Rose-Hulman Undergraduate Mathematics Journal

Volume 4
Issue 1

Article 4

Classifying and Using Polynomials as Maps of the Field F_{p^d}s

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

Dylan Cutler

Jesse Johnson

Benjamin Rosenfield

Kudzai Zvoma

Middlebury College

January 30, 2003

1 Abstract

Every function from a finite field to itself can be represented by a polynomial. 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. 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 allows more opportunity to maneuver and gain intuition about the occurrence of such polynomials.

2 Introduction

Before starting discussion of these polynomials we give a brief summary of the main relevant ideas in finite fields. The following facts are used. Proofs are are found in [4].

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

  For example, $\mathbf{F}_5 = \{0,\ 1,\ 2,\ 3,\ 4\}$ with addition and multiplication mod 5.

- The set of all polynomials with coefficients in $\mathbf{F}_p$ forms a ring. We denote 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 factor 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, $\mathbf{F}_{5^2} = \mathbf{F}_{25} = \{0, 1, 2, 3, 4, \alpha, \alpha+1, \alpha+2, \alpha+3, \alpha+4, 2\alpha, 2\alpha+1, 2\alpha+2, 2\alpha+3, 2\alpha+4, 3\alpha, 3\alpha+1, 3\alpha+2, 3\alpha+3, 3\alpha+4, 4\alpha, 4\alpha+1, 4\alpha+2, 4\alpha+3, 4\alpha+4\}$.

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

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 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 not unique, 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 the multiplicative group of $\mathbf{F}_{p^d}$ is $p^d - 1$. For any nonzero element $\lambda \in \mathbf{F}_{p^d}$, $\lambda^{p^d} = \lambda$ and $\lambda^p = \lambda$ if and only if $\lambda \in \mathbf{F}_p$.*

Consequently we adopt the convention of expressing each polynomial in a form with degree less than p^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 $a_i \in \mathbf{F}_p[x]$.

3 Degree Preserving Polynomials and Degree Annihilating Polynomials

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.

If the mapping induced by a polynomial $\mathbf{f}$ upon $\mathbf{F}_{p^d}$ is one-to-one and onto, thus 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]. In our particular approach, we shifted focus from permutation polynomials exclusively to work on a related broader class of polynomials.

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

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

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 $\mathbf{F}_p[x]$.*

For the remainder of the paper we assume that p and d are prime. Thus 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 (private communication).

2 Definition. *A polynomial $f(x) \in \mathbf{F}_{p^d}$ preserves degree d over $\mathbf{F}_p$ if for all $\alpha \in \mathbf{F}_{p^d}$ 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 $\mathbf{F}_p$. 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 generalizations 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 $\alpha \cdot f(x)$, $f(\alpha \cdot x)$, $f(x) + \alpha$, and $f(x + \alpha)$, for any non-zero $\alpha \in \mathbf{F}_p$.*

Proof. If α is an element of the base field $\mathbf{F}_p$ and β has degree d over $\mathbf{F}_p$ then $\alpha + \beta$, $\alpha \cdot \beta$ cannot be elements of the base field, which is closed under addition and multiplication. Therefore $\alpha + \beta$, $\alpha \cdot \beta$ also have degree d. □

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 (private communication).

1 Lemma. *For any polynomial $f(x) \in \mathbf{F}_p[x]$, $[f(x)]^p = f(x^p)$.*

Proof. Consider $(x_1 + x_2)^p$. This is equal to $\sum_{k=0}^{p}(\binom{p}{k})x_1^k x_2^{p-k}$ where $(\binom{p}{k}) = \frac{p!}{k!(p-k)!}$. But for $k = 1...p-1$, $(\binom{p}{k})$ will be a multiple of p, and will vanish in $\mathbf{F}_p$. Only the first and last terms, x_1^p and x_2^p remain. Now in general, consider $(x_1 + x_2 + ... + x_n)^p$. We set $y = x_1 + ... + x_{n-1}$ and obtain $(y + x_n)^p$, which will give us $y^p + x_n^p$. □

