ISRAEL JOURNAL OF MATHEMATICS, Vol. 46, Nos. 1-2, 1983

LIKEABLE FUNCTIONS IN FINITE FIELDS

BY
STEPHEN D. COHEN

ABSTRACT
The concept of a likeable function over a finite field of order $q = p^r$ was introduced by W. Kantor [3] for the purpose of constructing certain interesting translation planes of order q^2. It is shown that when q is odd then, except for the class shown by Kantor to occur in fields of characteristic 5, any other non-zero likeable function can exist only if $r > \max(\frac{1}{2}\sqrt{p}, 2)$.

1. Introduction

A function $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$, where $q = p^r$ is not a power of 3, is called *likeable* if (a) f is additive and (b) the equation

$$x^2 = xy^2 - \tfrac{1}{3}y^4 + yf(y)$$

over $\mathrm{GF}(q)$ has the unique solution $(x, y) = (0, 0)$. The concept was introduced by W. Kantor [3], who showed that to each likeable function corresponds a translation plane of order q^2 and kern $\mathrm{GF}(q)$. The translation planes so contructed admit an abelian group of collineations having a point orbit of length q^2 on the line at infinity but having only q elations. Furthermore, the planes obtained by deriving the corresponding dual translation planes are of Lenz–Barlotti type II.1 and admit a collineation group sharply-transitive on the affine points. For full details the reader is referred to [3].

Known examples of likeable functions are as follows (see [3], [1]).

(i) f is the zero function and $q \equiv -1 \pmod 6$. This yields the Walker translation planes.

(ii) $f(y) = c^2y + cy^2$ and $q = 2^r$ where r is odd, $r \geqq 3$ and $c \in \mathrm{GF}(2^r)$. Here the corresponding translation plane is the Betten plane.

(iii) $f(y) = ny^5 + n^{-1}y$ and $q = 5^r$ where $r \geqq 2$ and n is a non-square in $\mathrm{GF}(5^r)$. We shall refer to these as Kantor's functions.

Received January 24, 1983

In fact, M. J. Ganley [2] has shown that, if q is even, then the examples of (ii) are the only likeable functions. We therefore assume from now on that $p > 3$. We show that other likeable functions, if they exist at all, are rare. In particular they can occur only if $r > \max(\frac{1}{2}\sqrt{p}, 2)$.

We round off this introduction with some preliminaries. Observe that the definition of a likeable function f can be recast as follows.

(a) f can be represented uniquely as a polynomial of degree p^{r-1} of the form $\Sigma_{i=0}^{r-1} f_i x^{p^i}$ (see [5]).

(b) $F(y) = y^{-1}f(y) - y^2/12$ is a non-square for all $y \neq 0$ in $\mathrm{GF}(q)$ (see [3]).

(We shall assume below that f has the form (a) and $F(y)$ is given by (b).) In the light of this formulation the following consequence of Weil's theorem will clearly be useful.

LEMMA. *Let $g(y)$ be a polynomial of degree d over* $\mathrm{GF}(q)$ *not identically of the form $ch^2(y)$ ($c \in \mathrm{GF}(q)$). Suppose that $d < \sqrt{q}$. Then $g(y)$ is a square for some non-zero y in* $\mathrm{GF}(q)$.

PROOF. Let χ denote the quadratic character in $\mathrm{GF}(q)$. Then the number of non-zero y for which $g(y)$ is a non-square is at most

$$\begin{aligned}\frac{1}{2}\sum_{\substack{y \neq 0\\ y \in \mathrm{GF}(q)}} (1-\chi(g(y))) &\leqq \frac{1}{2}\left(q-1+\left|\sum_{y\in \mathrm{GF}(q)}\chi(g(y))\right|+1\right)\\ &\leqq \tfrac{1}{2}(q+(d-1)\sqrt{q}) \qquad \text{(see [4], p. 43)}\\ &< q-1,\end{aligned}$$

since $d < \sqrt{q}$ and $q > 4$.

2. Canonical extensions of a likeable function

A *canonical extension* of a function f defined over $\mathrm{GF}(q)$ by a polynomial of degree $< q-1$ is a function over a proper finite extension of $\mathrm{GF}(q)$ defined by the same polynomial. Clearly, the canonical extension of a Kantor likeable function over $\mathrm{GF}(5^r)$ to $\mathrm{GF}(5^{rt})$ (where t is odd) is a likeable function in $\mathrm{GF}(5^{rt})$. We prove that no other non-zero likeable function has such a property.

