Bull. Math. Soc. Sci. Math. Roumanie
Tome 60 (108) No. 4, 2017, 387–397

On subfield-compatible polynomials and a class of Vandermonde-like matrices

by
Florian Enescu[(1)] and John J. Hull[(2)]

Dedicated to Dorin Popescu in honour of his 70th birthday

Abstract

Let K and L be finite fields of characteristic p, where p is prime. This note investigates polynomial representations of functions that map K to L by providing a canonical basis for the set of minimally represented such polynomials. This interpolation problem leads to a class of Vandermonde-like matrices that are also fully described. This problem has potential applications to the hardware design of arithmetic circuits.

Key Words: interpolation, Frobenius permutation, cycle bases, Vandermonde matrices.
2010 Mathematics Subject Classification: 12E20, 15B99

1 Introduction

Let p a prime number, $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$, and K, L finite subfields of $\overline{\mathbb{F}_p}$. In this note, we will investigate the special form of the polynomials f in $\overline{\mathbb{F}_p}[x]$ mapping K into L, that is $f(K) \subseteq L$. Interpolation theory has been well studied over time ([4]), but this particular aspect has received little to no attention. Our note will reveal that there is considerable structure hidden in the objects defined by this interpolation set-up, building upon Hull's work in [1].

In electrical engineering, arithmetic circuits are often represented via interpolating polynomials over a finite field, which in turn can be used for validating the hardware design of the circuit. In practice, one limitation is the size of the circuit that leads to polynomials with very large degrees. To mitigate this problem, it is often useful to break up a large circuit in several small ones which can be analyzed more easily. This leads to devising tools that can allow investigating the structure of functions that are defined over a large field but restrict naturally to smaller subfields. Our work will describe the algebraic situation behind this set-up.

The following example is explaining and motivating the problem we study.

Example 1.1. Let $p = 2$. Let K, L be subfields of $\overline{\mathbb{F}_2}$, such that K has 8 elements and L has 4 elements. What polynomials f in $\overline{\mathbb{F}_2}[x]$ satisfy $f(K) \subseteq L$?

Say α satisfies $\alpha^6 = \alpha^4 + \alpha^3 + \alpha + 1$. Then $\mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/\langle x^6 + x^4 + x^3 + x + 1\rangle$ is contained in $\overline{\mathbb{F}_2}$. Note that α is a primitive generator for $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$. Take $K = \mathbb{F}_2(\alpha^9)$ and $L = \mathbb{F}_2(\alpha^{21})$ which are subfields with 8, respectively 4 elements. The function $f(X) = \alpha^9 X + \alpha^{36} X^4 + \alpha^{28} X^2$ maps K to L, according to [1], or as in Theorem 2.4 below. The collection of polynomials f of degree strictly less than 64 such that $f(K) \subseteq L$ is a L-vector

space and describes all the polynomials functions with coefficients in $\overline{\mathbb{F}_2}$ mapping K to L. In this paper, we will present a canonical basis for this vector space, as a particular case to the main theorem.

Throughout this paper, F represents the Frobenius endomorphism on $\overline{\mathbb{F}_p}$ and on the polynomial ring $\overline{\mathbb{F}_p}[x]$. For any function f, when we write f^n for some $n \in \mathbb{N}$ we mean the composition of f with itself n times.

Definition 1.2. Let $K, L \subset \overline{\mathbb{F}_p}$ be finite fields. An element of $f \in \overline{\mathbb{F}_p}[x]$ such that $f(K) \subseteq L$ is called K *to* L *compatible*. The set of all functions $K \to K$ will be denoted $\mathcal{F}_K$, a vector space over K. Similarly, $\mathcal{F}_K^L$ will denote the set of all functions defined on K and mapping K to L. This is a vector space over L.

It is well known that Lagrange interpolation can be used to get a more precise description of the vector space $\mathcal{F}_K$, in that each function in $\mathcal{F}_K$ has a polynomial representation in $K[x]$ when K is finite (see Theorem 1.71 in [2]).

Observation 1.3. Let $K \subseteq K'$ be a field extension and $f \in \mathcal{F}_K$. We will say that $g \in K'[x]$ *represents* f *with respect to* K if $g(\alpha) = f(\alpha)$ for all $\alpha \in K$. If $g \in K'[x]$ represents f with respect to K and it is of smallest possible degree with this property, then we say that g *minimally represents* f. When K' is finite, then, for any function $f \in \mathcal{F}_K$ (or polynomial in $K[x]$), there is polynomial $g \in K[x]$ representing f with respect to K, by Lagrange interpolation. If K has p^n elements, g can be taken of degree less than p^n.

Assume K has p^n elements. Let $g, h \in \overline{\mathbb{F}_p}[x]$ representing $f \in K[x]$ with respect to K. It is easy to see that $g - h = (x^{p^n} - x)f_0(x)$ where $f_0 \in \overline{\mathbb{F}_p}[x]$. This shows that if g, h have degrees less than p^n, then they are equal. So, the concept of minimal representation of a polynomial $f \in K[x]$ is well-defined, independent of the finite field extension $K \subseteq K'$ and therefore it is also well defined over $\overline{\mathbb{F}_p}$.

