Classifying and Using Polynomials as Maps of the Field $\mathbf{F}_{p^d}$

Dylan Cutler

Jesse Johnson

Benjamin Rosenfield

Kudzai Zvoma

Middlebury College

September 1, 2002

1 Abstract

Every function from a finite field to itself can be represented by a polynomial. So the functions which are also permutations give rise to "permutation polynomials," which have potential applications in cryptology. We will introduce a generalization of permutation polynomials called "degree-preserving polynomials" and show a classification scheme of the latter.

2 Introduction

The criteria for a polynomial to qualify as degree preserving are certainly less stringent than those for the permuting qualification. Thus the idea to study degree-preserving polynomials, as credited to Theresa Vaughan, allows more opportunity to maneuver and gain intuition about the occurrence of such polynomials. Before further discussion of concepts a brief summary of the main relevant ideas in finite fields is given. The following facts are used. Proofs are referenced [4].

- For a given prime p, the field $\mathbf{F}_p$ is isomorphic to $\mathbf{Z}$ mod p.

  For example, $\mathbf{F}_3 = \{0,1,2\}$.

- The set of all polynomials with coefficients in $\mathbf{F}_p$ forms a ring. We express the ring of polynomials over $\mathbf{F}_p$ as $\mathbf{F}_p[x]$.

- For each such polynomial ring and each integer d there exists at least one monic irreducible polynomial $\mathbf{m}(x)$(a polynomial that will not factorize and maintain coefficients from $\mathbf{F}_p$ in its factors) of degree d so that the ring $\mathbf{F}_p[x]$ modulo $\mathbf{m}(x)$ is a field. We express this field as $\mathbf{F}_p[x]/ < \mathbf{m}(x) >$.

- In $\mathbf{F}_p[x]/ < \mathbf{m}(x) >$ the monic irreducible $\mathbf{m}(x)$ has a root α such that $\mathbf{m}(\alpha) = 0$.

- We may now speak of the extension field $\mathbf{F}_{p^d}$ as the set.

  $\{a_0 + a_1\alpha^1 + ... + a_{d-1}\alpha^{d-1} | a_i \in \mathbf{F}_p\}$.

  For example, $\mathbf{F}_{3^2} = \mathbf{F}_9 = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

- Addition of elements within $\mathbf{F}_{p^d}$ is carried out modulo p. Multiplication is also modulo p and $\mathbf{m}(\alpha) = 0$ is applied as necessary to reduce products to standard equivalent expressions in degree less than d.

  For instance consider from the field $\mathbf{F}_{25}$, generated by the monic irreducible polynomial $\mathbf{m}(x) = x^2 + x + 1$, elements $3\alpha + 1$ and $1\alpha + 4$, $2\alpha + 3$, $4\alpha + 1$.

We have $3\alpha + 1 + 1\alpha + 4 = 4\alpha$ and

$(2\alpha + 3) \cdot (4\alpha + 1) = 3\alpha^2 + 4\alpha + 3 = 3(\alpha^2 + \alpha + 1) + \alpha = \alpha.$

- The extension field $\mathbf{F}_{p^d}$ contains a subfield isomorphic to $\mathbf{F}_p$. Henceforth we will merely refer to $\mathbf{F}_{p^d}$ as containing $\mathbf{F}_p$ so that $\mathbf{F}_9$ contains $\mathbf{F}_3$.
- The motivating idea in the handling the of $\mathbf{f} \in \mathbf{F}_p[x]$, the ring of polynomials over $\mathbf{F}_p$, is as follows: consider that each of these polynomials has the form

  $\mathbf{f}(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + ... + a_n x^n$ for $a_i \in \mathbf{F}_p[x]$

This expression is in need of refinement, as there remains a considerably inconvenient amount of redundancy here we will expose and remove, using the following ideas [4].

1 Proposition. *The multiplicative group of the field $\mathbf{F}_{p^d}$ is cyclic.*

2 Proposition. *The order of $\mathbf{F}_{p^d}$ is p^d. For any nonzero element $\lambda \in \mathbf{F}_{p^d}$, $\lambda^{p^d-1} = 1$.*

Consequently we adopt a convention and express each polynomial in the form with degree less than d. So we may assume $\mathbf{f}(x) = \sum_{i=0}^{p^d-1} a_i x^i = a_0 + a_1 x + ... + a_{p^d-1} x^{p^d-1}$ where $a_i \in \mathbf{F}_p[x]$.

We proceed now to recognize that as a result of the additional and multiplicative closure of properties of the field $\mathbf{F}_p$ each of these polynomials of $\mathbf{f} \in \mathbf{F}_p[x]$ represents a mapping from $\mathbf{F}_{p^d}$ to itself.

