Characterization of $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials

Gary Salazar
Department of Mathematics
Trinity University
San Antonio, TX 78212
gsalazar@trinity.edu

January 22, 2004

Abstract

We extend L. Rédei's definition of polynomials with a restricted range to include multivariable polynomial functions. Given a proper subfield $\mathbb{F}_s$ of the finite field $\mathbb{F}_q$, we identify all $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ (with $\deg_{x_i} f < q$ for $1 \leq i \leq k$) such that for all $\gamma \in \mathbb{F}_q^k$ we have $f(\gamma) \in \mathbb{F}_s$.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and let $\mathbb{F}_q^k$ be the set of all k-tuples of elements in $\mathbb{F}_q$. In this paper we examine multivariable functions with restricted range. Specifically, for a field $\mathbb{F}_q$ and a proper subfield $\mathbb{F}_s$, we wish to classify all functions $f(x_1, \ldots, x_k)$ such that $f(\gamma) \in \mathbb{F}_s$ for all $\gamma \in \mathbb{F}_q^k$.

We first review some facts about finite fields and functions defined over them. Recall that for a finite field $\mathbb{F}_q$ the multiplicative group of nonzero elements is cyclic, i.e. $\mathbb{F}_q^\times = \langle \alpha \rangle$. Suppose that $q = s^a$ where s and a are positive integers greater than 1. Then, there exists a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ with $\mathbb{F}_s^\times = \langle \alpha^b \rangle$ where $b = (q-1)/(s-1) = \sum_{i=0}^{a-1} s^i$.

It is well-known that every function $f(x_1, \ldots, x_k)$ such that $f(\gamma) \in \mathbb{F}_q$ for all $\gamma \in \mathbb{F}_q^k$ can be uniquely represented by a polynomial function in $\mathbb{F}_q[x_1, \ldots, x_k]$ in which no variable exponent exceeds $q-1$. Henceforth, we can restrict our attention to all such polynomial functions.

Definition 1.1. Let $\mathbb{F}_s$ be a subfield of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called an $(\mathbb{F}_q, \mathbb{F}_s)$-*polynomial* if for each $\gamma \in \mathbb{F}_q$, we have $f(\gamma) \in \mathbb{F}_s$.

Rédei [1] classified all such $(\mathbb{F}_q, \mathbb{F}_s)$-polynomials. We extend this notion to include multivariable polynomials.

Definition 1.2. Let $\mathbb{F}_s$ be a subfield of $\mathbb{F}_q$. A polynomial $f(x_1, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$ is called an $(\mathbb{F}_q^k, \mathbb{F}_s)$-*polynomial* if for each $\gamma \in \mathbb{F}_q^k$, we have $f(\gamma) \in \mathbb{F}_s$.

We can see that there are $s^{(q^k)}$ distinct functions f such that $f(\gamma) \in \mathbb{F}_s$ for all $\gamma \in \mathbb{F}_q^k$. In addition if f and g are both $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials and $c \in \mathbb{F}_s$, then we see that both $f + g$ and cf are $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials. Furthermore, it can be easily verified that the set of all $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials forms an $\mathbb{F}_s$-vector space of dimension q^k. We wish to find a basis for this vector space and provide an easy method to not only generate these polynomials, but also to be able to verify by inspection whether or not a given polynomial is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial.

2 Cycles and Periods

Definition 2.1. For any nonnegative integer $i < q$ we can write its s-adic representation

$$i = i_0 + i_1 s + i_2 s^2 + \cdots + i_{a-1} s^{a-1}$$

where $0 \leq i_j < s$ for $0 \leq j \leq a-1$. From this we define the *cyclic numeral-permutation*

$$(is)_{q-1} := i_{a-1} + i_0 s + i_1 s^2 + \cdots + i_{a-2} s^{a-1}.$$

More generally, for any positive integer $j < a$ put

$$(is^j)_{q-1} := i_{a-j} + \cdots + i_{a-1} s^{j-1} + i_0 s^j + \cdots + i_{a-j-1} s^{a-1}.$$

In essence, this results in j cyclic shifts of the numerals $i_0, \ldots, i_{a-1}$.

Remark 2.1. i) Note that $(is^j)_{q-1} = 0$ if and only if $i = 0$.
ii) The representation of $(is^j)_{q-1}$ is well-defined since $0 \leq (is^j)_{q-1} < q$ and $(is^j)_{q-1} \equiv is^j \pmod{q-1}$.