More specifically, the following holds.

Proposition 1.4. *Let $K \subseteq K'$ be a finite field extension and $g(x) \in K'[x]$ a polynomial representing $f \in K[x]$. The following statements are equivalent:*

1. $\deg(g) \leq p^n - 1$
2. *$g(x)$ is a polynomial of smallest degree representing f with respect to K.*

Under these conditions, g is uniquely determined and belongs to $K[x]$. It will be denoted by f_r.

We will review below a few definitions and results from [1] that are useful in this work. The following result is immediate.

Proposition 1.5. *Let $f \in \overline{\mathbb{F}_p}[x]$, not a multiple of $x^{p^n} - x$. Then the minimal representation of f with respect to $K = \mathbb{F}_{p^n}$ 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.*

Let K, L be finite fields of equal characteristic p, where p is prime, and E their composite field. We will identify $K = \mathbb{F}_{p^n}$, $L = \mathbb{F}_{p^m}$ with the splitting fields of $X^{p^n} - X$ and, respectively, $X^{p^m} - X$ over $\mathbb{F}_p$, where $n, m \in \mathbb{N}$. Therefore, $E = \mathbb{F}_{p^{[n,m]}}$ is the splitting field of $X^{p^{[n,m]}} - X$ over $\mathbb{F}_p$, where $[n, m] = lcm(n, m)$.

Proposition 1.6 ([1]). *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 $\mathbb{F}_{p^{[n,m]}}$.*

This motivates the following definition.

Definition 1.7. Let K, L be finite fields and E their composite field. Let $\mathbb{P}_K$ denote the collection of all polynomials in $E[\mathbf{x}]$ that are minimally represented with respect to K and let $\mathbb{P}_K^L \subset \mathbb{P}_K$ be those minimally represented polynomials that have images in L when evaluated at elements of K. Note that $\mathbb{P}_K$ is naturally a vector space over E and $\mathbb{P}_K^L$ is an L-subspace of $\mathbb{P}_K$.

Remark 1.8. There is an isomorphism of vector spaces between $\mathbb{P}_K^L$ and $\mathcal{F}_K^L$. Simply identify each minimally represented polynomial P with its corresponding function $f_P : K \to L$.

In our work, the following concept is essential.

Definition 1.9 ([1]). **(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 $i \in \{1, \ldots, p^n - 1\}$, $F(\beta^i) = \beta^{pi} = \beta^{\varphi(i)}$ where $\varphi(i) \in \{1, \ldots, p^n - 1\}$ and $\varphi(0) = 0$. We will refer to φ as the *Frobenius permutation of order n* and we will at times write φ_n to emphasize that the order of φ is n, see Proposition 1.10.

It is known that φ does not depend on the choice of the generator β for $\mathbb{F}_{p^n}^\times$. In fact, the permutation φ *does* depend only the characteristic p. This follows from the result below.

Proposition 1.10 ([1]). *Let φ be as defined above. Then φ is a permutation of order n on the set $\{0, \ldots, p^n - 1\}$ (i.e. $\varphi^n = id$). Furthermore, for $i \in \{0, \ldots, p^n - 1\}$, $\varphi(i) = q + r$ where $pi = p^n q + r$, $0 \leq r < p^n$.*

The rest of the paper is organized as follows. In Section 2, we will introduce the notion of cycle basis and provide a canonical basis for the vector space $\mathbb{P}_K^L$. In Section 3, we discuss the concept of Vandermonde-Frobenius matrix that is naturally associated to a cycle basis, and describe how to computed its determinant.

2 Cycle bases

Definition 2.1. Let E be a field containing $\mathbb{F}_{p^m}$. A *cycle polynomial* is a polynomial $f \in E[x]$ such that there exists a cycle σ of length r, a term ax^i in f with i in the support of σ, and a positive integer m such that $a^{p^{rm}} = a$ such that

$$f = ax^i + a^{p^m} x^{\sigma(i)} + a^{p^{2m}} x^{\sigma^2(i)} + \cdots + a^{p^{(r-1)m}} x^{\sigma^{r-1}(i)}$$

In the above case, we say that f is *a cycle polynomial of magnitude m corresponding to σ* and that ax^i is *a generating term* for f. Moreover, the collection of all cycle polynomials of magnitude m corresponding to σ will be denoted by $\mathbb{P}_{\sigma,m}$. This is a subset of $\mathbb{F}_{p^m}[x] \subseteq E[x]$.

Proposition 2.2. *Let r, m positive integers. Let σ a cycle of length r, and $f \in \mathbb{P}_{\sigma,m}$. Then any term of f is a generating term for f. Moreover $\mathbb{P}_{\sigma,m}$ is an $\mathbb{F}_{p^m}$-vector space and $\dim_{\mathbb{F}_{p^m}}(\mathbb{P}_{\sigma,m}) = r$.*

Proof. The first observation is that $\mathbb{P}_{\sigma,m}$ is a $\mathbb{F}_{p^m}$-vector space, since the Frobenius map, and its iterations, are additive and $a^{p^m} = a$ for all $a \in \mathbb{F}_{p^m}$.