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 $\beta^p, \beta^{(p^2)}, ..., \beta^{(p^d-1)}$. 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 $\mathbf{F}_p$ if and only if for any monic irreducible polynomial $g(x)$ of degree d over $\mathbf{F}_p$, $f(x^p) \not\equiv f(x)$ mod $g(x)$.*

Proof. i) First, suppose α is of degree d over $\mathbf{F}_p$ where $g(x)$ is its minimum polynomial and $f(x)$ preserves degree d. If $f(x^p) \equiv f(x)$ mod $g(x)$, then $f(x^p) - f(x) = p(x)g(x)$ for some polynomial $p(x)$. As $g(x)$ is α's minimum polynomial, $g(\alpha) = 0$. Thus we have $[f(\alpha)]^p - f(\alpha) = 0$. So $[f(\alpha)]^p = f(\alpha)$, therefore $f(\alpha) \in \mathbf{F}_p$. But then $f(x)$ does not preserve degree d. Thus $f(x^p) \not\equiv f(x)$ mod $g(x)$ for any monic irreducible polynomial $g(x)$.

ii) Now assume $f(x^p) \not\equiv f(x)$ mod $g(x)$ for any monic irreducible polynomial $g(x)$ of degree d. Let α be a root of $g(x)$ with degree d over $\mathbf{F}_p$. Then $f(x^p) - f(x) = p(x)g(x) + r(x)$ where $0 < deg\ r(x) < d$. Since $g(x)$ is α's minimum polynomial, $r(\alpha) \neq 0$. So we have $[f(\alpha)]^p - f(\alpha) \neq 0$. Thus $f(\alpha) \notin \mathbf{F}_p$. Therefore, $f(x)$ preserves degree d. □

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 if and only if $f(\alpha^{p^i})$, $0 < i < p-1$, has degree d for any conjugate α^{p^i} of α.*

Proof. This follows immediately from the previous proof as the conjugates of α are precisely the other roots of the minimum polynomial and the proof did not depend on the choice of root. □

Conjugates turn out to be very useful. For example in testing for DPP's: Corollary 6 tells us that if we test one representative from each set of conjugates we can tell if a polynomial is a DPP or not (see Appendix for algorithms). 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 for all $\alpha \in \mathbf{F}_{p^d}$, $f(\alpha) \in \mathbf{F}_p$.*

This class of polynomials turns out to be very useful in generating DPP's due to the fact that the addition of a DAP to a DPP generates another DPP. This follows from Theorem 3 as the value set of a DAP consists only of elements in the base field. It is important to note the following features of DAP's, namely the closures under addition (DAP + DAP = DAP) and scalar multiplication by an element of the base field (kDAP = DAP with $k \in \mathbf{F}_p$). Also, if $f(x)$ is a DAP and $g(x)$ is some polynomial over the base field, then $f(g(x))$ is a DAP, since $g(x)$ maps $\mathbf{F}_{p^d}$ into itself and $f(x)$ maps $\mathbf{F}_{p^d}$ into $\mathbf{F}_p$. Thus DAP's form a subspace of the vector space of all polynomials with coefficients in the base field. We will next find a basis for this subspace.

2 Lemma. *[4] Both the trace, $tr(x) = x + x^p + x^{(p^2)} + ... + x^{(p^{(d-1)})}$, and the norm, $n(x) = x^{((p^d-1)/(p-1))}$, are DAP's over $\mathbf{F}_{p^d}$.*

