Classifications of $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials

Jaime Lamb

June 6, 2002

1 Introduction

Much research has been conducted examining functions mapping a finite field into itself. Dickson [?] established that each multivariate function that maps $\mathbb{F}_q^k \rightarrow \mathbb{F}_s$ can be represented by a polynomial function in the ring $\mathbb{F}_q[x_1, ...x_k]$. Redeí [?] examined polynomials that mapped $\mathbb{F}_q \rightarrow \mathbb{F}_s$ where $\mathbb{F}_s$ is a subfield of $\mathbb{F}_q$. We shall use the notation of Redeí beginning with the following definition.

Definition 1. *A polynomial $f(x) \in \mathbb{F}_q[x]$ is called an $(\mathbb{F}_q, \mathbb{F}_s)$-polynomial if all the values of $f(\gamma)$ (with $\gamma \in \mathbb{F}_q$) are contained in a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$.*

Polynomials that map $\mathbb{F}_4^k \rightarrow \mathbb{F}_2$ has not been an area that has been examined extensively. By examining these polynomials, we will establish necessary and/or sufficient conditions for identification of these so-called $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials.

Recall, $\mathbb{F}_4$ is the finite field with 4 elements, i.e. $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 = \alpha+1$. From this we have the additional relationships $\alpha^3 = 1$ and $\alpha^4 = \alpha$. The field $\mathbb{F}_4$ has only one proper subfield, namely $\mathbb{F}_2 = \{0, 1\}$. Dickson [?] determined that all functions that map $\mathbb{F}_4$ into itself can be represented as polynomials of degree less than four. The following table illustrates Dickson's reasoning:

x	x^4
0	0
1	1
α	$\alpha^4 = \alpha$
α^2	$(\alpha^2)^4 = \alpha^8 = \alpha^2$

The polynomials $f(x) = x$ and $g(x) = x^4$ are the same function. Therefore, any polynomial of degree four or higher is equivalent (as functions) to one whose degree does not exceed 3.

2 $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials

The first type of polynomials we will investigate are $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials. Let α denote a fixed primitive element of $\mathbb{F}_4$, i.e. $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 = \alpha + 1$. The following is an example of an $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial.

x	$f(x) = x^2 + x + 1$
0	1
1	$1^2 + 1 + 1 = 1$
α	$\alpha^2 + \alpha + 1 = 0$
α^2	$\alpha^4 + \alpha^2 + 1 = \alpha + \alpha^2 + 1 = 0$

Since $\mathbb{F}(\gamma)$ is in $\{0, 1\}$ for all $\gamma \in \mathbb{F}_4$, we know that this polynomial does map $\mathbb{F}_4$ into $\mathbb{F}_2$. On the other hand, an example of a function that is not an $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial is x^2. The following table illustrates this fact.

x	$g(x) = x^2$
0	0
1	1
α	α^2
α^2	$\alpha^4 = \alpha$

We see that since $g(\alpha) = \alpha^2 \notin \mathbb{F}_2$, we have that $g(x)$ does not map to $\mathbb{F}_2$.

By Dickson's observations [**?**], all functions that map $\mathbb{F}_4$ into $\mathbb{F}_2$ are precisely represented by the polynomials in $\mathbb{F}_4[x]$ of degree less than four. In 1973, Redeí [**?**] examined the more general case of $(\mathbb{F}_q, \mathbb{F}_s)$-polynomials where $\mathbb{F}_s$ is a subfield of $\mathbb{F}_q$. He was able to classify all $(\mathbb{F}_q, \mathbb{F}_s)$-polynomials with the following theorem.

Theorem 1. *(Redeí): A polynomial*

$$f(x) = \sum_{i=0}^{q-1} \beta_i x^i \quad (\beta_i \in \mathbb{F}_q)$$

is an $(\mathbb{F}_q, \mathbb{F}_s)$-polynomial if and only if its coefficients satisfy the two following conditions:

(i) $\beta_j = \beta_i^s$ *whenever* $j \equiv si \mod(q-1)$ *for* $0 \leq i, j < q-1$; *and*
(ii) $\beta_{q-1} = \beta_{q-1}^s$.

We claim that there are 16 $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials. Given such a polynomial f, for each domain element $\gamma \in \mathbb{F}_4$ we have two choices for $f(\gamma)$, namely 0 or 1. Since there are four domain elements we have $2^4 = 16$ possibilities. By Redeí's Theorem, when $q = 4$ and $s = 2$ we have that $f(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3$ is a $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial if and only if $\beta_j = \beta_i^2$ when $j \equiv 2i \pmod 3$ for $i, j \in \{0, 1, 2\}$ and $\beta_3 = \beta_3^2$. This implies that $\beta_1^2 = \beta_2$ and $\beta_2^2 = \beta_1$ and both β_0 and β_3 are in $\mathbb{F}_2$. In our case this reduces to the following polynomials of degree less than four.