3 Observation

If the mapping induced by a polynomial $\mathbf{f}$ upon $\mathbf{F}_{p^d}$ is one-to-one and onto, simply describing a permutation of the elements in $\mathbf{F}_{p^d}$, then $\mathbf{f}$ is a permutation polynomial (**PP**).

Permutation polynomials over finite fields have potential applications in coding and encryption [2]. Research and development in this industry continues to reconcile security and efficiency in cryptographic systems . In our particular approach, we shifted focus from permutation polynomials exclusively to work on a related broader class of polynomials.

4 Degree Preserving Polynomials

Before we discuss this broader class. We need to a few definitions about the elements of $\mathbf{F}_{p^d}$.

1 Theorem. *Each element $\alpha \in \mathbf{F}_{p^d}$ is the root of a unique, monic, irreducible polynomial in $\mathbf{F}_p[x]$ [1].*

This theorem leads us to a very important concept in our specific area of study for this paper. That is the concept of the degree of an element. We present the most general definition below.

1 Definition. *The degree of an element α over $\mathbf{F}_p$ is the degree of its unique, monic, irreducible polynomial in $\mathbf{F}_p[x]$.*

It is also worth noting that in our case, where p and d are prime, we have that every $\alpha \in \mathbf{F}_{p^d}$ but not in $\mathbf{F}_p$ is of degree d. The concept of degree leads us into a discussion of the actual topic of this paper: degree preserving polynomials over finite fields (DPP's). First let us define what it means for a polynomial to be degree preserving. The definition is due to Theresa Vaughan.

2 Definition. *A polynomial $f(x) \in \mathbf{F}_{p^d}$ preserves degree d over $\mathbf{F}_p$ if $\forall \alpha \in \mathbf{F}_{p^d}$ of degree d, $f(\alpha)$ also has degree d.*

DPP's are a relatively new area of study. We have been looking for classes of these polynomials and ways to generate them. One reason they might be interesting is their close connection with the afore mentioned permutation polynomials. This connection, also due to Theresa Vaughan, is shown in the next theorem.

2 Theorem. *If $f(x) \in \mathbf{F}_p[x]$ and $f(x)$ is a permutation polynomial for $\mathbf{F}_{p^d}$ then $f(x)$ preserves degree d.*

Proof. If $f(x) \in \mathbf{F}_p[x]$ then all of the elements of $\mathbf{F}_p$ will be mapped to elements of $\mathbf{F}_p$. Thus assume for contradiction that $\varphi \in \mathbf{F}_{p^d}$, $\varphi \notin \mathbf{F}_p$ is mapped to an element of $\mathbf{F}_p$. Then there are not enough elements left in the field to map to all of the elements in $\mathbf{F}_{p^d}$. Thus $f(x)$ does not permute the field, contradicting our given information. Therefore $f(x)$ preserves degree. □

Thus we can see that DPP's are a generalization of permutation polynomials. We will now touch upon some important qualities of degree preserving polynomials. This will lead us into a discussion of how to generate all of the DPP's for a given finite field.

3 Theorem. *If $f(x) \in \mathbf{F}_p[x]$ preserves degree d over $\mathbf{F}_p$, then so do $\alpha \cdot f(x)$, $f(\alpha \cdot x)$, $f(x) + \alpha$, $f(x + \alpha)$, for any non-zero $\alpha \in \mathbf{F}_p$.*

Proof. If β has degree d over $\mathbf{F}_p$ then so do $\alpha + \beta$, $\alpha \cdot \beta$ since $\alpha \in \mathbf{F}_p$ and β is not. □

3 Definition. *For β of degree d over $\mathbf{F}_p$, the conjugates of β are $\beta, \beta^p, \beta^{(p^2)}, ..., \beta^{(p^d-1)}$.*

The following results about conjugates are due to Priscilla Bremser.

