A note on constructing permutation polynomials

Robert Coulter [a,*] Marie Henderson [b,1] Rex Matthews [c]

[a] *Department of Mathematical Sciences, 520 Ewing Hall, University of Delaware, Newark, Delaware, 19716, U.S.A.*
email: coulter@math.udel.edu

[b] *State Services Commission, Wellington, New Zealand*

[c] *6 Earl St., Sandy Bay, Tasmania 7005, Australia*

Abstract

Let H be a subgroup of the multiplicative group of a finite field. In this note we give a method for constructing permutation polynomials over the field using a bijective map from H to a coset of H. A similar, but inequivalent, method for lifting permutation behaviour of a polynomial to an extension field is also given.

Key words: permutation polynomial, finite field, subfield.

Throughout $\mathbb{F}_q$ denotes the finite field of characteristic p with q elements ($q = p^e$, $e \in \mathbb{N}$), and $\mathbb{F}_q^*$ the non-zero elements of $\mathbb{F}_q$. Let $\mathbb{F}_q[X]$ be the ring of polynomials over $\mathbb{F}_q$ in the indeterminate X. A *permutation polynomial* is a polynomial which, under evaluation, permutes the elements of $\mathbb{F}_q$. For example, a *linearised polynomial* $L \in \mathbb{F}_q[X]$ has the shape

$$L(X) = \sum_{i=0}^{k} a_i X^{p^i},$$

and permutes $\mathbb{F}_q$ if and only if the only root of $L(X)$ in $\mathbb{F}_q$ is $x = 0$. This class of polynomials will be useful later in this note. For further properties of linearised polynomials see [3].

Determining new classes of permutation polynomials is an open problem, see [4]. The following theorem describes a method for constructing permutation

* Corresponding author

[1] This author was supported by a RMIT VRII grant while employed by RMIT University in 2002 and 2003.

polynomials.

Theorem 1 *Let g be a primitive element of $\mathbb{F}_q$ and $H = \langle g^n \rangle$ where $nd = q-1$. Let $T \in \mathbb{F}_q[X]$ be any polynomial which maps $\mathbb{F}_q$ into $H \cup \{0\}$ satisfying $T(\lambda x) = \lambda T(x)$ for all $\lambda \in H$ and $x \in \mathbb{F}_q$. For any polynomial $h \in \mathbb{F}_q[X]$ and any positive integer s, define $f(X) = X^s h(X)$ and $F(X) = X^s h(T(X))$. If F is a permutation polynomial over $\mathbb{F}_q$ and T does not induce the zero map on $\mathbb{F}_q$, then f is one to one on H. Conversely, if f maps H onto Ha for some $a \in \mathbb{F}_q^*$, $(s,n) = 1$ and either*

(i) $T(x) = 0$ implies $x = 0$, or
(ii) $(s,d) = 1$ and $h(0) \in Ha$,

then F is a permutation polynomial over $\mathbb{F}_q$.

PROOF. Let F be a permutation polynomial over $\mathbb{F}_q$ and suppose there exists an $x \in \mathbb{F}_q$ such that $T(x) = \alpha \neq 0$. Then

$$\begin{aligned} o(H) &= \#\{(\lambda x)^s h(T(\lambda x)) \ : \ \lambda \in H\} \\ &= \#\{\lambda^s h(\lambda T(x)) \ : \ \lambda \in H\} \\ &= \#\{\lambda^s h(\lambda \alpha) \ : \ \lambda \in H\} \\ &= \#\{(\lambda \alpha)^s h(\lambda \alpha) \ : \ \lambda \in H\} \\ &= \#\{y^s h(y) \ : \ y \in H\}. \end{aligned}$$

It follows f is one to one on H.

