Groups of Permutation Polynomials over Finite Fields

Richard M. Stafford

Center for Communications Research, 4320 Westerra Court, San Diego, California 92121
E-mail: rmstaff@ccrwest.org

Communicated by Rudolf Lidl

Received November 3, 1997; revised May 27, 1998

Let $F$ be a finite field. We apply a result of Thierry Berger (1996, Designs Codes Cryptography, 7, 215–221) to determine the structure of all groups of permutations on $F$ generated by the permutations induced by the linear polynomials and any power map which induces a permutation on $F$. This generalizes a result of Leonard Carlitz (1953, Proc. Amer. Math. Soc., 4, 538).

1. INTRODUCTION

Let $p$ be a prime and let $F$ be the finite field $F = GF(q)$ where $q = p^n$. We consider certain permutations on $F$. To start with, there are the permutations induced by the linear polynomials $\tau_{a,b} : x \mapsto ax + b$ for all $a \in F^*$ and $b \in F$. In addition, there are the power maps $\pi_k : x \mapsto x^k$ where $1 \leq k \leq q - 2$ and $k$ is prime to $q - 1$. Notice that $\tau_{a,b} \tau_{c,d} = \tau_{ac,bc+d}$ and thus $AGL(1,F) = \{\tau_{a,b} | a \in F^*, b \in F\}$ is closed under composition and hence is a subgroup of the symmetric group $Sym(F)$. We reserve the symbol $AGL(1,F)$ to denote this group. Also notice that $AGL(1,F)$ is a semidirect product of the translation group, $T = \langle \tau_{1,b} | b \in F \rangle$, and the $F$-linear maps, $S = \langle \tau_{a,0} | a \in F^* \rangle$. Next, consider the permutation induced by the Frobenius map $\sigma : x \mapsto x^p$. A calculation shows that $\sigma^{-1} \tau_{a,b} \sigma = \tau_{a^p,b^p}$, and hence $\sigma$ normalizes $AGL(1,F)$. The subgroup of $Sym(F)$ generated by the linear polynomials and the Frobenius map is the semidirect product of $T$ and the semilinear mappings on $F$ and is denoted $AGL(1,F)$.

In [2] Carlitz proved for any finite field $F$, with cardinality greater than 2, that the whole symmetric group $Sym(F)$ is generated by the power map $x \mapsto x^{q-2}$ and the linear polynomials over $F$. Notice that this map takes
a non-zero field element to its inverse and hence is an involution. In this paper we generalize this result to all power maps. Specifically our result is:

**Theorem 1.** Let $F$ be the finite field $F = GF(q)$ where $q = p^n > 2$ and let $1 < k < q - 2$ be an integer relatively prime to $q - 1$. Define $G_k$ to be the subgroup of $\text{Sym}(F)$ generated by the permutations induced by the linear polynomials and the power map $\pi_k$, that is, $G_k = \langle \tau_{a,b}, \pi_k | a \in F^*, b \in F \rangle$. Then:

(i) If $k = p^t$ and $d = \gcd(n, t)$, then $G_k$ is the semidirect product of $\text{AGL}(1, F)$ and the subgroup of order $\frac{q}{d}$ generated by the semilinear map $\pi_{p^d}$.

(ii) If $p$ is odd and $k$ is not a power of $p$, then $G_k$ is the full symmetric group, $\text{Sym}(F)$.

(iii) If $p = 2$ and $k$ is not a power of 2, then $G_k \geq \text{Alt}(F)$. Moreover, $G_k = \text{Sym}(F)$ if and only if $\pi_k$ is an odd permutation.

The above theorem specializes to Carlitz's result when $k = q - 2$. This is immediate when $p$ is odd. We are left with the case $q = 2^n, n \geq 2$. In this case, the fixed points of $\pi_{q-2}$ are 0 and 1 and since $\pi_{q-2}$ is an involution, $\pi_{q-2}$ is a product of $\frac{1}{2} (q - 2) = 2^{n-1} - 1$ transpositions. Thus in this case $\pi_{q-2}$ is an odd permutation and so $G_{q-2} = \text{Sym}(F)$ by (iii) of the theorem above.

