Functions over finite fields that determine few directions

Simeon Ball [1]

Departament de Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya, Barcelona.

Abstract

We investigate functions f over a finite field $\mathbb{F}_q$, with q prime, with the property that the map x goes to $f(x) + cx$ is a permutation for at least $2\sqrt{q-1}$ elements c of the field. We also consider the case in which q is not prime and f is a function in many variables and pairs of functions (f, g) with the property that the map x goes to $f(x) + cg(x) + dx$ is a permutation for many pairs (c, d) of elements of the field.

Let $\mathbb{F}_q$ denote the finite field with q elements and suppose that f is a function from $\mathbb{F}_q$ to $\mathbb{F}_q$ for which there are $M(f)$ elements $c \in \mathbb{F}_q$ with the property that

$$x \mapsto f(x) + cx$$

is a permutation of $\mathbb{F}_q$. Equivalently, for all distinct x and y in $\mathbb{F}_q$ we have $f(x)+cx \neq f(y)+cy$ and so $-c \neq (f(y) - f(x))/(y - x)$, and so $-c$ is not a direction determined by the graph of the function f.

In [10] Rédei proved that if q is prime and $M(f) > (q - 1)/2$ then f is linear, and so $M(f) = q - 1$. As a corollary to this result he proved that if G is an elementary abelian group of size q^2 and A and B are subsets of G with the property that any element of G can be written uniquely as the sum of an element of A and an element of B, then either A or B is a coset.

In the articles [5] (not characteristic 2 or 3) and [1] (all characteristics) it was proved for any q that if $M(f) > (q-1)/2$ then either f is linear or $q-q/s \geq M(f) \geq q+1-(q-1)/(s-1)$ for some subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ and if $s > 2$ then f is linear over $\mathbb{F}_s$.

As mentioned above $M(f)$ is the number of directions (not including the infinite direction) not determined by the graph of f, $\{(x, f(x)) \mid x \in \mathbb{F}_q\}$. Clearly applying affine transformations to the graph of f does not alter $M(f)$ and so we are only interested in functions f up to affine transformations.

If q is odd and we take $f(x) = x^{(q+1)/2}$ then $M(f) = (q - 1)/2$. Moreover, Lovász and Schrijver [8] proved that if $M(f) = (q - 1)/2$ and q is prime then the function f is affinely equivalent to $x^{(q+1)/2}$. This may extend to all odd q, no proof or counterexample is known.

[1] The author acknowledges the support of the Ramon y Cajal programme and the project MTM2005-08990-C02-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

For q square there are examples of functions with $M(f) = (q - \sqrt{q})/2$ constructed by Polverino, Szőnyi and Weiner [9].

However, for q prime, Gács [6] proved that if $M(f) \geq (q+2)/3$ then f is affinely equivalent to $x^{(q+1)/2}$ or f is linear. In fact, Gács proved that the graph of f is contained in the union of two lines and then applied a result of Szőnyi [13] which classifies all functions whose graph is contained in the union of two lines and for which $M(f) \geq 3$.

In recent work with Gács and Sziklai we have been able to determine additional properties of the graph of f, in the case that q is prime, whenever $M(f) \geq 2\sqrt{q-1}$. With these additional properties the hope is to classify the functions f for which $M(f) \geq (q+5)/4$.

In the geometric setting the problem generalises to three dimensions in two ways. Either we consider the graph of a function in two variables $\{(x, y, h(x, y)) \mid x, y \in \mathbb{F}_q\}$ or we consider the graph of a pair of functions $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_q\}$.

The first case has applications to ovoids of generalised quadrangles and the second case may help in resolving an unsolved problem of Rédei regarding factorising the elementary abelian group of size p^3, p prime, into subsets of size p^2 and p.

In [4] and [2] it is shown that if h is a function in two variables with $M(h) > p^e(q-1)$ directions not determined, where $q = p^t$, then every hyperplane is incident with 0 modulo p^{e+1} points of the graph of h. The bound is almost tight in the case that $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$. The bound is particularly useful in the case q is prime and led to the following conjecture, which is the *strong cylinder conjecture*.

A set of p^2 points S in $\mathrm{AG}(3, p)$, p prime, with the property that every plane is incident with 0 modulo p points of S is the union of p parallel lines.

If $M(h) > q(q-1)/2$ then Storme and Sziklai [12] proved that the results in the planar case can be direcly applied to h.

The two variable case generalises to n variables without any surprises, see [2].

In the case of two functions f and g we define $M(f, g)$ to be the number of pairs (c, d), where c and d are elements of $\mathbb{F}_q$, with the property that

$$x \mapsto f(x) + cg(c) + dx,$$

is a permutation of $\mathbb{F}_q$. In geometric terms to each pair (c, d) there is a set of q parallel planes with equation $dX + Y + cZ = e$ all of which are incident with exactly one point of the graph, $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_q\}$, of (f, g).

Gács planar result from [6] implies that when q is prime and $M(f, g) \gtrsim q^2/3$ the graph of (f, g) is contained in a plane, and is affinely equivalent to the graph of $x^{(q+1)/2}$ or a straight line. However, using algebraic curves and a bound of Stohr-Voloch [11] on the number of points on an algebraic curve [3], one can improve this to $M(f, g) \gtrsim 2q^2/9$. Moreover there are functions f and g when $q = 1$ modulo 3 for which $M(f, g)$ has this order of magnitude.

References

[1] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, **104** (2003) 341–350.

[2] S. Ball, On the graph of a function in many variables over a finite field, *Des. Codes Cryptogr.*, to appear.

[3] S. Ball, A. Gács, P. Sziklai, On the number of directions determined by a pair of functions over a prime field, *J. Combin. Theory Ser. A*, to appear.

[4] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.*, **23** (2006) 243–253.

[5] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined over a finite field, *J. Combin. Theory Ser. A*, **86** (1999) 187–196.

[6] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, **23** (2003) 585–598.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge University Press, 1997.

[8] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981) 449–454.

[9] O. Polverino, T. Szőnyi and Z. Weiner, Blocking sets in Galois planes of square order, *Acta Sci. Math. (Szeged)*, **65**, (1999), 773–784.

[10] L. Rédei, *Lückenhafte Polynome über endlichen Körpen*, Birkhäuser-Verlag, Basel, 1970. (English translation: *Lacunary Polynomials over finite fields*, North-Holland, Amsterdam, 1973.)

[11] K-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.*, **52** (1986) 1–19.

[12] L. Storme and P. Sziklai, Linear point sets and Rédei type k-blocking sets in $PG(n,q)$, *J. Algebraic Combin.*, **14** (2001) 221–228.

[13] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991) 197–212.