The $(\mathbb{F}_4, \mathbb{F}_2)$ polynomials of degree zero are $f(x) = 0$ and $f(x) = 1$. There are no such polynomials of degree one. The polynomials of degree two are

$$\begin{array}{lll} f(x) = x^2 + x; & f(x) = x^2 + x + 1; & f(x) = \alpha x^2 + \alpha^2 x; \\ f(x) = \alpha x^2 + \alpha^2 x + 1; & f(x) = \alpha^2 x^2 + \alpha x; & f(x) = \alpha^2 x^2 + \alpha x + 1, \end{array}$$

where α denotes a primitive element of $\mathbb{F}_4$. Finally, the polynomials of degree three are of the form x^3 plus some $\mathbb{F}_2$-linear combination of the preceding $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials of lesser degree. By inspection we see that

$$\{1,\, x^2 + x,\, \alpha^2 x^2 + \alpha x,\, x^3\},$$

is an $\mathbb{F}_2$ basis for the $(\mathbb{F}_4,\ \mathbb{F}_2)$-polynomials. Furthermore, note that no proper summand of any polynomial of this basis is an $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial. In other words, if you partition the terms of a polynomial to form two polynomials, neither polynomial will be an $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial. For example, for the basis polynomial $x^2 + x$, neither x^2 nor x is an $(\mathbb{F}_4, \mathbb{F}_2)$-polynomial. In this manner, we may say this basis is minimal.

We shall extend the definition of an $(\mathbb{F}_q, \mathbb{F}_s)$-polynomial to include multivariable functions.

Definition 2. *A multivariate polynomial* $f(x_1, ..., x_k) \in I\!F_q[x_1, ..., x_k]$ *shall be called an* $(I\!F_q^k, I\!F_s)$*-polynomial if all the values of* $f(\gamma)$ *(with* $\gamma \in I\!F_q$*) are contained in a subfield* $I\!F_s$ *of* $I\!F_q^k$*.* .

Lemma 1. *Suppose* f *is in* $I\!F_4[x_1, x_2, ..., x_k]$*. Then* f *is an* $(I\!F_4^k, I\!F_2)$*-polynomial if and only if* $[f(\gamma)]^2 = f(\gamma)$*.*

Proof. Let f be a polynomial in $I\!F_4[x_1, x_2, ..., x_k]$. If f is an $(I\!F_4^k, I\!F_2)$-polynomial, then $f(\gamma) \in I\!F_2$ for all $\gamma \in I\!F_4^k$. Therefore, $[f(\gamma)]^2 = f(\gamma)$.
Conversely, since $f \in I\!F_4[x_1, x_2, ..., x_k]$, then for each $\gamma \in I\!F_4^k$ we have that $f(\gamma) \in I\!F_4$. If in addition, $[f(\gamma)]^2 = f(\gamma)$ for all γ, then $f(\gamma) \in I\!F_2$. Thus, f is an $(I\!F_4^k, I\!F_2)$-polynomial. □

Theorem 2. *The function* $f(x_1, ..., x_k) = c^2x_1^{2e_1}x_2^{2e_2}...x_k^{2e_k} + cx_1^{e_1}...x_k^{e_k}$ *with* $c \in I\!F_4$ *is an* $(I\!F_4^k, I\!F_2)$*-polynomial.*

Proof. By the lemma, we need to show that $(f^2 - f)(\gamma) = 0$ for all $\gamma \in I\!F_4^k$. Note that modulo 2,we have

$$\begin{aligned} f^2 - f &= (c^2x_1^{2e_1}...x_k^{2e_k} + cx_1^{e_1}...x_k^{e_k})^2 - (c^2x_1^{2e_1}...x_k^{2e_k} + cx_1^{e_1}...x_k^{e_k}) \\ &= c^4x_1^{4e_1}...x_k^{4e_k} + 2(c^3x_1^{3e_1}...x_k^{3e_k}) + (c^2x_1^{2e_1}...x_k^{2e_k}) \\ &\quad -(c^2x_1^{2e_1}...x_k^{2e_k} + cx_1^{e_1}...x_k^{e_k}) \\ &= c^4x_1^{4e_1}...x_k^{4e_k} + (c^2x_1^{2e_1}...x_k^{2e_k} - c^2x_1^{2e_1}...x_k^{2e_k}) - cx_1^{e_1}...x_k^{e_k} \\ &= (cx_1^{e_1}x_2^{e_2}...x_k^{e_k})^4 - (cx_1^{e_1}x_2^{e_2}...x_k^{e_k}). \end{aligned}$$