Definition 2.2. For each integer i such that $0 \leq i \leq q-1$ we define the *s-period* of i, denoted $l(i)$, to be the smallest natural number j such that $(is^j)_{q-1} = i$. In other words, $l(i)$ is the fewest number of cyclic shifts needed to restore the values of the s-adic numerals of i.

Remark 2.2. Let p be a divisor of a. Since we have s possibilities for each s-adic numeral, the number of nonnegative integers $i < q$ such that $(is^p)_{q-1} = i$ is s^p. For each such i we know that $l(i)$ must divide p. Otherwise, if $p = dl(i) + r$ for integers d and r with $0 < r < l(i)$, then we would have $(is^r)_{q-1} = i$ which is a contradiction. As a result, there are exactly s^p integers whose s-period divides p. In particular, for $p = a$ we know that $l(i)|a$ for $0 \leq i < q$.

Definition 2.3. Let

$$M = \{x_1^{e_1} x_2^{e_2} \dots x_k^{e_k} : 0 \leq e_i < q \text{ for } 1 \leq i \leq k\}$$

and

$$I_q = \langle x_1^q - x_1, x_2^q - x_2, \dots, x_k^q - x_k \rangle.$$

For any monomial m, let $\overline{m} \in M$ denote the residue of m modulo I_q.

Definition 2.4. For $m = x_1^{e_1} x_2^{e_2} \dots x_k^{e_k} \in M$ we define the s-period of m, denoted $l(m)$ or simply l, as $l(m) = \text{lcm}\{l(e_1), \dots, l(e_k)\}$.

Remark 2.3. i) Since $l(e_i)|a$ for $1 \leq i \leq k$, we know that $l(m)|a$.
ii) The s-period $l(m)$ is the smallest natural number j such that $\overline{m^{s^j}} = m$. This follows since if $m = x_1^{e_1} x_2^{e_2} \dots x_k^{e_k}$, then $m^{s^j} = x_1^{e_1 s^j} x_2^{e_2 s^j} \dots x_k^{e_k s^j}$ and $\overline{m^{s^j}} = x_1^{(e_1 s^j)_{q-1}} x_2^{(e_2 s^j)_{q-1}} \dots x_k^{(e_k s^j)_{q-1}}$.

Proposition 2.1. *Let $m = x_1^{e_1} x_2^{e_2} \dots x_k^{e_k} \in M$ and put $b = (q-1)/(s-1)$. Then, m has s-period $l(m) = 1$ if and only if $b|e_i$ for $1 \leq i \leq k$.*

Proof. From Definition 2.4, $l(m) = 1$ if and only if $l(e_i) = 1$ for $1 \leq i \leq k$. Furthermore, $l(e_i) = 1$ if and only if there exists a nonnegative integer $j < s$ such that

$$e_i = j + js + js^2 + \dots + js^{a-1} = j \sum_{i=0}^{a-1} s^i = j(q-1)/(s-1).$$

□

Corollary 2.1. *There are s^k monomials in M with an s-period value of* 1.

We can recursively determine the number of monomials in M with any arbitrary s-period using the following proposition.

Proposition 2.2. *Let $N(d)$ denote the number of monomials in M with an s-period of d. For any divisor p of a, we have $\sum_{d|p} N(d) = s^{pk}$.*

Proof. Let p be a divisor of a. From Definition 2.4 we see that for any $m = x_1^{e_1} x_2^{e_2} \dots x_k^{e_k} \in M$ that $l(m)|p$ if and only if $l(e_i)|p$ for $1 \leq i \leq k$. By Remark 2.2, there are s^p such values for each exponent e_i. Hence, the conclusion holds. □

Definition 2.5. For $m \in M$ with s-period l, we define

$$\Psi(m) = \{m, \overline{m^s}, \overline{m^{s^2}}, \dots, \overline{m^{s^{l-1}}}\}$$

to be the *monomial cycle* of m.

Remark 2.4. i) If $m' \in \Psi(m)$, then $\Psi(m') = \Psi(m)$.
ii) The monomial cycles constitute a partition of M.

3 Basis Generation

Place a total ordering $<_t$ on the monomials of M and let

$$A = \{m \in M : m \leq_t m' \text{ for all } m' \in \Psi(m)\}.$$

Observe that A is simply a set of cycle representatives.