Now suppose f maps H onto a coset Ha with $a \neq 0$, $(s,n) = 1$ and either condition (i) or (ii) holds. For any $\lambda, \mu \in H$ we must have $h(\lambda)/h(\mu) \in H$. Further, either condition (i) or (ii) implies $h(T(x)) \neq 0$ for all $x \in \mathbb{F}_q^*$. Let $x, y \in \mathbb{F}_q$ satisfy $F(x) = F(y)$. If $x = 0$, then $y^s h(T(y)) = 0$, implying $y = 0$. Now suppose $x \neq 0$, in which case $y \neq 0$ also. We have

$$\frac{x^s}{y^s} = \frac{h(T(y))}{h(T(x))} \tag{1}$$

and so $(x/y)^s \in H$. As $(s,n) = 1$, there exists integers i, j such that $is + jn = 1$. It follows that $x/y \in H$. Therefore $T(x) = (x/y)T(y)$, implying $T(x)^s = (x/y)^s T(y)^s$. We claim $T(x) = T(y)$. Clearly $T(x) = 0$ if and only if $T(y) = 0$. If $T(x)T(y) \neq 0$, then since $F(x) = F(y)$ we have

$$\frac{x^s}{y^s} h(T(x)) = h(T(y))$$

and multiplying by $T(y)^s$ gives

$$T(x)^s h(T(x)) = T(y)^s h(T(y)).$$

Since f is one to one on H, it follows that $T(x) = T(y) = \mu$ for some $\mu \in H \cup \{0\}$. Thus $F(x) = F(y)$ implies $x^s = y^s$. If condition (i) holds, then $\mu \neq 0$ and since $x/y = T(x)/T(y)$, we have $x = y$. Otherwise, condition (ii) holds and so $(s, d) = 1$, implying $(s, q-1) = 1$. Hence $x^s = y^s$ implies $x = y$. In either case, we have F is a permutation polynomial over $\mathbb{F}_q$.

We say a polynomial T satisfies the criteria of Theorem 1 when (i) T maps $\mathbb{F}_q$ into $H \cup \{0\}$, and (ii) $T(hx) = hT(x)$ for all $h \in H$ and $x \in \mathbb{F}_q$. The polynomials T satisfying the criteria of the theorem will be described by the authors in a more general context elsewhere.

We next make some comments regarding the scope and limitations of Theorem 1. Clearly, by multiplying through by a^{-1}, the restriction on the behaviour of f would simply be that it is bijective on H, but we prefer to state the theorem as given here.

If $o(H) = q-1$, then the only polynomials T satisfying the criteria of Theorem 1 are equivalent to cX for some $c \in \mathbb{F}_q^*$. Hence $F(X) = c^{-s}f(cX)$ and clearly the permutation behaviour of $f(X)$ and $F(X)$ are equivalent in this case. If $o(H) = 1$, then $(s, q-1) = 1$ and so X^s permutes $\mathbb{F}_q$. In this case, X^{q-1} is the only reduced polynomial which satisfies (i) and the criteria of Theorem 1. We then have $F(X) \equiv X^s \bmod (X^q - X)$. For (ii) to be satisfied we need $h(0) = h(1)$, and then $F(X) \equiv h(1)X^s \bmod (X^q - X)$.

Now set $o(H) = d$ and let $nd = q-1$. If $n \equiv 1 \bmod d$, then $T(X) = X^n$ satisfies the criteria of Theorem 1. In such cases, it can be seen that Theorem 1 with $T(X) = X^n$ describes precisely a subset of the Wan-Lidl permutations, [5], of the form $X^s h(X^n)$ with n a divisor of $q-1$. The permutation condition of $X^s h(X^n)$ simplifies to (i) $X^s h(X)$ maps H onto a coset Ha, and (ii) $(r, n) = 1$ (compare with the more general conditions given in [5, Theorem 1.2]). If $n \not\equiv 1 \bmod d$, then there appears to be no overlap between the Wan-Lidl permutations and permutations generated by Theorem 1.

In practice, it is very simple to use Theorem 1 to generate permutation polynomials not of the form of Wan-Lidl. For example, consider the finite field $\mathbb{F}_q$ with $q = 16$ and primitive element z and let $H = \langle z^3 \rangle$. Then there are 315 suitable reduced polynomials f and 125 distinct choices for polynomial T which satisfy condition (i). They combine to produce 501 distinct reduced monic permutation polynomials (including X, of course). A specific example is $f(X) = Xh(X)$ with $h(X) = X^3 + z^{11}X^2 + z^7X + z^3$. Setting $T(X) = X^{11} + zX^6 + z^{12}X$, the resulting permutation polynomial $F(X) = Xh(T(X))$ is a degree 34 polynomial, clearly not of the form $X^sM(X^d)$ and its reduced form has degree $q - 2 = 14$ (as almost all examples do) and has 10 terms.

