Permutations amongst the Dembowski-Ostrom Polynomials

Aart Blokhuis[1], Robert S. Coulter*[2], Marie Henderson[2], and Christine M. O'Keefe**[3]

[1] Technische Universiteit, Eindhoven, The Netherlands
[2] Centre for Discrete Mathematics and Computing, The University of Queensland, Brisbane, Australia
[3] Department of Pure Mathematics, The University of Adelaide, 5005 Australia

1 Dembowski-Ostrom Polynomials and Linearised Polynomials

Let p be a prime and $q = p^e$. Let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_q^*$ represent the set of non-zero elements of $\mathbb{F}_q$. The ring of polynomials in the indeterminate X with coefficients from $\mathbb{F}_q$ will be represented by $\mathbb{F}_q[X]$. A polynomial $f \in \mathbb{F}_q[X]$ which permutes $\mathbb{F}_q$ under evaluation is called a *permutation polynomial* of $\mathbb{F}_q$. Permutation polynomials have important applications in cryptography. This is because one of the basic requirements of a mapping used to encrypt a message is that it be invertible so that the original message can be recovered. In particular, Dembowski-Ostrom polynomials have been used for a cryptographic application in the public key cryptosystem HFE, see [7]. There the author states that "it seems difficult to choose f (a DO polynomial) such that it is a permutation". It is the purpose of this article to provide some examples of Dembowski-Ostrom permutations. We consider this problem in the purely theoretical spirit of problem P2 of [5]. We do not claim that any of the classes identified in this article could be used to provide a "secure" cryptosystem when implemented in HFE. The class of polynomials of primary interest in this article is now defined.

Definition 1. The polynomial $f \in \mathbb{F}_q[X]$ is called a *Dembowski-Ostrom polynomial* (DO polynomial) if f has the shape

$$f(X) = \sum_{i,j=0}^{n} a_{ij} X^{p^i+p^j}.$$

This class of polynomials was described by Dembowski and Ostrom in [4]. In that article, the authors considered projective planes of order n which admitted a collineation group of order n^2. They introduced the notion of a planar function as an aid for describing these planes. A polynomial $g \in \mathbb{F}_q[X]$

* Supported by an Australian Research Council grant
** Supported by the Australian Research Council and the University of Ghent

is called a *planar polynomial* if $g(X+a)-g(X)$ is a permutation polynomial for every $a \in \mathbb{F}_q^*$. It is a simple matter to show that a polynomial can not be planar on $\mathbb{F}_q$ when q is even. In contrast, a DO polynomial f can not be a permutation polynomial of $\mathbb{F}_q$ if q is odd as, in such cases, $f(x) = f(-x)$ for each $x \in \mathbb{F}_q^*$. For this reason, we can restrict to the case q even when searching for DO permutation polynomials.

A set of permutation polynomials is easily obtained from the following class of polynomials.

Definition 2. A *linearised polynomial* (or *additive polynomial*), $L \in \mathbb{F}_q[X]$, is a polynomial of the shape

$$L(X) = \sum_{i=0}^{n} a_i X^{p^i}.$$

It is easily seen from this definition that these polynomials are additive in the sense that $L(x+y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$. A permutation condition for this class of polynomials can be directly determined from this property: a linearised polynomial $L(X)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $x = 0$ is its only root in $\mathbb{F}_q$. Linearised polynomials have many other interesting properties and applications, see Chapter 3 of [6].

It is interesting to note that if q is even then it is possible for a DO polynomial to be a linearised polynomial, for example, take $f = L^2$ (consequently f permutes $\mathbb{F}_q$ if and only if L does). In fact, it is easy to show that a DO polynomial f is a linearised polynomial if and only if q is even and $f = L^2$, where L is a linearised polynomial.

The reduction of a linearised polynomial modulo $X^q - X$ is again a linearised polynomial. We shall call a polynomial *bilinear* if it can be written as the product of two reduced linearised polynomials. (Note that this is not the same definition of bilinear as used in some other articles, for example [1].) The stipulation that the linearised polynomials be reduced makes sense when we consider the following trivial lemma.