4 Theorem. *If $f(x)$ is the minimum polynomial for β of degree d over $\mathbf{F}_p$, the roots of $f(x)$ are the conjugates of β.*

Proof. Since $[f(x)]^p = f(x^p)$ if $f(x) \in \mathbf{F}_p[x]$, $f(\alpha^{(p^j)}) = [f(\alpha)]^{p^j}$ for $j = 1, 2, ..., d-1$. Since f is the minimum polynomial for β, the other roots are $\beta, \beta^p, \beta^{(p^2)}, ..., \beta^{(p^d-1)})$. Since f is a polynomial of degree d, and we have d unique roots, these are all the roots for $f(x)$. □

5 Theorem. *A polynomial $f(x) \in \mathbf{F}_p[x]$ preserves degree d over $\mathbf{F}_p$ iff for any monic irreducible polynomial $g(x)$ of degree d over $\mathbf{F}_p$, $f(x^p) \equiv f(x)$ mod $g(x)$.*

Proof. i) → Suppose α is of degree d over $\mathbf{F}_p$ and $g(x)$ is its minimum polynomial. If $f(x^p) \not\equiv f(x)$ mod $g(x)$, then $f(x^p) - f(x) = p(x)g(x) + r(x)$ with $0 < degr(x) < d$. Since $r(\alpha) = 0$ ($g(x)$ is α's minimum polynomial), we have $[f(\alpha)]^p - f(\alpha) = r(\alpha) \neq 0$. Thus $[f(\alpha)]^p \neq f(\alpha)$, therefore $f(\alpha) \in \mathbf{F}_p$, implying that $f(\alpha)$ has degree d.

ii) ← Assume $g(x)$ is a monic, irreducible polynomial of degree d and $f(x^p) \equiv f(x)$ mod $g(x)$. For a root α of $g(x)$, $[f(\alpha)]^p - f(\alpha) = g(\alpha)k(x) = 0$ for some $k(x)$, thus $[f(\alpha)]^p = f(\alpha)$. This implies that $f(\alpha) \in \mathbf{F}_p$, thus $f(x)$ does not preserve degree d. Therefore $f(x^p) \not\equiv f(x)$ mod $g(x)$. □

6 Corollary. *For a polynomial $f(x) \in \mathbf{F}_p[x]$ and any α of degree d over $\mathbf{F}_p$, $f(\alpha)$ has degree d iff $f(\alpha^{p^i})$, $0 < i < p-1$ has degree d for any conjugate α^{p^i} of α.*

This idea of conjugates turns out to be quite useful in two ways. First, in testing for DPP's, by corollary 1, if we test one from each set of conjugates we can tell if a polynomial is a DPP or not (see appendix). The second way that these conjugates are useful will become apparent shortly. Next we will introduce another class of polynomials over finite fields . We named these degree annihilating polynomials (DAP's), because they take every element in the field and send it to an element in the base field.

4 Definition. *A polynomial $f(x) \in \mathbf{F}_p[x]$ is described as degree annihilating if $\forall \alpha \in \mathbf{F}_{p^d}$, $f(\alpha) \in \mathbf{F}_p$.*

This class of polynomials turns out to be very useful in generating DPP's due to the fact that the addition of any two DPP's yields another distinct DPP. Similarly the addition of a DAP to a known DPP generates another DPP. This is because the addition of a DAP to a DPP is essentially adding an element of the base field to every element in the value set of the DPP. Thus all of the elements of degree d stay of degree d. It is important to note the following features of DAP's, namely the closures under addition (DAP + DAP = DAP) and scalar multiplication (kDAP = DAP). Thus DAP's form a subspace of all polynomials with coefficients in the base field. In our generation of these polynomials (see appendix) we find a basis for this subspace of DAP's.

7 Theorem. *We can generate all of the DAP's for a given finite field by linear combinations of polynomials of the forms i)*$tr(x^i) = (x^i) + (x^i)^p + (x^i)^{(p^2)} + ... + (x^i)^{(p^{(d-1)})}$ *for* i *not a multiple of* $(p^d - 1)/(p-1)$ *and exponents reduced mod* $p^d - 1$*. ii)* $n(x^k) = x^{k((p^d-1)/(p-1))}$ *for* $k = 0, 1, 2, ..., p-1$.

Proof. First we will prove that all of these polynomials are DAP's. This is simple enough. Note that $tr(x)$ and $n(x)$ are the trace and the norm, and are being composed with x^i and x^k respectively to give us our basis of DAP's. Since the trace and the norm are established DAP's, their composition with x^n will certainly result in another DAP. Next we note that all of these polynomials are linearly independent seeing as no two of them contain an x to the same power. Next we will show that they form a basis for the DAP's over a given finite field. We know that we are in an n-dimensional space with $n = p^d$, and with each vector being expressed as an ordered n-tuple. We also know that each set of conjugates gets mapped to a single set of conjugates. However in $\mathbf{F}_p$ a set of conjugates is just a single element. So the subspace of DAP's is isomorphic to the vector space over $\mathbf{F}_p$ of functions from conjugacy classes to $\mathbf{F}_p$. Therefore the dimension of the subspace is $(p^d - p)/d - p$. This dimension is exactly equal to the number of linearly independent DAP's in our set generated by the modified trace and the modified norm. Therefore we have generated a basis for the sub space of DAP's with coefficients in $\mathbf{F}_p$ over the field $\mathbf{F}_p$. □

