J. Austral. Math. Soc. (Series A) 41 (1986), 336–338

ON A PROBLEM OF NIEDERREITER AND ROBINSON ABOUT FINITE FIELDS

DAQING WAN

(Received 26 October 1984; revised 2 April 1985)

Abstract

In this article, we prove that for a finite field F_q with even $q > 3$, any complete mapping polynmial of F_q has reduced degree at most $q - 3$. This is a solution to a problem of Niederreiter and Robinson about finite fields.;

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 C 05.

In this article, we consider a special class of mappings of a finite field into itself. We start with the following definition.

DEFINITION. Let $f(x)$ be a polynomial over a finite field F_q.

(1) If the mapping $c \in F_q \mapsto f(c)$ is a bijection, then $f(x)$ is called a *permutation polynomial* of F_q.

(2) If both $f(x)$ and $f(x) + x$ are permutation polynomials of F_q, then $f(x)$ is called a *complete mapping polynomial* of F_q.

(3) The degree of the reduction of $f(x)$ modulo $(x^q - x)$ is called the *reduced degree* of $f(x)$. It is unique and is always less than q.

Dickson [1] proved that a permutation polynomial $f(x)$ of F_q has reduced degree at most $q - 2$.

Recently, Niederreiter and Robinson [2] proved that for a finite field F_q with odd $q > 3$, any complete mapping polynomial $f(x)$ has reduced degree at most $q - 3$. They indicated that it would be of interest to determine whether this result holds also for even q.

We obtain an affirmative answer to this problem in the following theorem.

THEOREM. *Let $q = 2^k > 3$. Then any complete mapping polynomial of F_q has reduced degree at most $q - 3$.*

This bound is also in a sense best possible since $f(x) = ax$ $(a \neq 0, 1)$ is a complete mapping polynomial of F_4 of reduced degree 1.

PROOF (of the theorem). It is well known that F_q can be identified with the residue class ring $E/2E$ for a suitable ring E of algebraic integers in an algebraic number field. Let η be the canonical ring homomorphism from E onto $F_q = E/2E$. Then η can be extended to a homomorphism η' of $E[x]$ to $F_q[x]$ $(\eta'(x) = x)$; we still write the map η' as η.

Now, let g be a generator of F_q, g_1 be an inverse image of g. Then we have

$$g_1^{q-1} \equiv 1 \pmod 2, \quad g_1^i \not\equiv 1 \pmod 2, \quad \text{for } 0 < i < q - 1.$$

If $g_1^{q-1} \not\equiv 1 \pmod 4$, then

$$\begin{aligned}\left(g_1\left(1 + 2\left(\frac{g_1^{q-1} - 1}{2}\right)\right)\right)^{q-1} &\equiv g_1^{q-1} + 2g_1^{q-1}(q-1)\left(\frac{g_1^{q-1} - 1}{2}\right) \\ &\equiv 1 + 2\left(\frac{g_1^{q-1} - 1}{2}\right) - 2g_1^{q-1}\left(\frac{g_1^{q-1} - 1}{2}\right) \equiv 1 \pmod 4\end{aligned}$$

and

$$\eta\left(g_1\left(1 + 2\left(\frac{g_1^{q-1} - 1}{2}\right)\right)\right) = \eta(g_1) = g.$$

Hence, without loss of generality, we may suppose that

$$g_1^{q-1} \equiv 1 \pmod 4. \tag{1}$$

For a permutation polynomial $f(x)$ of F_q, let $F(x)$ be an inverse image of $f(x)$, that is, $\eta(F(x)) = f(x)$, and let $S = \{g_1^i \mid 1 \leqslant i \leqslant q - 1\} \cup \{0\}$.

From the definition, we have

$$\{\eta(x) \mid x \in S\} = F_q, \qquad \{\eta(F(x)) \mid x \in S\} = F_q.$$

Hence

$$\sum_{x \in S} F^2(x) = \sum_{x \in S} (x + 2 \cdot G(x))^2, \tag{2}$$

where $G(x) \in E$ for any $x \in S$. By (2), we have

$$\sum_{x \in S} F^2(x) \equiv \sum_{x \in S} x^2 \pmod 4 = g_1^2\left(\frac{g^{2(q-1)} - 1}{g_1^2 - 1}\right) \equiv 0 \pmod 4 \tag{3}$$

https://doi.org/10.1017/S1446788700033784 Published online by Cambridge University Press

by (1). If $f(x)$ is a complete mapping polynomial of F_q, then both $f(x)$ and $f(x)+x$ are permutation polynomials of F_q. In terms of (3), this given

$$\sum_{x\in S} F^2(x) \equiv 0 \pmod 4, \tag{4}$$

and

$$\sum_{x\in S} (F(x)+x)^2 \equiv 0 \pmod 4. \tag{5}$$

By Dickson's theorem, the permutation polynomial $f(x)$ can be taken in the form

$$f(x) = a_{q-2}x^{q-2} + a_{q-3}x^{q-3} + \cdots + a_0, \qquad a_i \in F_1.$$

Let $F(x)$ be an inverse image of $f(x)$ such that

$$F(x) = b_{q-2}x^{q-2} + b_{q-3}x^{q-3} + \cdots + b_0, \qquad b_i \in E.$$

From (4) and (5), we have

$$\begin{aligned} 0 &\equiv \sum_{x\in S} (F(x)+x)^2 = \sum_{x\in S} F^2(x) + \sum_{x\in S} x^2 + 2\sum_{x\in S} xF(x) \\ &\equiv 0 + 0 + 2\sum_{x\in S} b_{q-2}x^{q-1} \equiv -2b_{q-2} \pmod 4. \end{aligned}$$

Hence, $b_{q-2} \equiv 0 \pmod 2$, and $a_{q-2} = \eta(b_{q-2}) = 0$, that is, $f(x)$ has reduced degree at most $q-3$, and the theorem is proved.

The author is grateful to Professor Ko Chao and Professor Sun Oi for their kind guidance.

References

[1] L. E. Dickson, *Linear groups* (Dover, New York, 1958).

[2] H. Niederreiter and K. H. Robinson, 'Complete mappings of finite fields,' *J. Austral. Math. Soc.* (*Ser. A*) **33** (1982), 197–212.

Department of Mathematics
Sichuan University
Chengdu
China