Let a such that $a^{p^{rm}} = a$ and

$$f = ax^i + a^{p^m} x^{\sigma(i)} + a^{(p^m)^2} x^{\sigma^2(i)} + \cdots + a^{(p^m)^{r-1}} x^{\sigma^{r-1}(i)}.$$

Clearly, $a^{p^{jm+rm}} = a^{p^{jm}}$ for all $j = 0, \ldots, r-1$ and σ is a cycle of length r, so any term of f is a generating term.

The coefficients of f are in $\mathbb{F}_{p^{rm}}$. Let α a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{rm}}$. This is an element of $\mathbb{F}_{p^{rm}}$ of degree r over $\mathbb{F}_{p^m}$.

Let $D_{\sigma,\alpha}$ be the set containing the following cycle polynomials:

$$\begin{aligned}
\delta_0 &= x^i + x^{\sigma(i)} + \cdots + x^{\sigma^{r-1}(i)} \\
\delta_1 &= \alpha x^i + \alpha^{p^m} x^{\sigma(i)} + \cdots + \alpha^{p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
\delta_2 &= \alpha^2 x^i + \alpha^{2p^m} x^{\sigma(i)} + \cdots + \alpha^{2p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
&\vdots \\
\delta_{r-1} &= \alpha^{r-1} x^i + \alpha^{(r-1)p^m} x^{\sigma(i)} + \cdots + \alpha^{(r-1)p^{(r-1)m}} x^{\sigma^{r-1}(i)}
\end{aligned}$$

Let $g = ax^i + a^{p^m} x^{\tau(i)} + \cdots + a^{p^{(r-1)m}} x^{\tau^{r-1}(i)}$ be any cycle polynomial corresponding to σ, $a \in E$. Note that since $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{rm}}$ is an extension of fields, $a = b_0 + b_1\alpha + \cdots + b_{r-1}\alpha^{r-1}$ with $b_0, \ldots, b_{r-1}$ in $\mathbb{F}_{p^m}$.
It follows then that:

$$ax^i + a^{p^m} x^{\sigma(i)} + \cdots + a^{p^{(r-1)m}} x^{\sigma^{r-1}(i)} =$$

$$(b_0 + \cdots + b_{r-1}\alpha^{r-1})x^i + (b_0 + \cdots + b_{r-1}\alpha^{r-1})^{p^m} x^{\sigma(i)} + \cdots +$$

$$+ (b_0 + \cdots + b_{r-1}\alpha^{r-1})^{p^{(r-1)m}} x^{\sigma^{r-1}(i)} =$$

$$(b_0 + \cdots + b_{r-1}\alpha^{r-1})x^i + (b_0^{p^m} + \cdots + b_{r-1}^{p^m}\alpha^{(r-1)p^m})x^{\sigma(i)} + \cdots +$$

$$+ (b_0^{p^{(r-1)m}} + \cdots + b_{l-1}\alpha^{(r-1)p^{(r-1)m}})x^{\sigma^{r-1}(s)} =$$

$$(b_0 x^i + \cdots + b_0 x^{\sigma^{r-1}(i)}) + (b_1\alpha x^i + \cdots + b_1\alpha^{p^{(r-1)m}} x^{\sigma^{r-1}(i)}) + \cdots +$$

$$+ (b_{r-1}\alpha^{r-1}x^i + \cdots + b_{l-1}\alpha^{(r-1)p^{(r-1)m}} x^{\sigma^{r-1}(i)}).$$

This shows that

$$g = b_0\delta_0 + b_1\delta_1 + \cdots + b_{r-1}\delta_{r-1}.$$

Therefore $D_{\sigma,\alpha}$ spans $\mathbb{P}_{\sigma,m}$. The linear independence of the set $D_{\sigma,\alpha}$ over $\mathbb{F}_{p^m}$ follows immediately from the linear independence of $\{1, \alpha, \ldots, \alpha^{r-1}\}$ over $\mathbb{F}_{p^m}$, hence $D_{\sigma,\alpha}$ is a basis for $\mathbb{P}_{\sigma,m}$ and $\dim(\mathbb{P}_{\sigma,m}) = r$, the order of σ.

□

Definition 2.3. Let r, m positive integers. Let σ be a cycle of length r, and i an element in the support of σ. Let α be a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{rm}}$.

The basis $\{\delta_0(x), \ldots, \delta_{r-1}(x)\}$ where

$$\begin{aligned}
\delta_0 &= x^i + x^{\sigma(i)} + \cdots + x^{\sigma^{r-1}(i)} \\
\delta_1 &= \alpha x^i + \alpha^{p^m} x^{\sigma(i)} + \cdots + \alpha^{p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
\delta_2 &= \alpha^2 x^i + \alpha^{2p^m} x^{\sigma(i)} + \cdots + \alpha^{2p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
&\vdots \\
\delta_{r-1} &= \alpha^{r-1} x^i + \alpha^{(r-1)p^m} x^{\sigma(i)} + \cdots + \alpha^{(r-1)p^{(r-1)m}} x^{\sigma^{r-1}(i)}
\end{aligned}$$

is called the *cycle basis* for $\mathbb{P}_{\sigma,m}$ associated to α. We will denote it by $D_{\sigma,\alpha}$.