5 Representatives for Conjugacy Classes

Let α be a primitive element of the field $\mathbf{F}_{p^n}$. Two elements α^a, α^b of $\mathbf{F}_{p^n}$ will be conjugates iff $a \equiv b * p^m (\text{mod } p^n - 1)$ for some $m \in \mathbf{Z}_n$. We shall write a in base p. That is, we consider $a = \sum_{i=0}^{n-1} a_i p^i$. Then, $ap = \sum_{i=0}^{n-1} a_i p^{i+1} = \sum_{i=1}^{n} a_{i-1} p^i$. Since a is considered mod $p^n - 1$, $p^n \equiv 1$ so $ap = a_n + \sum_{i=1}^{n-1} a_{i-1} p^i$.

In other words, we have shifted all the base-p digits of a over one, then moved the last digit to the first. If we do this m times, we transform a into b. Thus, all the conjugates of an element a can be found by a sort of cyclic permutation of the digits of a in base p.

6 Basic Polynomials

Now that we can generate a list of all the DAPs for F_{p^d}, we would like to take advantage of this to generate DPPs. Let α be a primitive element of F_{p^d} Each element $\beta = \alpha^a \in F_{p^d}$ is in a conjugacy class $\{\beta^{(p^k)} | k \in \mathbf{N}\}$. If we think of each element of the conjugacy class as a power of α, we can indicate the class by the associated powers of α. That is, for a given a we consider $\{ap^k | k \in \mathbf{N}\}$, where ap^k is considered modulo $p^d - 1$. We would like to pick a representative for each of these classes, and we will choose the maximal element, $m(a) = \max\{ap^k | k \in \mathbf{N}\}$ (again modulo $p^d - 1$.) We can then collect all out representatives in a set $M = \{m(a) | a \in \mathbf{Z}_{p^d-1}\}$.

For each $m \in M$, there is a monic DAP f_m of degree m, either the trace composed with x^m or the norm composed with x^m. If f is a DPP whose mth coefficient is b, then $f - bf_m$ is a DPP whose mth coefficient is 0. By continuing this process, we can find a DPP f' such that the mth coefficient of f' is 0 for every $m \in M$ and f can be constructed from f' by adding a number of $DAPs$. We call f' a *basic DPP.* Since every DPP is the sum of a basic DPP and a number of DAPs, we can generate every DPP by simply generating the basic DPPs.

7 Characterizing Base Field Polynomials

We will find a necessary and sufficient criterion for a function $f : F_{p^d} \to F_{p^d}$ to be represented by a polynomial with coefficients in the base field. We begin by counting the number of unique base field polynomials. Since every polynomial over F_{p^d} can be written as $f(x) = \sum_{n=0}^{p^d-1} a_n x^n$, where the set $\{a_n\}$ is uniquely defined, there are $p^{(p^d)}$ unique base field polynomials.

We will say that a function f has property (P) if $f(x^p) = f(x)^p \; \forall x \in F_{p^d}$. This property essentially means that the image of any element in a given conjugacy class is determined by the image of any other element of that conjugacy class. Thus if we choose a set of representatives for the conjugacy classes, the function f is determined by the images of our representatives.

If d is prime, there are $\frac{p^d-p}{d}$ conjugacy classes of degree d and p singleton conjugacy classes of degree 1. There are p^d choices for the image of the representative for each degree d conjugacy class and p choices for the image of each degree 1 conjugacy class. Let $a = \frac{p^d-p}{d}$, then there are $(p^d)^a p^p = p^{ad+p}$ functions with property (P). But $ad + p = d\frac{p^d-p}{d} + p = p^d$.

We see that there are the same number of base field polynomials as functions with property (P). We also know that every base field polynomial has property (P). It follows that every function with property (P) is represented by a base field polynomial. We state this as a theorem:

8 Theorem. *A function f is represented by a base field polynomial if and only if f has property (P).*

We can now use this result to calculate the number of PPs, DPPs and basic DPPs for a field F_{p^d}. For DPPs, we do the same calculation as we did to find functions with property (P), except that we only allow f to map degree d conjugacy classes to other degree d conjugacy classes. We thus find that there are $(p^d - p)^{\frac{p^d-p}{d}} p^p$ DPPs.