THEOREM 1. *Let f be a non-zero likeable function if* $\mathrm{GF}(q)$ *(q odd). Suppose that f possesses a canonical extension which is also likeable. Then f is a Kantor function.*

PROOF. By the lemma $F(y) = nh^2(y)$ (identically), where h is some monic polynomial and n some non-square in GF(q). Clearly, f cannot be a monomial and so, taking the degree of F to be $p^k - 1$, we may write

$$F(y) = f_k y^{p^k-1} + f_j y^{p^j-1} + \cdots - \tfrac{1}{12}y^2,$$

where $0 \leqq j < k$ and $f_j f_k \neq 0$. Now, if $h(y)$ begins $y^{\frac{1}{2}(p^k-1)} + cy^u + \cdots$ ($c \neq 0$), then, of course,

$$h^2(y) = y^{p^k-1} + 2cy^{\frac{1}{2}(p^k-1)+u} + \cdots.$$

But, since $p > 2$, then $\frac{1}{2}(p^k - 1) + u$ exceeds $p^j - 1$. We must therefore have $j = 0$ and $\frac{1}{2}(p^k - 1) + u = 2$ which can occur only if $p^k = 5$ and $u = 0$. Thus $q = 5^r$ and

$$F(y) = f_1 y^4 + 2y^2 + f_0 = n(y^2 + c)^2;$$

whence $f_1 = n$ and $f_0 f_1 = 1$. This completes the proof.

3. Restrictions on r

THEOREM 2. *Suppose that f is a non-zero likeable function which is not a Kantor function over* GF(p^r) $(p > 3)$. *Then* $r > \max(\frac{1}{2}\sqrt{p}, 2)$.

PROOF. Suppose first that $r = 2$. Then $F(y)$ has degree $p - 1 < \sqrt{q}$ and the result follows from the lemma and Theorem 1.

For a general r, select any θ in GF(q) for which $f(\theta) \neq 0$, put $\gamma = f(\theta)/\theta^3 \neq 0$ and let s be the smallest divisor of r for which $\gamma \in$ GF(p^s). Let x be any non-zero element of GF(p). Since f is additive then $f(x\theta) = xf(\theta)$ and so $F(x\theta) = \theta^2(\gamma - x^2/12)$. Further, the norm of $\gamma - x^2/12$ from GF(p^r) to GF(p) obviously takes the form $(g(x^2/12))^{r/s}$ where

$$g(y) = (\gamma - y)(\gamma^p - y) \cdots (\gamma^{p^{s-1}} - y),$$

an irreducible polynomial of degree s over GF(p). Moreover, it is an elementary fact that, if $\gamma - x^2/12$ is a non-square in GF(q), then its norm is a non-square in GF(p). Hence r/s is odd and $g(x^2/12)$, which has degree $2s$, is a non-square in GF(p) for all $x \neq 0$. It follows from the lemma that $(2r \geqq)\ 2s > \sqrt{p}$.

REMARKS. For a likeable function f, we cannot have $f(\theta)/\theta^3$ $(\neq 0)$ in GF(p) for any θ in GF(q); otherwise we could take $s = 1$ in the above proof to yield a contradiction. Again, if $f(y)/y$ is constant for all y in GF(p^s) where $s \mid r$, then $f(y) = \sum_{i=0}^{(r/s)-1} f_{is} y^{p^{is}}$ and the above argument implies that $r > \max(\frac{1}{2}s\sqrt{p^s}, 2s)$

unless f is a Kantor function. It is my guess that no further likeable functions remain to be discovered.

REFERENCES

1. J. B. Fink, N. L. Johnson and F. W. Wilke, *A characterisation of "likeable" translation planes*, submitted for publication.

2. M. J. Ganley, *On likeable translation planes of even order*, Archiv. Math., to appear.

3. W. Kantor, *On point transitive affine planes*, Isr. J. Math. **42** (1982), 227–234.

4. W. M. Schmidt, *Equations over finite fields, an elementary approach*, Lecture Notes in Mathematics **536**, Springer–Verlag, 1976.

5. T. P. Vaughan, *Polynomials and linear transformations over finite fields*, J. Reine Angew. Math. **262** (1974), 179–206.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GLASGOW
GLASGOW G12 8QW, SCOTLAND