7 Theorem. *We can generate all of the DAP's for a given finite field by linear combinations of polynomials of the forms: (i) the composed trace $tr_i(x) = tr(x^i) = (x^i)+(x^i)^p+(x^i)^{(p^2)}+...+(x^i)^{(p^{(d-1)})}$ for all i not a multiple of $\frac{p^d-1}{p-1}$ and exponents reduced mod $p^d - 1$; (ii) the composed norm $n_k(x) = n(x^k) = x^{k(\frac{p^d-1}{p-1})}$ 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. We see that if the polynomials $tr(x^i)$ and $tr(x^j)$ have one term in common, then they have all terms in common. This is due to the fact that if $l \equiv k \bmod p^d - 1$, then $lp, lp^2, ..., l(p^d-1) \equiv kp, kp^2, ..., k(p^d-1) \bmod p^d - 1$. This gives us $\frac{p^d-p}{d}$ distinct polynomials of type (i); there are clearly p polynomials of type (ii). 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 subspace of DAP's over a given finite field. We know that we are in an p^d-dimensional vector space of polynomials with each vector being expressed as an ordered p^d-tuple of the coefficients of a polynomial. We also know that each set of conjugates gets mapped to a single set of conjugates. We see this by noting that the set $\{\alpha, \alpha^p, \alpha^{(p^2)}, ..., \alpha^{(p^{(d-1)})}\}$ of conjugates gets mapped to the set $\{f(\alpha), [f(\alpha)]^p, [f(\alpha)]^{(p^2)}, ..., [f(\alpha)]^{(p^{(d-1)})}\}$ of conjugates of $f(\alpha)$. However in $\mathbf{F}_p$ a set of conjugates contains just a single element. So the subspace of DAP's is in 1-1 correspondence with the family of functions from the set of conjugacy classes to $\mathbf{F}_p$.There are $\frac{p^d-p}{d}$ conjugacy classes of degree d elements, and p conjugacy classes of elements in $\mathbf{F}_p$. Therefore the dimension of the subspace is $\frac{p^d-p}{d}+p$. This dimension is exactly the number of linearly independent DAP's in our set generated by the composed trace and the composed norm. Therefore we have generated a basis for the sub space of DAP's with coefficients in $\mathbf{F}_p$ over the field $\mathbf{F}_p$. □

4 Representatives for Conjugacy Classes

Let α be a primitive element of the field $\mathbf{F}_{p^d}$. Two elements α^a, α^b of $\mathbf{F}_{p^d}$ will be conjugates if and only if $a \equiv b * p^m (\text{mod } p^n - 1)$ for some $m \in \mathbf{Z}_n$. We shall write a in base p. That is, we consider $a = \sum_{i=0}^{n-1} a_i p^i$ with $0 \leq a_i < p$. 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 cyclic permutation of the digits of a in base p. This proved to be very useful in our work in Maple. In this way we could easily produce all the sets of conjugates. This let us choose a representative for each set of conjugates that we could then use to test a polynomial.

5 Basic DPP's

Now that we can generate a list of all the DAP's for F_{p^d}, we would like to take advantage of this to generate DPP's. 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 our 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, because in both cases we are taking the highest integer after reduction mod$(p^d - 1)$. 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 DAP's. We call an f' with this property a *basic DPP*. Thus every DPP is the sum of a basic DPP and a number of DAP's, so we can generate every DPP by simply generating the basic DPP's.

6 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 $f(x^p) = f(x)^p$ for all $x \in F_{p^d}$. 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.

As we have seen, if d is prime, there are $\frac{p^d-p}{d}$ conjugacy classes of elements of degree d and p singleton conjugacy classes of elements of degree 1. There are p choices for image of each degree 1 conjugacy class, because under a well-defined mapping a single element can only have a single image. There are p^d choices for the image of the representative for each degree d 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 PP's, DPP's and basic DPP's for a field $\mathbf{F}_{p^d}$. For DPP's, 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 $(p^d - p)^{\frac{p^d-p}{d}} p^p$ DPP's.

We saw already that there are $p^{\frac{p^d-p}{d}+p}$ DAP's over $\mathbf{F}_{p^d}$. We also saw that there is a natural partition of the set of all DPP's into subsets. Each subset has one basic DPP, and every other DPP is the sum of that basic one and a DAP. Thus for every $p^{\frac{p^d-p}{d}+p}$ DPP's, there is exactly one basic DPP. We divide the number of DPP's by the number of DAP's and we see that there are $(p^{d-1} - 1)^{\frac{p^d-p}{d}}$ basic DPP's.