The following characterization of subfield-compatible polynomials will be important next.

Theorem 2.4. *([1]) 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 $m \equiv k (mod\ n)$.*

We are now ready to completely describe the collection of all polynomials in $E[\mathbf{x}]$ that are minimally represented with respect to K, and K to L compatible.

Theorem 2.5. *Let $K = \mathbb{F}_{p^n}, L = \mathbb{F}_{p^m}$ and their composite field E. Let k such that $m \equiv k\ (mod\ n)$ and $\phi_n^k = \sigma_1 \cdots \sigma_s$ a complete factorization, where σ_h is a cycle of order r_h, $h = 1, \ldots, s$.*

Then we have the following direct sum decomposition $\mathbb{P}_K^L = \oplus_{h=1}^s \mathbb{P}_{\sigma_h,m}$ and $\mathbb{P}_K^L$ has dimension p^n over $\mathbb{F}_{p^m}$.

Proof. First let us note that, for all $h = 1, \ldots, s$, $\mathbb{P}_{\sigma_h,m}$ is an $L = \mathbb{F}_{p^m}$-vector space by Proposition 2.2.

Let $\sigma = \sigma_h$ one of the cycles in the factorization of φ_n^k. We observe that $\mathbb{P}_{\sigma,m} \subset \mathbb{P}_K^L$:

Let $f \in \mathbb{P}_{\sigma,m}$. Therefore there exists $a \in E$ and i an integer in the support of the cycle σ such that

$$f = ax^i + a^{p^m} x^{\sigma(i)} + a^{p^{m\,2}} x^{\sigma^2(i)} + \cdots + a^{p^{m\,r-1}} x^{\sigma^{r-1}(i)}.$$

Note that f is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible by Theorem 2.4, since φ^k acts as σ_h on the support of σ_h. This proves the desired inclusion.

Now let $f \in \mathbb{P}_K^L$. Let $a_i x^i$ be a term in f and hence $0 \leq i \leq p^n - 1$. Theorem 2.4 shows that $a_i^{p^m} = a_{\varphi^k(i)}$. So, the cycle polynomial of magnitude p^m generated by this term is part of f. This shows that $\mathbb{P}_{p_n^m} = \mathbb{P}_{\sigma_1,m} + \cdots + \mathbb{P}_{\sigma_s,m}$. The degrees of all nonzero terms of the cycle polynomials in $\mathbb{P}_{\sigma_i,p^m}$ are determined by the support of the disjoint cycle σ_i of length r_i, so it follows immediately that if $f \in \mathbb{P}_{\sigma_i,m} \cap \sum_{i \neq j} \mathbb{P}_{\sigma_j,m}$, then $f = 0$. Then $\mathbb{P}_{p_n^m} = \bigoplus_{i=1}^s \mathbb{P}_{\sigma_i,m}$ and $\cup_{i=1}^s D_{\sigma_i,\alpha_i}$ forms a basis for $\mathbb{P}_{p_n^m}$, where α_i denotes a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{r_i m}}$, for every $i = 1, \ldots, s$. Since $|D_{\sigma_i}| = r_i$ where r_i is the length of σ_i, we have that $\dim(\mathbb{P}_{p_n^m}) = \sum_{i=1}^s r_i = p^n$, as claimed. ∎

Definition 2.6. Maintaining the notations from proof of Theorem 2.5, we will call the union $\cup_{i=1}^{s} D_{\sigma_i,\alpha_i} := \{\delta_0(x), \ldots, \delta_{p^n-1}(x)\}$ a *cycle basis* for $\mathbb{P}_K^L$. It depends on a choice of generators for the extensions $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{r_i m}}$, where $i = 1, \ldots, s$.

3 Vandermonde-Like Matrices

Definition 3.1. For a field E and $\{\alpha_1, \ldots, \alpha_m\} \subset E$, define the Vandermonde Matrix $V(\alpha_1, \ldots, \alpha_m)$ as follows:

$$V(\alpha_1, \ldots, \alpha_m) = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{m-1} \end{bmatrix}$$

The determinant of this matrix is

$$v(\alpha_1, \ldots, \alpha_m) = \prod_{1 \le i < j \le m} (\alpha_j - \alpha_i).$$

Proposition 3.2. *The coefficients of the interpolating polynomial passing through a set S of given points $(\alpha_i, f(\alpha_i)), i = 1, \ldots, m$ can be obtained by finding the solutions in E for the following system:*

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{m-1} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix} = \begin{bmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_m) \end{bmatrix}$$

The polynomial interpolating the function is then $\sum_{i=1}^{m} c_i x^{i-1}$, and this polynomial is sometimes referred as the Lagrange polynomial of the set S.