Before leaving our discussion of Wan-Lidl permutation polynomials, we also

Finite Fields Appl. 15 (2009), 553-557

note the following implication of Theorem 1.

Lemma 2 *Let $H = \langle g^n \rangle$ with $dn = q-1$ and $d > 1$. Let $1 < k < q-1$ be any integer satisfying $(k, d) = 1$ and $T \in \mathbb{F}_q[X]$ satisfy the criteria of Theorem 1 with $x = 0$ the only root of T in $\mathbb{F}_q$. Then $X^s T(X)^{k-s}$ is a permutation polynomial over $\mathbb{F}_q$ whenever $0 < s < k$ and $(s, n) = 1$. Set*

$$S = \{X^s T(X)^{k-s} \bmod (X^q - X) \mid 0 < s < k \wedge (s, n) = 1\}.$$

Then $|S| \geq Min(\phi(n), \varphi(k, n))$ where $\phi(n)$ is the Euler ϕ-function of n and $\varphi(k, m)$ is the number of positive integers less than k and relatively prime to n.

PROOF. Since $(k, d) = 1$, X^k is bijective on H. It follows from Theorem 1 that $X^s T(X)^{k-s}$ is a permutation polynomial over $\mathbb{F}_q$ whenever $0 < s < k$ satisfies $(s, n) = 1$. It remains to count the number of distinct functions. Suppose

$$X^s T(X)^{k-s} \equiv X^{s-t} T(X)^{k-s+t} \bmod (X^q - X).$$

Then it follows that $x^t = T(x)^t$ for all $x \in \mathbb{F}_q$. In particular, we must have $x^t \in H$ for all $x \in \mathbb{F}_q^*$, implying n divides t. The result follows.

Theorem 1 is described in terms of a finite field $\mathbb{F}_q$ and a subgroup H of the multiplicative group of $\mathbb{F}_q$. For the remainder of this note we consider specifically the case where we have a finite field $\mathbb{F}_{q^m}$ and H is the multiplicative group of $\mathbb{F}_q$, so that $H \cup \{0\}$ forms a subfield of $\mathbb{F}_{q^m}$. In this case, Theorem 1 can be used as a lifting criteria: given a permutation f of $\mathbb{F}_q$ and a polynomial T satisfying the criteria of Theorem 1, one can construct a permutation polynomial F over $\mathbb{F}_{q^m}$ if the conditions of the theorem are met.

Some well known polynomials can be used for T in this case. Let k and m be integers with $k|m$. Define the polynomial

$$\mathrm{Tr}_{m,k}(X) = X + X^{q^k} + \cdots + X^{q^{m-k}}$$

(this is a polynomial which induces the trace mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^k}$). Then $\mathrm{Tr}_{m,k}(\alpha x) = \alpha \mathrm{Tr}_{m,k}(x)$ and $\mathrm{Tr}_{m,k}(x) \in \mathbb{F}_{q^k}$ for all $\alpha \in \mathbb{F}_{q^k}$ and $x \in \mathbb{F}_{q^m}$. So $\mathrm{Tr}_{m,k}$ satisfies the criteria for the polynomial T in Theorem 1 (where H is the multiplicative group of $\mathbb{F}_{q^k}$). We recall that for any k dividing m, $\mathrm{Tr}_{m,1}(x) = \mathrm{Tr}_{k,1}(\mathrm{Tr}_{m,k}(x))$ for all $x \in \mathbb{F}_{q^m}$.

Let $f \in \mathbb{F}_q[X]$ be any permutation polynomial satisfying $f(X) = X^s h(X)$ with $(s, q^m - 1) = 1$ and $h(0) \neq 0$. These conditions could be met by any linearised permutation polynomial, for example, with $s = p^i$ where i is the smallest integer for which $a_i \neq 0$. Define $F_k(X) = X^s h(\mathrm{Tr}_{k,1}(X))$ for any positive integer k dividing m. By Theorem 1, $F_k(X)$ permutes $\mathbb{F}_{q^k}$. In particular, $F_m(X)$ permutes $\mathbb{F}_{q^m}$ and since $F_m \in \mathbb{F}_q[X]$, it must also permute each subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$. In fact, for any $x \in \mathbb{F}_{q^k}$, if p divides m/k, then $F_m(x) = x^s h(0)$; otherwise $F_m(x) = (m/k)^{-s} F_k((m/k)x)$.