If f is a PP of $\mathbf{F}_{p^d}$ with property (P), then each conjugacy class must be sent to a distinct conjugacy class of elements of the same degree. (If f does not have property (P), then f has coefficients outside of $\mathbf{F}_p$ and might send a degree 1 element to another of degree d.) There are $(\frac{p^d-p}{d})!$ ways to assign conjugacy classes to conjugacy classes and for each such assignment there are d ways to choose the images of individual elements (because of property (P)). 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 $(\frac{p^d-p}{d})!d^{\frac{p^d-p}{d}}p!$ PP's with coefficients in F_p, out of the $p^d!$ PP's of F_{p^d}.

7 Conclusion

The subject of permutation polynomials continues to be an active area of research. We have participated in this by looking at the related degree-preserving polynomials which are in a sense a generalization of permutation polynomials. By using the vector space of degree-annihilating polynomials, we have developed a method for generating all the base field DPP's of $\mathbf{F}_{p^d}$ where d is prime. This has allowed us to count the permutation polynomials with coefficients in the base field.

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. 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 (see Corollary 6 above).

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 by the user for particular cases 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 of degree d elements:

```
L:=['the representatives separated by commas'];
t:='the number of elements of L'
```

Now choose a degree m to check. We define a generic polynomial function $f_{'m'}$:

```
fd := (x, a1, a2, ..., a('m − 1'))− >
G[‘ + ‘](G[‘ ∗ ‘](G[‘ ∧ ‘](x, 1), a1), G[‘ ∗ ‘](G[‘ ∧ ‘](x, 2), a2), ..., G[‘ ∧ ‘](x,' m'));
```

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

```
for a(m-1) from 0 to 'p-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, ..., a(m − 1), 1)), T)
od;
if(v,print(a1,a2,...,1,DPP),print(a1,a2,...,1,no))
od ... od od;
```

(Note that “od” must appear as often as “do” so that each loop is completed.)

The output is a list of ordered m-tuples, the entries in each corresponding to the coefficients of a polynomial, and each followed by "DPP" or "no" depending on whether that polynomial is a DPP or not.

The degree annihilating case is similar:

```
for b(m-1) from 0 to 'p-1' do
...
for b2 from 0 to 'p-1' do
for b1 from 0 to 'p-1' do
v:=true;
for n from 1 to t while v do
v:=member (G[ConvertOut](f(G[‘ ∧ ‘](q, L[n]), b1, b2, ..., b(m − 1), 1)), T)
```

```
od;
if(v,print(b1,b2,...,1,DAP),print(b1,b2,...,1,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.

For example, for $p = 3$ and $d = 2$, we found the following DPP's of degree up to 4 (because of Theorem 3, we can restrict our attention to monic polynomials with constant term 0):

x,

x^3, $2x + x^3$,

$x + x^4$, $2x + x^4$, $x^3 + x^4$, $2x + x^3 + x^4$, $2x^3 + x^4$, $x + 2x^3 + x^4$.

We also found the following DAP's of degree up to 4 (again, monic with constant term 0):

$x + x^3$,

x^4, $x + x^3 + x^4$, $2x + 2x^3 + x^4$.

Note that the first two DAP's are the trace and the norm, respectively, for $\mathbf{F}_9$, and that some of the DPP's listed clearly differ from others by DAP's. We now know, of course, that a basis for the vector space of DAP's is $\{1, x^4, x^8, x + x^3, x^2 + x^6, x^5 + x^7\}$, the set $M = \{0, 3, 4, 6, 7, 8\}$ (the degrees of the DAP's), and the basic DPP's are

$\{x, 2x, x^5, 2x^5, x + x^2 + x^5, 2x + 2x^2 + 2x^5, x + 2x^2 + x^5, 2x + x + x^5\}$.

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.