BULL. AUSTRAL. MATH. SOC. 11T06, 11T71
VOL. 57 (1998) [351–351]

Several classes of single variable polynomials over finite fields

MARIE HENDERSON

In this thesis we investigate several well-known classes of polynomials defined over a finite field $\mathbb{F}_q$. We consider various properties of the Dickson polynomials, in particular the Dickson polynomials of the second kind, and the linearised and sub-linearised polynomials.

A polynomial which represents a function that permutes the elements of $\mathbb{F}_q$ is called a permutation polynomial. We find new classes of permutation polynomials of $\mathbb{F}_q$ which are members of the class of Dickson polynomials of the second kind (DPSK). If $a = 0$ then the DPSK are given by $f_k(X, a) = S^k$. The permutation behaviour of these polynomials is well understood so we focus on those where $a \in \mathbb{F}_q^*$. It is shown that the permutation behaviour of the tow DPSK, $f_k(X, a)$ and $f_k(X, a')$ where $a, a' \in \mathbb{F}_q^*$ and $\eta(a) = \eta(a')$, is equivalent (here η represents the quadratic character of $\mathbb{F}_q$). That is to say, either both polynomials are permutation polynomials of $\mathbb{F}_q$ or both polynomials fail to be permutation polynomials of $\mathbb{F} - q$. Various classes dependent on k, q and whether $a \in \mathbb{F}_q^*$ is a square or non-square in $\mathbb{F}_q$ are given. Simple restrictions on those k for which the Dickson polynomial of the second kind $f_k(X, a)$ is a permutation polynomial of $\mathbb{F}_q$ are obtained.

The composition behaviour of the linearised and sub-linearised polynomials is discussed. A connection between the composition behaviour of certain linearised and sub-linearised polynomials is established. The question of which linearised and sub-linearised polynomials are indecomposable over $\mathbb{F}_q$ is examined. An application of these results to cryptography is then developed. Cryptosystems based on both the linearised and sub-linearised polynomials are introduced. The security of the systems is discussed briefly.

School of Information Technology
The University of Queensland
Queensland 4072
Australia
e-mail: marie@it.uq.edua.u

Received 15th October, 1997
Thesis submitted to The University of Queensland, March 1997. Degree approved, July 1997. Supervisor: Dr. R. Matthews, Dr. K. Matthews and Dr G. Havas.