Corollary 3.3. *Let f be any function from $K = \mathbb{F}_{p^n}$ to $L = \mathbb{F}_{p^m}$, and let $\{\delta_0(x), \ldots, \delta_{p^n-1}(x)\}$ be a cycle basis for $\mathbb{P}_K^L$. Let $\mathbb{F}_{p^n} = \{\alpha_1, \ldots, \alpha_{p^n}\}$. Then the minimally represented polynomial giving f is as follows:*

$$f_r(x) = c_1\delta_0(x) + c_2\delta_2(x) + \cdots + c_{p^n}\delta_{p^n-1}(x)$$

where the c_i form the unique solution to the following system:

$$\begin{bmatrix} \delta_0(\alpha_1) & \delta_2(\alpha_1) & \cdots & \delta_{p^n-1}(\alpha_1) \\ \delta_0(\alpha_2) & \delta_2(\alpha_2) & \cdots & \delta_{p^n-1}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \delta_0(\alpha_{p^n}) & \delta_2(\alpha_{p^n}) & \cdots & \delta_{p^n-1}(\alpha_{p^n}) \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_{p^n} \end{bmatrix} = \begin{bmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_{p^n}) \end{bmatrix}$$

Proof. Clear. □

Definition 3.4. Define the matrix of evaluated basis elements (polynomials) in the proposition above to be the *Frobenius-Vandermonde Matrix* of the cycle basis $\{\delta_0, \ldots, \delta_{p^n-1}\}$ and let $V_F(\delta_0, \ldots, \delta_{p^n-1})$ denote this matrix. Its determinant will be denoted $v_F(\delta_0, \ldots, \delta_{p^n-1})$. Just as the cycle basis, the Frobenius-Vandermonde matrix and determinant depend upon a choice of generators for the extensions $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{r_i m}}$, where $i = 1, \ldots, s$.

Proposition 3.5. *For $n = m$, $V_F = V$, where V is the Vandermonde matrix over the entire field $\mathbb{F}_{p^n}$.*

Proof. When $n = m$, the Frobenius permutation is the identity. Since the cycles in φ_n^0 are therefore all of length one, the cycle basis is given by $D = \{\delta_0(x) = 1, \delta_1(x) = x, \delta_2(x) = x^2, \ldots, \delta_{p^n-1}(x) = x^{p^n-1}\}$. Then V_F is clearly:

$$\begin{bmatrix} \delta_0(\alpha_1) & \delta_1(\alpha_1) & \cdots & \delta_{p^n-1}(\alpha_1) \\ \delta_0(\alpha_2) & \delta_1(\alpha_2) & \cdots & \delta_{p^n-1}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \delta_0(\alpha_{p^n}) & \delta_1(\alpha_{p^n}) & \cdots & \delta_{p^n-1}(\alpha_{p^n}) \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{p^n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{p^n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{p^n} & \cdots & \alpha_{p^n}^{p^n-1} \end{bmatrix}$$

This is exactly V considered over all of the elements of $\mathbb{F}_{p^n}$. □

Remark 3.6. If one approaches an interpolation problem for a function $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ in the composite field $\mathbb{F}_{p^e}$, $e = [n, m]$, using a Vandermonde matrix, the size of the matrix will be $p^e \times p^e$. In contrast, the size of the Frobenius-Vandermonde matrix for such a problem is $p^n \times p^n$. This is notably smaller in cases where n and m are relatively prime, and such a difference could be important in situations where matrix size is a limiting factor.

The following examples illustrates the theory and will be revisited a few times in this note.

Example 3.7. (Construct V_F for $\mathbb{F}_8 \to \mathbb{F}_4$) Let $\mathbb{F}_{64} = \mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/\langle x^6 + x^4 + x^3 + x + 1\rangle$. Note that α is a primitive generator for $\mathbb{F}_{64}$ and α^9 generates $\mathbb{F}_8$ over $\mathbb{F}_2$. In fact, $\mathbb{F}_8 = \mathbb{F}_2(\alpha^9) = \{\alpha^{9i} : i = 1, \ldots, 7\} \cup \{0\}$ and $\mathbb{F}_4 = \mathbb{F}_2(\alpha^{21})$. Moreover, α^9 is an element of degree 3 over $\mathbb{F}_2$, so it is a generator for $\mathbb{F}_4 \subset \mathbb{F}_{64}$. Since the appropriate permutation is $\varphi_3^2 = (0)(1, 4, 2)(3, 5, 6)(7)$, the cycle basis for polynomial space is:

1. $(0) \sim \delta_0(X) = 1$
2. $(1, 4, 2) \sim \delta_1(X) = X + X^4 + X^2$
3. $(1, 4, 2) \sim \delta_2(X) = \alpha^9 X + \alpha^{9\cdot 4} X^4 + \alpha^{9\cdot 16} X^2$
4. $(1, 4, 2) \sim \delta_3(X) = \alpha^{18} X + \alpha^{18\cdot 4} X^4 + \alpha^{18\cdot 16} X^2$
5. $(3, 5, 6) \sim \delta_4(X) = X^3 + X^5 + X^6$
6. $(3, 5, 6) \sim \delta_5(X) = \alpha^9 X^3 + \alpha^{9\cdot 4} X^5 + \alpha^{9\cdot 16} X^6$
7. $(3, 5, 6) \sim \delta_6(X) = \alpha^{18} X^3 + \alpha^{18\cdot 4} X^5 + \alpha^{18\cdot 16} X^6$
8. $(7) \sim \delta_7(X) = X^7$

