). Cambridge University Press, Cambridge, 1994.

[2] Yaotsu Chang, Chong-Dao Lee, and Keqin Feng. Multivariate Interpolation Formula over Finite Fields and Its Applications in Coding Theory. arXiv:1209.1198, 2012.

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra* (3rd ed.). John Wiley and Sons, New Jersey, 2004.

[4] Nathan Jacobson. *Basic Algebra I* (2nd ed.). Dover, New York, 1985.

[5] Jinpeng Lv, Priyank Kalla, and Florian Enescu. Efficient Gröbner Basis Reductions for Formal Verification of Galois Field Arithmetic Circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 32.9: 1409-1420, 2013.

[6] Dhiraj K. Pradhan. A Theory of Galois Switching Functions. *IEEE Transactions on Computers* C-27.3:239-248, 1978.

[7] Anthony J. Preslicka. *The Topology and Algebraic Functions on Affine Algebraic Sets Over an Arbitrary Field*. MS Thesis in Mathematics, 2012.

[8] Joseph Rotman. *A First Course in Abstract Algebra With Applications* (3rd ed.). Pearson Prentice Hall, New Jersey, 2006.