ABSTRACT

An attempt is made to classify permutation binomials of the type $ax^k + bx^j$, $ab \neq 0$, $i \leqslant j < k$. In particular when $a = 1$ and $j = 1$, the binomials $x^k + bx$, $b \neq 0$ are studied. When $\gcd (k-1, q-1) = 1$, $f(x) = x^k + bx$, $b \neq 0$ does not permute F_q , and when $\gcd (k-1, q-1) = k-1$, $x^k + bx$ can be written in the form $x^{\frac{q+n-1}{n}} + bx$ for some integer $n | q-1$. There are necessary and sufficient conditions for these polynomials to permute F_q. But the case when $\gcd (k-1, q-1) \neq 1, k-1$, remains unresolved. Such polynomials sometimes permute F_q and sometimes not, and a criterion for such polynomials to be permutation polynomials has not been obtained. Necessary and sufficient conditions for binomials of the form $x^k \left(bx + ax^{\frac{q+n-1}{n}} \right)$, $ab \neq 0$, $n | q-1$ to permute F_q are obtained. Permutation binomials of degrees 7 and 9 are studied. The possible finite fields of prime power order permuted by binomials of degrees 7 and 9 are identified.

It is proved that the union of permutation binomials H_q of G_q and K_q where $G_q = \{ax + bx^{\frac{q+1}{2}} \mid a, b \in F_q, \psi(a^2 - b^2) = 1\}$ and $K_q = \{cx^{q-2} + dx^{(q-3)/2} \mid c, d \in F_q, \psi(c^2 - d^2) = 1\}$ is a group, and that G_q is normal in H_q. The structure of H_q is studied. Given a permutation binomial $ax + bx^{\frac{q+1}{2}}$, $a, b \in F_q$, the permutation binomial $x^k\left(ax + bx^{\frac{q+1}{2}}\right)$ can be expressed in the form $f(x^\ell)$ such that $(\ell, q-1) = 1$, $f(x) \in G_q$. Conversely, every permutation polynomial $f(x^\ell)$ where $f(x) \in G_q$, gcd $(\ell, q-1) = 1$, can be written in the form $x^k\left(ax + bx^{\frac{q+1}{2}}\right)$, k an integer. The class of permutation binomials of the form $x^k\left(ax + bx^{\frac{q+1}{2}}\right)$ form a group U_q. It is seen that G_q is normal in H_q and H_q is normal in U_q.