Then we must have that $(f^2 - f)(\gamma) = 0$ since $\gamma \in I\!F_4^k$ implies that $cx_1^{e_1}x_2^{e_2}...x_k^{e_k} \in I\!F_4$. □

3 $(I\!F_4^2, I\!F_2)$-polynomials

Put $S = \{1, x^2 + x, \alpha^2x^2 + \alpha x, x^3\}$ and $T = \{1, y^2 + y, \alpha^2y^2 + \alpha y, y^3\}$. A basis for the $(I\!F_4^2, I\!F_2)$-polynomials consists of the elements of the set ST where $ST = \{st | s \in S \text{ and } t \in T\}$. Since S and T are each $I\!F_2$-linearly independent and $\text{span}(S) \bigcap \text{span}(T) = \{1\}$, then the set ST is $I\!F_2$-linearly independent as well [**?**]. These basis polynomials are the following:

1	$x^2 + x$	$\alpha^2x^2 + \alpha x$	x^3
$y^2 + y$	$(x^2 + x)(y^2 + y)$	$(\alpha^2x^2 + \alpha x)(y^2 + y)$	$x^3(y^2 + y)$
$\alpha^2y^2 + \alpha y$	$(x^2 + x)(\alpha^2y^2 + \alpha y)$	$(\alpha^2x^2 + \alpha x)(\alpha^2y^2 + \alpha y)$	$x^3(\alpha^2y^2 + \alpha y)$
y^3	$(x^2 + x)y^3$	$(\alpha^2x^2 + \alpha x)y^3$	x^3y^3

However, these basis polynomials fail to have the property that no proper summand is a basis polynomial. For example, consider the $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomial $(x^2+x)(y^2+y)$. Observe that

$$\begin{aligned}(x^2+x)(y^2+y) &= x^2y^2 + x^2y + xy^2 + xy \\ &= (x^2y^2+xy) + (x^2y+xy^2).\end{aligned}$$

However, it can be verified that x^2y^2+xy and x^2y+xy^2 are both $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials.

Our goal is to build a basis that maintains this property. The only monomials which are $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials are $1, x^3, y^3$, and x^3y^3. In order to find the non-monomial $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials we first introduce some notation and comments about general multivariable polynomial functions. Given a term $m = cx_1^{e_1}x_2^{e_2}...x_k^{e_k}$, where $e_i \in \{0,1,2,3\}$ for all i and $c \in \mathbb{F}_4$. We define $\overline{m^2}$ to be the term given by $\overline{m^2} = c^2x_1^{p_1}x_2^{p_2}...x_k^{p_k}$ where

$$p_i = \begin{cases} 2e_i & \text{if } e_i < 2 \\ 2e_i - 3 & \text{if } e_i \geq 2. \end{cases}$$

In other words, the term $\overline{m^2}$, is the reduction of m^2 modulo the ideal

$$(x_1^4 - x_1, x_2^4 - x_2, ..., x_k^4 - x_k).$$

Remarks.

(i) $e_i = 0$ *if and only if* $p_i = 0$
(ii) $\overline{m^2}$ *divides* m^2

Proposition 1. *Let* $m = cx_1^{e_1}x_2^{e_2}...x_k^{e_k}$ *be a term and* $\overline{m^2} = c^2x_1^{p_1}x_2^{p_2}...x_k^{p_k}$ *as defined above. Then, viewing* m *and* $\overline{m^2}$ *as functions we see that for any choice of* $\gamma = (x_1,...,x_k) \in \mathbb{F}_4^k$, *we have* $\overline{m^2}(\gamma) = m^2(\gamma)$.

Proof. Suppose that $m^2(\gamma) = 0$. This implies that $x_i = 0$ for some $x_i \in \gamma$ and $e_i \neq 0$. By the above remark, $p_i \neq 0$ implies that $\overline{m^2}(\gamma) = 0$. Now, we may assume that $m^2(\gamma) \neq 0$. Note that $m^2 = \overline{m^2}(x_1^{r_1}...x_k^{r_k})$ where $r_i = 2e_i - p_i \in \{0,3\}$. Thus, $x_1^{r_1}...x_k^{r_k} = 1$ for any $\gamma \in \mathbb{F}_4^k$. Therefore, $\overline{m^2}$ is the same function as m^2. □

From Theorem 2 and Proposition 1 we receive the following corollary.