Proposition 3.1. *Suppose $m \in A$ with s-period l and $c \in \mathbb{F}_{s^l}$. Put*

$$\mathcal{P}_c(m) = cm + c^s \overline{m^s} + \dots + c^{s^{l-1}} \overline{m^{s^{l-1}}}.$$

The polynomial $\mathcal{P}_c(m)$ is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial.

Proof. Since $\overline{m^{s^l}} = m$, then for each $\gamma \in \mathbb{F}_q^k$ we have $[m(\gamma)]^{s^l} = m(\gamma)$. Therefore, $m(\gamma) \in \mathbb{F}_{s^l}$. Put $\delta = cm(\gamma) \in \mathbb{F}_{s^l}$, then note that

$$[\mathcal{P}_c(m)](\gamma) = \delta + \delta^s + \dots + \delta^{s^{l-1}} = Tr(\delta)$$

where Tr is the well-known (cf. [2]) trace function from $\mathbb{F}_{s^l}$ into $\mathbb{F}_s$. □

Remark 3.1. If $c = 0$, then $\mathcal{P}_c(m) = 0$. If $c \neq 0$, then Supp $\mathcal{P}_c(m) = \Psi(m)$.

Definition 3.1. Suppose $m \in A$ with s-period l and $\{\beta_1, \ldots, \beta_l\}$ is a basis of $\mathbb{F}_{s^l}$ over $\mathbb{F}_s$ where $\mathbb{F}_s \subseteq \mathbb{F}_{s^l} \subseteq \mathbb{F}_q$. Put

$$B(m) = \{\mathcal{P}_{\beta_1}(m), \mathcal{P}_{\beta_2}(m), \ldots, \mathcal{P}_{\beta_l}(m)\}.$$

Suppose $c = a_1\beta_1 + \cdots + a_l\beta_l \in \mathbb{F}_{s^l}$ with $a_i \in \mathbb{F}_s$ for $1 \leq i \leq l$. Then, observe that

$$c^s = (a_1\beta_1)^s + \cdots + (a_l\beta_l)^s = a_1\beta_1^s + \cdots + a_l\beta_l^s$$

implies that

$$\mathcal{P}_c(m) = \sum_{i=1}^{l} \mathcal{P}_{a_i\beta_i}(m) = \sum_{i=1}^{l} a_i\mathcal{P}_{\beta_i}(m).$$

From this observation we obtain the following remarks.

Remark 3.2. i) Since $\{\beta_1, \ldots, \beta_l\}$ is $\mathbb{F}_s$-linear independent, we know that $B(m)$ is also $\mathbb{F}_s$-linear independent. Therefore, $\mathrm{Span}_{\mathbb{F}_s} B(m)$ is an $\mathbb{F}_s$-vector space of dimension $l(m)$.
ii) A polynomial f is in $\mathrm{Span}_{\mathbb{F}_s} B(m)$ if and only if f is of the form $\mathcal{P}_c(m)$ for some $c \in \mathbb{F}_{s^l}$.

Theorem 3.1. *Put $\mathcal{U} := \cup_{m\in A} B(m)$. Then, $\mathcal{U}$ is a basis for the $\mathbb{F}_s$-vector space of all $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials.*

Proof. Note that for any nonzero $f \in \mathrm{Span}_{\mathbb{F}_s} B(m)$, we have $\mathrm{Supp}(f) = \Psi(m)$ by Remarks 3.2 ii) and 3.1. Also, for any distinct $m_1, m_2 \in A$, we have $\Psi(m_1) \cap \Psi(m_2) = \emptyset$. Therefore, $\mathrm{Span}_{\mathbb{F}_s}\mathcal{U}$ is the internal direct sum of the family $\{\mathrm{Span}_{\mathbb{F}_s} B(m) : m \in A\}$ of $\mathbb{F}_s$-vector spaces. Hence, $\mathrm{Span}_{\mathbb{F}_s}\mathcal{U}$ is an $\mathbb{F}_s$-vector space of dimension

$$\sum_{m\in A} \dim_{\mathbb{F}_s} \mathrm{Span}_{\mathbb{F}_s} B(m) = \sum_{m\in A} l(m) = \sum_{m\in A} |\Psi(m)| = q^k$$

with basis $\mathcal{U}$. On the other hand, every $f \in \mathcal{U}$ is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial by Proposition 3.1. Therefore, $\mathcal{U}$ is also a basis for the $\mathbb{F}_s$-vector space of all $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomials of dimension q^k. □