We saw already that there are $p^{\frac{p^d-p}{d}+p}$ DAPs over F_{p^d}. Thus for every $p^{\frac{p^d-p}{d}+p}$ DPPs, there is exactly one basic DPP. We divide the number of DPPs by the number of DAPs and we see that there are $(p^{d-1}-1)^{\frac{p^d-p}{d}}$ basic DPPs.

If f is a PP with property (P), then each conjugacy class must be sent to a distinct conjugacy class of the same degree. There are thus $(\frac{p^d-p}{d})!$ ways to distribute the degree-d conjugacy classes and $d^{\frac{p^d-p}{d}}$ ways to arrange them. For the degree 1 classes, there are $p!$ ways to distribute them. Thus there are $(\frac{p^d-p}{d})!d^{\frac{p^d-p}{d}}p!$ PPs.

These calculations are all done for prime d. It is left to the reader to generalize this to non-prime d. The theorem still holds in this case, but the counts for DPPs and PPs are messy.

8 Appendix

This section will introduce ways to explore our work computationally. We computed examples in many special cases which suggested the results presented above.

For an arbitrary polynomial, the task of determining whether or not it is a permutation polynomial is difficult. With degree preserving polynomials, the situation is easier. Recall that for each element α^k (where α is a primitive element of the field $\mathbf{F}_{p^d}$) the n-1 elements α^{k*p}, α^{k*p^2},..., $\alpha^{k*p^{d-1}}$ of $\mathbf{F}_{p^d}$ will be called the conjugates of α^k.

It is immediate that there are $(\frac{p^d-p}{d})$ conjugacy classes of elements of degree d in $\mathbf{F}_{p^d}$. Additionally, p classes are single-element subsets of $\mathbf{F}_p$.

3 Proposition. *Let $f \in \mathbf{F}_p[x]$. If f preserves the degree of $\beta \in \mathbf{F}_{p^d}$, then f preserves the degree of all the conjugates of β.*

Therefore, to check whether a polynomial preserves degree d or not, it is only necessary to check one member of each conjugacy class in $\mathbf{F}_{p^d}$, excluding the p in the base field.

For our computations, we used Maple V. We will now proceed through two algorithms for finding DPPs and DAPs.

The following code must be executed in Maple before the main algorithm is performed (values that must be entered manually will be enclosed in quotes (’ ’)):

```
readlib(GF):
G :=GF(’p’,’n’,’enter a monic irreducible polynomial of degree n’):
a:= G[ConvertIn](alpha);
G[isPrimitiveElement](’a+some number such that the output is true’);
```

q:=’the element input in above’;

T:={’the elements of the base field $\mathbf{F}_p$ separated by commas’};

Now create a list L of the representatives of the conjugacy classes:

L:=[’the representatives separated by commas’];

t:=’the size of L’

Now choose a degree d to check. Then we define a function f_d:

$fd := (x, a1, a2, ..., ad)- >$

$G[‘+‘](G[‘*‘](G[‘‘](x, 1), a1), G[‘*‘](G[‘‘](x, 2), a2), ..., G[‘*‘](G[‘‘](x, d), ad));$

Here is the algorithm which cycles through all polynomials of degree d and prints out which ones preserve degree and which ones do not:

```
for ad from 1 to 1 do
...
for a2 from 0 to 'p-1' do
for a1 from 0 to 'p-1' do
v:=true;
for n from 1 to t while v do
v:=not member(G[ConvertOut]($fd(G[‘‘](q, L[n]), a1, a2, ..., ad)), T$)
od;
‘if‘(v,print(a1,a2,...,ad,DPP),print(a1,a2,...,ad,no))
od ... od od; - (Note that “od” must appear as often as “do”)
```

The degree annihilating case is similar:

```
for bd from 1 to 1 do
...
for b2 from 0 to 'p-1' do
for b1 from 0 to 'p-1' do
v:=true;
for m from 1 to t while v do
v:=member (G[ConvertOut]($f(G[‘‘](q, L[m]), b1, b2, ..., bd)), T$)
od;
‘if‘(v,print(b1,b2,...,bd,DAP),print(b1,b2,...,bd,no))
od ... od od;
```

Using this algorithm we generated lists of DPP's in several special cases. In studying the patterns of distribution of DPP's among non-DPP's , we conjectured that there was a set of basic DPP's from which all others could be derived by adding DAP's.

References

[1] J.A. Gallian, Contemporary Abstract Algebra, *Houghton Mifflin Company* **Fourth Edition**(1998), 98.

[2] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* **95** (1988), 243-246.

[3] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, II, *American Math. Monthly* **100** (1993), 71-74.

[4] R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley, Reading, MA, 1983.