Lemma 3. *Let $B \in \mathbb{F}_q[X]$ satisfy $B(X) = L_1(X)L_2(X)$ where L_1 and L_2 are linearised polynomials. Set $L_i'(X) = L_i(X) \bmod (X^q - X)$ for $i = 1, 2$ and define $B' = L_1'L_2'$. Then $B(X) \bmod (X^q - X) = B'(X)$ unless $q = 2^e$ and degree(L_1') =degree(L_2') $= 2^{e-1}$, in which case $B(X) \bmod (X^q - X) = B'(X) + \beta(X^q - X)$ where β is the coefficient of X^q in $B'(X)$.*

Hence, except for one particular case, a bilinear polynomial is still a bilinear polynomial after reduction. This is also the case for DO polynomials with a similar exception: the reduction of a DO polynomial is again a DO polynomial unless there existed a term with degree divisible by q before reduction. This can only occur in characteristic 2 to a term of the shape X^{2p^i} where $i \bmod e = e - 1$.

Clearly every bilinear polynomial is a DO polynomial. However, for $e > 1$, a DO polynomial is not necessarily a bilinear polynomial. This can be seen

from a simple counting argument. In $\mathbb{F}_q[X]$, there are $(q^{e(e+1)/2}-1)/(q-1)$ reduced monic DO polynomials. There are $(q^e-1)/(q-1)$ monic linearised polynomials and therefore

$$\binom{(q^e-1)/(q-1)}{2} + (q^e-1)/(q-1)$$

monic bilinear polynomials. This is easily seen to be less than the number of DO polynomials for $e > 1$ and any q.

2 Permutation Behaviour of Dembowski-Ostrom Polynomials

Suppose that $f(X) = L_1(X)L_2(X)$ is a permutation polynomial of $\mathbb{F}_q$. We have $f(x) = 0$ for $x \in \mathbb{F}_q$ if and only if $x = 0$. Therefore, L_1 and L_2 must also be permutation polynomials of $\mathbb{F}_q$. As $L_1(X)$ permutes $\mathbb{F}_q$, there exists a linearised compositional inverse $L_1^{-1}(X)$ such that $L_1(L_1^{-1}(X)) \bmod (X^q - X) = X$. From this we have $f(L_1^{-1}(X)) \bmod (X^q - X) = XL(X)$ is also a DO permutation polynomial where $L(X) = L_2(L_1^{-1}(X)) \bmod (X^q - X)$ is a linearised permutation polynomial. Hence, for bilinear DO polynomials, we have only to consider the permutation behaviour of DO polynomials with the shape $XL(X)$ where $L(X)$ is a linearised permutation polynomial. All other bilinear DO permutation polynomials can be obtained by composing with linearised permutation polynomials. We now present several classes of permutation polynomials obtained from bilinear DO polynomials. The examples described by the following two theorems were first found using MAGMA [2]. They describe all bilinear DO permutation polynomials over $\mathbb{F}_q$ with $q = 2^e$, $e \leq 6$ known to the authors.

Theorem 4. *Let $q = 2^e$ and g be any primitive element of $\mathbb{F}_q$. Let k be any integer and set $d = (k, e)$. Suppose $f \in \mathbb{F}_q[X]$ is a DO polynomial satisfying $f(X) = XL(X)$ for some linearised polynomial L. Then f permutes $\mathbb{F}_q$ when any of the following conditions are satisfied.*

(i) $L(X) = X^{2^k}$ *where e/d is odd.*

(ii) $L(X) = X^{2^k} + aX^{2^{e-k}}$ *where e/d is odd and $a \neq g^{t(2^d-1)}$ for any integer t.*

(iii) $L(X) = X^{2^{2k}} + a^{2^k+1}X^{2^k} + aX$ *where $e = 3k$ and $a \neq g^{t(2^k-1)}$ for any integer t.*

Proof. (i) Immediate since $(2^k + 1, q - 1) = 1$ if and only if e/d is odd, see [3, Lemma 2.1].

(ii) Suppose $a \in \mathbb{F}_q$ satisfies $a \neq g^{t(2^d-1)}$ for any integer t. Then $X^{2^k} + aX$ is a permutation polynomial. If e/d is odd then by (i), $X^{2^{e-k}+1}$ also permutes $\mathbb{F}_q$. Composing, and reducing mod $(X^q - X)$, we obtain $X(X^{2^k} + aX^{2^{e-k}})$, which must also permute $\mathbb{F}_q$.