Corollary 3.1. *Let f be an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial. Suppose $A \cap \mathrm{Supp}(f) = \{m_1, \ldots, m_n\}$ and let c_i be the coefficient of m_i in f. Then, $f = \sum_{i=1}^{n} \mathcal{P}_{c_i}(m_i)$.*

Proof. From the proof of Theorem 3.1, we know that $\mathrm{Span}_{\mathbb{F}_s}\mathcal{U}$ is the direct sum of the family $\{\mathrm{Span}_{\mathbb{F}_s} B(m) : m \in A\}$. By Remark 3.2 ii) the conclusion holds. □

Definition 3.2. Suppose $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ with $\mathrm{Supp}(f) \subseteq M$. We will say that f satisfies the *s-power property* if for each monomial $m \in \mathrm{Supp}(f)$ with coefficient c, we have $\overline{m^s} \in \mathrm{Supp}(f)$ with coefficient c^s.

In the single variable case the s-power property is the same as the conjugacy conditions of Proposition 6 in [1]. Observe that the polynomial $\mathcal{P}_c(m)$ in Proposition 3.1 satisfies the s-power property since $c^{s^l} = c$ and $\overline{m^{s^l}} = m$ by Remark 2.3 ii).

Theorem 3.2. *A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ with $Supp(f) \subseteq M$ is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial if and only if f satisfies the s-power property.*

Proof. Suppose that f satisfies the s-power property. Choose a monomial $m \in \mathrm{Supp}(f)$ which has s-period l and coefficient c. Since $\overline{m^{s^l}} = m$, the s-power property implies that $c^{s^l} = c$. Hence, $c \in \mathbb{F}_{s^l}$. Let $m' \in A$ denote the cycle representative of $\Psi(m)$. Then, the s-power property implies that $m' \in \mathrm{Supp}(f)$ with some coefficient in $\mathbb{F}_{s^l}$.

Suppose that $A \cap \mathrm{Supp}(f) = \{m_1, \ldots, m_n\}$ and define $l_i := l(m_i)$ and let $c_i \in \mathbb{F}_{s^{l_i}}$ be the coefficient of m_i in f. Then, $f = \sum_{i=1}^n \mathcal{P}_{c_i}(m_i)$ which by Proposition 3.1 is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial.

Conversely, assume that f is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial. By Corollary 3.1 f can be expressed as the direct sum of polynomials that satisfy the s-power property. Hence, f must satisfy the s-power property itself. □

Observe that Theorem 3.2 is independent of A. This has the benefit of enabling us to verify by inspection whether or not a polynomial is an $(\mathbb{F}_q^k, \mathbb{F}_s)$-polynomial. In addition we can also easily generate these polynomials by just ensuring that they satisfy the s-power property.

Example 3.1. Consider the field $\mathbb{F}_{16}$ where $\mathbb{F}_{16}^\times = \langle\alpha\rangle$ and the subfields $\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_{16}$. Examine the polynomial

$$f(x, y) = x^8y^9 + \alpha x^4y^{12} + \alpha^5x^{10} + x^2y^6 + \alpha^{10}x^5 + \alpha^4xy^3.$$

Observe that for each monomial $m \in \mathrm{Supp}(f)$ we have $\overline{m^2} \in \mathrm{Supp}(f)$. To see this more clearly we rewrite f as

$$f(x, y) = (\alpha^4xy^3 + x^2y^6 + \alpha x^4y^{12} + x^8y^9) + (\alpha^{10}x^5 + \alpha^5x^{10}).$$

Note that f does not satisfy the 2-power property since $m = xy^3 \in \mathrm{Supp}(f)$ with coefficient α^4, but $\overline{m^2} = x^2y^6$ has coefficient $1 \neq (\alpha^4)^2$. On the other hand, we see that f does satisfy the 4-power property. As a result, f is an $(\mathbb{F}_{16}^2, \mathbb{F}_4)$-polynomial, but not an $(\mathbb{F}_{16}^2, \mathbb{F}_2)$-polynomial.

References

[1] L. Rédei, *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.

[2] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York, 1982.