Fill the matrix:

$$V_F = \begin{bmatrix} \delta_0(0) & \delta_1(0) & \delta_2(0) & \delta_3(0) & \delta_4(0) & \delta_5(0) & \delta_6(0) & \delta_7(0) \\ \delta_0(\alpha^9) & \delta_1(\alpha^9) & \delta_2(\alpha^9) & \delta_3(\alpha^9) & \delta_4(\alpha^9) & \delta_5(\alpha^9) & \delta_6(\alpha^9) & \delta_7(\alpha^9) \\ \delta_0(\alpha^{18}) & \delta_1(\alpha^{18}) & \delta_2(\alpha^{18}) & \delta_3(\alpha^{18}) & \delta_4(\alpha^{18}) & \delta_5(\alpha^{18}) & \delta_6(\alpha^{18}) & \delta_7(\alpha^{18}) \\ \delta_0(\alpha^{27}) & \delta_1(\alpha^{27}) & \delta_2(\alpha^{27}) & \delta_3(\alpha^{27}) & \delta_4(\alpha^{27}) & \delta_5(\alpha^{27}) & \delta_6(\alpha^{27}) & \delta_7(\alpha^{27}) \\ \delta_0(\alpha^{36}) & \delta_1(\alpha^{36}) & \delta_2(\alpha^{36}) & \delta_3(\alpha^{36}) & \delta_4(\alpha^{36}) & \delta_5(\alpha^{36}) & \delta_6(\alpha^{36}) & \delta_7(\alpha^{36}) \\ \delta_0(\alpha^{45}) & \delta_1(\alpha^{45}) & \delta_2(\alpha^{45}) & \delta_3(\alpha^{45}) & \delta_4(\alpha^{45}) & \delta_5(\alpha^{45}) & \delta_6(\alpha^{45}) & \delta_7(\alpha^{45}) \\ \delta_0(\alpha^{54}) & \delta_1(\alpha^{54}) & \delta_2(\alpha^{54}) & \delta_3(\alpha^{54}) & \delta_4(\alpha^{54}) & \delta_5(\alpha^{54}) & \delta_6(\alpha^{54}) & \delta_7(\alpha^{54}) \\ \delta_0(1) & \delta_1(1) & \delta_2(1) & \delta_3(1) & \delta_4(1) & \delta_5(1) & \delta_6(1) & \delta_7(1) \end{bmatrix}$$

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

Example 3.8. Going the other way using the same field and generators, for $\mathbb{F}_4 \to \mathbb{F}_8$ the appropriate permutation is $\varphi_2^3 = \varphi_2 = (0)(1,2)(3)$. The basis is then:

1. $(0) \sim \delta_0(X) = 1$
2. $(1,2) \sim \delta_1(X) = X + X^2$
3. $(1,2) \sim \delta_2(X) = \alpha^{21}X + \alpha^{21\cdot 8}X^2$
4. $(3) \sim \delta_3(X) = X^3$

Fill the matrix:

$$\begin{bmatrix} \delta_0(0) & \delta_1(0) & \delta_2(0) & \delta_3(0) \\ \delta_0(\alpha^{21}) & \delta_1(\alpha^{21}) & \delta_2(\alpha^{21}) & \delta_3(\alpha^{21}) \\ \delta_0(\alpha^{42}) & \delta_1(\alpha^{42}) & \delta_2(\alpha^{42}) & \delta_3(\alpha^{42}) \\ \delta_0(1) & \delta_1(1) & \delta_2(1) & \delta_3(1) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

This leads to an obvious conclusion regarding the entries in the matrix V_F when n is prime and $n \neq m$.

Proposition 3.9. *For n prime, $n \nmid m$, V_F has entries in $\mathbb{F}_p$ only.*

Proof. By construction, the basis elements are determined by the cycles of $\varphi_n^m = \varphi_n^k$ where $m \equiv k \mod n$. Since n is prime, $n \nmid m$, we have first that every cycle of φ_n^k has length 1 or n (as the cycle length must divide the prime order n of the permutation) and also that $\mathbb{F}_{p^{[n,m]}} = \mathbb{F}_{p^m}(\beta)$ where $\mathbb{F}_{p^n} = \mathbb{F}_p(\beta)$.

If τ is a disjoint cycle of length 1 in the complete factorization of φ_n^k, then the basis for $\mathbb{P}_{\tau,p^m}$ is simply x^s where s is the element fixed by τ. Then for all $\alpha \in \mathbb{F}_{p^n}$, $\alpha^s \in \mathbb{F}_{p^n}$, but also, since x^s is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible, $\alpha^s \in \mathbb{F}_{p^m}$. Then for all $\alpha \in \mathbb{F}_{p^n}$, $\alpha^s \in \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_p$.