The following theorem is similar in theme to Theorem 1, but neither theorem follows fully from the other.

Theorem 3 *Let $f(X) = Xh(X)$ where $h \in \mathbb{F}_q[X]$. Define the polynomial $F \in \mathbb{F}_q[X]$ by $F(X) = L(X) + Xh(Tr_{m,1}(X))$ where $L \in \mathbb{F}_q[X]$ is a linearised polynomial. Then F is a permutation polynomial over $\mathbb{F}_{q^m}$ if and only if the following conditions hold:*

(i) $L(X) + f(X)$ is a permutation polynomial over $\mathbb{F}_q$.

(ii) For any $y \in \mathbb{F}_q$, $x \in \mathbb{F}_{q^m}$ satisfies $L(x) + xh(y) = 0$ and $Tr_{m,1}(x) = 0$ if and only if $x = 0$.

PROOF. For all $x \in \mathbb{F}_{q^m}$, we have $\mathrm{Tr}_{m,1}(F(x)) = L(\mathrm{Tr}_{m,1}(x)) + f(\mathrm{Tr}_{m,1}(x))$ as $\mathrm{Tr}_{m,1}(ax) = a\mathrm{Tr}_{m,1}(x)$ for all $a \in \mathbb{F}_q$. Suppose F is a permutation polynomial over $\mathbb{F}_{q^m}$. Then the cardinality of the set $\{\mathrm{Tr}_{m,1}(F(x)) \,|\, x \in \mathbb{F}_{q^m}\}$ is q. The cardinality of this set and $\{L(y)+f(y) \,|\, y \in \mathbb{F}_q\}$ are equal and so it follows that $L(X)+f(X)$ is a permutation polynomial over $\mathbb{F}_q$. To show that condition (ii) holds take two distinct elements $x, y \in \mathbb{F}_{q^m}$ satisfying $\mathrm{Tr}_{m,1}(x) = \mathrm{Tr}_{m,1}(y) = t$. Then $\mathrm{Tr}_{m,1}(x - y) = 0$ and

$$F(x) - F(y) = L(x - y) + (x - y)h(t).$$

As F is a permutation polynomial, $F(x) - F(y)$ is non-zero for distinct $x, y \in \mathbb{F}_{q^m}$ and condition (ii) follows.

Now assume (i) and (ii) hold. Suppose there exist $x, y \in \mathbb{F}_{q^m}$ such that $F(x) = F(y)$. As $L(X) + f(X)$ is a permutation polynomial $\mathbb{F}_q$, then $\mathrm{Tr}_{m,1}(x) = \mathrm{Tr}_{m,1}(y) = t$ for some $t \in \mathbb{F}_q$. Thus $\mathrm{Tr}_{n,1}(x-y) = 0$. Also $F(x) = L(x)+xh(t)$ and $F(y) = L(y) + yh(t)$ so that $L(x - y) + (x - y)h(t) = 0$. From condition (ii), $x = y$ and F is a permutation polynomial over $\mathbb{F}_{q^m}$.

As an application of this theorem, we have the following corollary which formed the motivation for this note.

Corollary 4 ([1, Theorem 5]) *Let q be even, m be odd. The polynomial*

$$F(X) = X\Big(Tr_{m,1}(X) + aX\Big)$$

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

PROOF. For any $a \in \mathbb{F}_q \setminus \{0,1\}$, the conditions of Theorem 3 are met by the polynomials $L(X) = aX^2$ and $h(X) = X$.

The proof of the corollary given in [1] is also particularly straightforward. We note that Corollary 4 was established earlier by W.M. Kantor in [2].

References

[1] A. Blokhuis, R.S. Coulter, M. Henderson, and C.M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite Fields and Applications: proceedings of the Fifth International Conference on Finite Fields and Applications (D. Jungnickel and H. Niederreiter, eds.), 2001, pp. 37–42.

[2] W.M. Kantor, *Spreads, translation planes and Kerdock sets I and II*, Siam J. Alg. Disc. Math. **3** (1982), 151–165 and 308–318.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[4] G.L. Mullen, *Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results*, Finite Fields Appl. **1** (1995), 242–258.

[5] D. Wan and R. Lidl, *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure*, Mh. Math **112** (1991), 149–163.