In 1953 Leonard Carlitz published a one-page elementary proof of his result. Our determination of $G_k$ is also quick but certainly is not elementary as it requires the main result of [1] which in turn relies on the classification of the finite simple groups. A proof of our result is given in the next section. Finally we mention that our notation is standard and will follow [4] or [6].

2. THE PROOF OF THEOREM 1

We have need of a slightly stronger version of Theorem 1 of [1]. Namely

**Theorem 2.** Let $G$ be a permutation group on the field $F = GF(p^n)$. If $G$ contains the affine group $\text{AGL}(1, p^n)$ in its standard action then either $G$ is a subgroup of $\text{AGL}(n, p)$, or

(i) if $p$ is odd, $G = \text{Sym}(F)$.

(ii) if $p = 2$, $G = \text{Sym}(F)$ or $G = \text{Alt}(F)$.

**Proof.** The case when $n \geq 2$ is the main result of [1]. When $n = 1$ the result is equivalent to proving that $\text{AGL}(1, p)$ is a maximal subgroup of $G$. But this is Proposition 7 of [3].

**Lemma 3.** The permutation $\pi_k$ normalizes $T$ if and only if $k = p^t$ for some integer $t$.

**Proof.** Suppose that $\pi_k \in N_{\text{Sym}(F)}(T)$. Then for all $a \in F$ there exists $c \in F$ such that $\pi_k^{-1} \tau_{1,a} \pi_k = \tau_{t,c}$. Calculating the image of 0 under $\tau_{t,c}$ we have $c = 0^{t,c} = 0^{\pi_k^{-1}(\tau_{t,c}) \pi_k} = a^k$. Thus $\pi_k^{-1} (\tau_{1,a}) \pi_k = \tau_{1,a^k}$. Calculating the image of
1 in this way we deduce that \(1 + a^k = (1 + a)^k \mod p\) and conclude for \(1 \leq j \leq k - 1\), that \(\binom{k}{j} \equiv 0 \mod p\). It is immediate from [5, p. 55, Lemma 5.1] that \(k\) is a power of \(p\). Conversely, if \(k\) is a power of \(p\) then \(\pi_k\) is a semilinear map and in particular normalizes \(T\).

**Proof of Theorem 1.** Let \(G_k\) be as in the hypothesis, and assume (i), so that \(k\) is a power of \(p\). Then, by Lemma 3, \(\pi_k\) normalizes \(T\) and hence is an element of \(\operatorname{AGL}(1, F)\). Thus our conclusion follows from the fact that \(\operatorname{AGL}(1, F)\) is a semidirect product of \(\operatorname{AGL}(1, F)\) and the subgroup \(\langle \pi_p \rangle\), and the fact that \(\langle \pi_p \rangle\) is a cyclic subgroup of \(\langle \pi_p \rangle\) of order \(\frac{n}{d}\), where \(d = \gcd(n, i)\).

In the remaining cases, when \(k\) is not a power of the prime \(p\), we claim that \(G_k \not\subseteq \operatorname{AGL}(n, p)\). If so, then by Theorem 2, \(T \lhd G_k\) which contradicts Lemma 3. Now assume (ii). Then \(p\) is odd and so the result follows from case (i) of Theorem 2.

We are left with (iii), that is, \(p = 2\). Because \(T\) is regular, and any non-identity element of \(T\) has order 2, we see that it is the product of \(2^n - 1\) transpositions. This is an even integer, since \(n \geq 2\), and so every element of \(T\) is an even permutation. Now since \(S\) is a cyclic group of odd order every element in \(S\) is also an even permutation. We have established that every element of \(\operatorname{AGL}(1, F)\) is an even permutation. Hence, \(G_k = \operatorname{Sym}(F)\) if and only if \(\pi_k\) is an odd permutation.

**ACKNOWLEDGMENTS**

The author thanks the anonymous referees for their helpful comments and in particular for pointing out Theorem 2.

**REFERENCES**