If τ has length n, then all of the polynomials in D_τ, the basis for $\mathbb{P}_{\tau,p^m}$, are of the form $\delta_k(x) = \beta^k x^s + \beta^{kp^m} x^{\tau(s)} + \cdots + \beta^{kp^{(n-1)m}} x^{\tau^{n-1}(s)}$. Again, when evaluated at $\alpha \in \mathbb{F}_{p^n}$, it is not hard to see that $\delta_k(\alpha) \in \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_p$. Since the entries of V_F consist entirely of images of the basis elements, V_F must necessarily have entries in $\mathbb{F}_p$ only. □

There is some additional structure that can be highlighted in the Vandermonde-Frobenius matrix associated to a cycle basis. Let $\mathbb{F}_p \subset \mathbb{F}_{p^{mn}}$ with n prime. The only nontrivial cycles in ϕ_n^m have length n, since ϕ_n has order n. Let σ be a cycle of length n in ϕ_n^m and i an element in the support of σ. Let α be a primitive generator of $\mathbb{F}_p \subset \mathbb{F}_{p^{nm}}$ and $\delta_0, \ldots, \delta_{r-1}$ be a cycle basis of $\mathbb{P}_{\sigma,p^m}$ corresponding to α^t, where $p^{nm} - 1 = (p^n - 1) \cdot t$. Note that indeed α^t is a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{mn}}$.

Proposition 3.10. *Using the notations above, let $\delta_0, \ldots, \delta_{r-1}$ be the cycle basis D_{σ,α^t} of $\mathbb{P}_{\sigma,p^m}$. Then if $1 \leq l, l' \leq r-1$ and $0 \leq s, s'$ with*

$$p^n - 1 \ \mid \ (l - l') + (s - s')i,$$

then $\delta_l(\alpha^{ts}) = \delta_{l'}(\alpha^{ts'})$.

Proof. Remark that

$$\delta_l((\alpha^t)^s) = \sum_{k=0}^{n} (\alpha^t)^{lp^{km}} \cdot (\alpha^t)^{s\sigma^k(i)} = \sum_{k=0}^{n} (\alpha^t)^{(lp^{km} + s\sigma^k(i))}.$$

Note that $(\alpha^t)^{s\sigma^k(i)} = (\alpha^t)^{sp^{km}i}$, for every $k = 0, \ldots, n$. It is now immediate that if $p^n - 1$ divides $(l - l') + (s - s')i$, then $\delta_l(\alpha^{ts}) = \delta_{l'}(\alpha^{ts'})$.

□

This pattern is illustrated by Examples 3.7 and 3.8. In Example 3.7, let $V_F = (v_{ij})_{1 \leq i,j \leq 8}$. Since $(1, 4, 2)$ is the cycle factorization of ϕ_2^3, $p = 2, n = 3$, we can take $i = 1$, $l - l' = -1$, $s - s' = 1$. Then the Proposition above shows that $v_{i,2} = v_{i-1,3}$ and $v_{i,3} = v_{i-1,4}$, for $3 \leq i \leq 8$ and $v_{2,2} = v_{8,3}, v_{2,3} = v_{8,4}$. Now, for $(3, 5, 6)$ we can take $i = 3$, $l - l' = 1, s - s' = 2$. So, $v_{i,5} = v_{i+2,6}, v_{i,6} = v_{i+2,7}$ for $2 \geq i \geq 6$. Also, $v_{7,5} = v_{2,6}, v_{8,5} = v_{3,6}, v_{7,6} = v_{2,7}, v_{8,6} = v_{3,7}$. A similar phenomenon appears in Example 3.8.

3.1 The structure of the Vandermonde-Frobenius matrix

Let $L = \mathbb{F}_{p^m} \subseteq L' = \mathbb{F}_{p^{rm}}$ be a field extension, let α be an element of L' and σ a cycle of length r.

Consider the following cycle polynomials:

$$\begin{aligned}
\delta_0 &= x^i + x^{\sigma(i)} + \cdots + x^{\sigma^{r-1}(i)} \\
\delta_1 &= \alpha x^i + \alpha^{p^m} x^{\sigma(i)} + \cdots + \alpha^{p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
\delta_2 &= \alpha^2 x^i + \alpha^{2p^m} x^{\sigma(i)} + \cdots + \alpha^{2p^{(r-1)m}} x^{\sigma^{r-1}(i)} \\
&\vdots \\
\delta_{l-1} &= \alpha^{r-1} x^i + \alpha^{(r-1)p^m} x^{\sigma(i)} + \cdots + \alpha^{(r-1)p^{(r-1)m}} x^{\sigma^{r-1}(i)}
\end{aligned}$$

Let

$$C = C_{r,m}(\alpha) = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{r-1} \\ 1 & \alpha^{p^m} & \alpha^{2p^m} & \cdots & \alpha^{(r-1)p^m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{p^{(r-1)m}} & \alpha^{2p^{(r-1)m}} & \cdots & \alpha^{(r-1)p^{(r-1)m}} \end{bmatrix}$$

Denote its determinant by $c_{r,m}(\alpha)$. Clearly,

$$C_{r,m}(\alpha) = V(\alpha, \ldots, \alpha^{p^{(r-1)m}}), \quad c_{r,m}(\alpha) = v(\alpha, \ldots, \alpha^{p^{(r-1)m}}).$$

Note that, using the notations of Definition 2.3,

$$[\delta_0, \delta_1 \ldots, \delta_{r-1}] = [x^i, x^{\sigma(i)}, \ldots, x^{\sigma^{r-1}(i)}] \cdot C.$$

Let us denote

$$X_\sigma(x) = [x^i, x^{\sigma(i)}, \ldots, x^{\sigma^{r-1}(i)}].$$

Now let us return to the original set-up. Let $K = \mathbb{F}_{p^n}, L = \mathbb{F}_{p^m}$ finite subfields of E, which is their composite field. Let k such that $m \equiv k \ (mod\ n)$ and $\phi_n^k = \sigma_1 \cdots \sigma_s$ a complete factorization, where σ_h has order r_h, $h = 1, \ldots, s$. For each $h = 1, \ldots, s$, let a_h be a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{r_h m}}$.