Corollary 1. *For a term m, the polynomial $m+\overline{m^2}$ is an $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial.*

Hence, the 2^{16}-many $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials are generated by the following 16 polynomials:

$$1,\ x^3,\ y^3,\ x^3y^3,$$

$$\begin{array}{rl} x+x^2 & \alpha x+\alpha^2x^2, \\ y+y^2 & \alpha y+\alpha^2y^2, \\ xy+x^2y^2 & \alpha xy+\alpha^2x^2y^2, \\ xy^2+x^2y & \alpha xy^2+\alpha^2x^2y, \\ x^3y+x^3y^2 & \alpha x^3y+\alpha^2x^3y^2, \\ xy^3+x^2y^3 & \alpha xy^3+\alpha^2x^2y^3 \end{array}$$

Clearly, the first 4 polynomials, namely $1, x^3, y^3$, and x^3y^3, cannot be represented as an $\mathbb{F}_2$-linear combination of the other 12 polynomials since none of $1, x^3, y^3$, or x^3y^3 appear in the other 12 polynomials. Further note that no two polynomials in the left column possess an identical monomial. Also, for each polynomial $m+\overline{m^2}$ in the left column, there is a corresponding polynomial $\alpha m+\alpha^2\overline{m^2}$ in the right column. Since
$(m+\overline{m^2})+(\alpha m+\alpha^2\overline{m^2}) = (1+\alpha)m+(1+\alpha^2)\overline{m^2} = \alpha^2 m+(\alpha^2)^2\overline{m^2} \neq 0$,
then these 16 polynomials are an $\mathbb{F}_2$-linearly independent set.

Remarks.

(*i*) *A polynomial f is an $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomial if and only if it is an $\mathbb{F}_2$-linear combination of these 16.*

(*ii*) *A polynomial f is an $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomial if and only if for every m in f, the term $\overline{m^2}$ is also in f.*

This gives us the two following benefits. First, it is very easy to form the $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials from this basis. That is, we can take any number of the 16 basis polynomials and add them together to find an $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomial. Secondly, we can tell by inspection whether or not a polynomial f is an $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomial by remark (ii).

4 $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials

There are 2^{4^k} $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials. Hence, an $\mathbb{F}_2$-basis would consist of 4^k polynomials. We will proceed to find a basis in a simliar vein as in section 3. For which monomials m does $\overline{m^2} = m$ hold? All the monomials of the form $x_1^{e_1} x_2^{e_2} ... x_k^{e_k}$ where $e_i \in \{0, 3\}$ have this property. There are 2^k of this type. All of these are $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials, since $\gamma^3 \in \{0, 1\}$ for all $\gamma \in \mathbb{F}_4$.

This leaves, $4^k - 2^k$ monomial whose "squares" are not themselves. Therefore, there are $\frac{1}{2}(4^k - 2^k)$ many $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials of the form $m + \overline{m^2}$ where $m <_t \overline{m^2}$ under some total monomial ordering $<_t$.
We have

$$\begin{array}{ll} \frac{1}{2}(4^k - 2^k) & \text{of the form } m + \overline{m^2}; \text{ and} \\ \frac{1}{2}(4^k - 2^k) & \text{of the form } \alpha m + \alpha^2 \overline{m^2}. \end{array}$$

¿From corollary 1, we know that all of these are $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials also. We now have

$$2^k \; + \; \tfrac{1}{2}(4^k - 2^k) \; + \; \tfrac{1}{2}(4^k - 2^k) \; = \; 4^k,$$

$\mathbb{F}^2$-linearly independent $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials. These form a basis for the $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials. Therefore, a polynomial f is an $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial if and only if it is an $\mathbb{F}_2$-linear combination of these 4^k polynomials. By our earlier argument on the two-dimentional case, since
$(m + \overline{m^2}) + (\alpha m + \alpha^2 \overline{m^2}) = (1 + \alpha)m + (1 + \alpha^2)\overline{m^2} = \alpha^2 m + (\alpha^2)^2 \overline{m^2} \neq 0$, is true for any term m in k variables, we see that we also obtain the following theorem.

Theorem 3. *A polynomial f is a $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial if and only if for every term m in f, the term $\overline{m^2}$ is also in f.*

5 Conclusion

By carefully examining the $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials we were able to generate bases for $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials and produced some very interesting results. We extended the case that we proved true for $(\mathbb{F}_4^2, \mathbb{F}_2)$-polynomials to hold for $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials. Through this we are able to tell by inspection if a polynomial is an $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial. It is also very easy to generate an $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial by simple addition of any number of the 2^{4^k} basis polynomials.

References

[1] L.E. Dickson, *General Theory of Modular Invariants*, Trans. America Mathematics Society, 1909.

[2] Rudolf Lidl, *Finite Fields*, Cambridge University Press, 1997.

[3] László Rédei, *Lacunary Polynomials Over Finite Fields*, Budapest, Akademiai Kiado, 1973.