(iii) As $a \neq g^{t(2^k-1)}$ for any integer t, the polynomials $X^{2^{2k}} + a^{2^k}X$ and $X^{2^k} + a^{2^k}X$ permute $\mathbb{F}_q$. Now

$$f(X^{2^{2k}} + a^{2^k}X) \equiv (1 + a^{2^{2k}+2^k+1})\big((X^{2^k} + a^{2^k}X) \circ X^{2^k+1}\big) \bmod X^q - X.$$

As X^{2^k+1} also permutes $\mathbb{F}_q$ it follows that $f(X)$ permutes $\mathbb{F}_q$.

We note that all of the DO permutation polynomials given above are constructed by composition from well known classes of permutation polynomials (monomials and linearised binomials). For our next result we set $T = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q$, the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

Theorem 5. *Let q be even and n be odd. The polynomial*

$$f(X) = X\left(T(X) + aX\right)$$

is a permutation polynomial over $\mathbb{F}_{q^n}$ for all $a \in \mathbb{F}_q \setminus \{0, 1\}$.

Proof. Note

$$\begin{aligned} T\left(f(x)\right) &= T\left(xT(x) + ax^2\right) \\ &= T(x)T(x) + aT(x)^2 \\ &= (1+a)T(x)^2 \end{aligned}$$

for all $x \in \mathbb{F}_{q^n}$. Suppose there exists elements $x, y \in \mathbb{F}_{q^n}$ such that $f(x) = f(y)$. Then $x\left(T(x) + ax\right) = y\left(T(y) + ay\right)$. Applying the trace function T gives

$$(1+a)\left(T(x)^2 + T(y)^2\right) = 0,$$

so $T(x) = T(y) = t$, say. Thus $tx + ax^2 = ty + ay^2$ from which $t = a(x+y)$, implying $x + y \in \mathbb{F}_q$. Therefore $T(x+y) = n(x+y) = 0$. So $x = y$.

Without reduction, it is clear that all of the permutation polynomials given in Theorems 4 and 5 cannot have a linearised decompositional factor since their degrees are never divisible by the characteristic. If we take into consideration the possibility that any of this class could be the reduced form modulo $X^{q^n} - X$ of some other polynomial, then as with all classes of permutation polynomials, it is quite possible that some examples of functionally equivalent polynomials will have linearised decompositional factors. However, it should be stressed that this will not, in general, be the case. To see this, let f be any permutation polynomial over $\mathbb{F}_q$. Then all polynomials of the form $F(X) = f(X) + h(X)(X^q - X)$, where h is any polynomial defined over $\mathbb{F}_q$, are equivalent to f under evaluation and permutations also. However, for every choice of h which provides an F which has a linearised decompositional factor, there are many which will not. In a cryptographic sense, it may be preferable that the permutations (as functions) can not easily be expressed as the composition of monomials and linearised polynomials. In this context, there

is a striking difference between the permutations of Theorem 4 and 5. While those permutations presented in Theorem 4 are easily shown to be equivalent under reduction to a simple composition of monomial and linearised binomial permutations (see the proof), the permutations presented in Theorem 5 have no such simple representation. Take the simplest case of Theorem 5: that is $n = 3$. Let $f_a(X) = X^{4^k+1} + X^{2^k+1} + aX^2$ with $a \in \mathbb{F}_{2^k} \setminus \{0, 1\}$. Then f_a is a permutation over $\mathbb{F}_q$ with $q = 8^k$. Let $L_1(X) = aX^{p^i} + bX$, $L_2(X) = cX^{p^j} + dX$ and s be an integer satisfying $(s, q-1) = 1$. Supposing f_a is functionally equivalent to a composition of L_1, L_2 and X^s (in any combination) always leads to a contradiction. While this does not constitute a rigorous proof, it seems safe to assert that, in general, the permutations given in Theorem 5 cannot be expressed as simple compositions of monomials and linearised binomials. Whether any of these permutations are of cryptographic relevance is another matter.

References

1. H.W. Bao, *On two exponential sums and their applications*, Finite Fields Appl. **3** (1997), 115–130.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
3. R.S. Coulter, *On the evaluation of a class of Weil sums in characteristic 2*, New Zealand J. Math. **28** (1999), 171–184.
4. P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.
5. 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.
6. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
7. J. Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, 1996, pp. 33–48.