Let $C = [C_{r_1,m}(a_1)| \cdots |C_{r_s,m}(a_s)]$, the matrix obtained by using $C_{r_h,m}(a_h)$, $h = 1, \ldots, s$, as blocks. This is a square matrix of size p^n with determinant equal to

$$c_{r_1,m}(a_1) \cdots c_{r_s,m}(a_s).$$

Let $X = [X_{\sigma_1}, \ldots, X_{\sigma_s}]$. Let $X(\alpha_1, \ldots, \alpha_{p^n})$ be the square matrix of size p^n that is equal to

$$\begin{bmatrix} X_{\sigma_1}(\alpha_1) & X_{\sigma_2}(\alpha_1) & \cdots & X_{\sigma_s}(\alpha_1) \\ X_{\sigma_1}(\alpha_2) & X_{\sigma_2}(\alpha_2) & \cdots & X_{\sigma_s}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ X_{\sigma_1}(\alpha_{p^n}) & X_{\sigma_2}(\alpha_{p^n}) & \cdots & X_{\sigma_s}(\alpha_{p^n}) \end{bmatrix}$$

The discussion above leads to the following description of the Vandermonde-Frobenius determinants.

Theorem 3.11. *Let $K = \mathbb{F}_{p^n}, L = \mathbb{F}_{p^m}$ subfields of $E = \mathbb{F}_{p^{[n,m]}}$. Let k such that $m \equiv k \ (mod\ n)$ and $\phi_n^k = \sigma_1 \cdots \sigma_s$ a complete factorization, where σ_h has order r_h, $h = 1, \ldots, s$. For each $h = 1, \ldots, s$, let a_h be a generator of the extension $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{r_h m}}$ and $\{\delta_0(x), \ldots, \delta_{p^n-1}(x)\}$ be a cycle basis for $\mathbb{P}_K^L$ associated to these generators.*

Then the Vandermonde-Frobenius matrix of this cycle basis is

$$V_F(\delta_0, \ldots, \delta_{p^n-1}) = X(\alpha_1, \ldots, \alpha_{p^n}) \cdot C,$$

where $E = \{\alpha_1, \ldots, \alpha_{p^n}\}$.

Moreover,

$$v_F(\delta_0, \ldots, \delta_{p^n-1}) = (-1)^{\mathrm{sgn}(\varphi_n^k)} \prod_{i=1}^{p^n} (\alpha_j - \alpha_i) \prod_{h=1}^{s} c_{r_h,m}(a_h).$$

Example 3.12. This is Example 3.8 revisited. Note that $n = 2, m = 3, k = 1$. As noted earlier, $\varphi_2 = (0)(1,2)(3)$.

The elements of $\mathbb{F}_4$ are $0, 1, \beta = \alpha^3 + \alpha^2 + \alpha = \alpha^{21}$ and β^2. So, β generates $\mathbb{F}_4$ over $\mathbb{F}_2$.

Withe the notations introduced earlier, $\sigma_1 = \sigma_3 = id, \sigma_2 = (12)$ and $\alpha_1 = \alpha_3 = 1, \alpha_2 = \beta = \alpha^{21}$.

Moreover, $v(0, 1, \beta, \beta^2) = \beta^2 + \beta = 1$ and $c_{2,3}(\alpha^{21}) = v(\beta, \beta^8) = \beta^8 + \beta = \alpha^{168} + \alpha^{21} = 1$.

According to our formula, we should have

$$v_F(\delta_0, \delta_1, \delta_2, \delta_3) = 1,$$

which can also be seen directly from Example 3.8.

Acknowledgement. The first author thanks Priyank Kalla for questions that motivated this research and Adil Virani for conversations related to this work. The first author was partially supported by the NSF grant CCF-1320385.

References

[1] J. Hull, Subfield-Compatible Polynomials over Finite Fields, *Rose-Hulman Undergraduate Mathematics Journal*, **14:2**, (2013).

[2] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications **20**, Cambridge Univ Press (1997).

[3] J. Lv, P. Kalla, and F. Enescu, Efficient Grobner Basis Reductions for Formal Verification of Galois Field Arithmetic Circuits, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **32**, 1409–1420 (2013).

[4] E. Meijering, A chronology of interpolation: from ancient astronomy to modern signal and image processing, *Proceedings of the IEEE* **90(3)**, 319–342, doi:10.1109/5.993400.

Received: 09.06.2017
Accepted: 02.08.2017

(1) Department of Mathematics and Statistics, Georgia State University, Atlanta GA 30303
E-mail: fenescu@gsu.edu

(2) Department of Mathematics, University of Utah, Salt Lake City, UT, 84112
E-mail: hull.john@gmail.com