Finite Fields and Their Applications 108 (2025) 102683

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Extending a result of Carlitz and McConnel to polynomials which are not permutations

Bence Csajbók [a,b,1]

[a] *Department of Computer Science, ELTE Eötvös Loránd University, Pázmány P. stny. 1/C, 1117 Budapest, Hungary* [2]
[b] *Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, 70125 Bari, Italy*

A R T I C L E I N F O

Article history:
Received 4 September 2024
Received in revised form 30 May 2025
Accepted 15 June 2025
Available online xxxx
Communicated by Gary L. Mullen

MSC:
12E05

Keywords:
Finite field
Direction problem
Linearized polynomial
Permutation polynomial

A B S T R A C T

Let D denote the set of directions determined by the graph of a polynomial f of $\mathbb{F}_q[x]$, where q is a power of the prime p. If D is contained in a multiplicative subgroup M of $\mathbb{F}_q^\times$, then by a result of Carlitz and McConnel it follows that $f(x) = ax^{p^k} + b$ for some $k \in \mathbb{N}$. Of course, if $D \subseteq M$, then $0 \notin D$ and hence f is a permutation. If we assume the weaker condition $D \subseteq M \cup \{0\}$, then f is not necessarily a permutation, but Sziklai conjectured that $f(x) = ax^{p^k} + b$ follows also in this case. When q is odd, and the index of M is even, then a result of Ball, Blokhuis, Brouwer, Storme and Szőnyi combined with a result of Göloğlu and McGuire proves the conjecture. Assume $\deg f \geq 1$. We prove that if the size of $D^{-1}D = \{d^{-1}d' : d \in D \setminus \{0\}, d' \in D\}$ is less than $q - \deg f + 2$, then f is a permutation of $\mathbb{F}_q$. We use this result to prove the conjecture of Sziklai.

E-mail address: bence.csajbok@ttk.elte.hu.

[1] This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and partially by the ELTE TKP 2021-NKTA-62 funding scheme.

[2] Current address.

https://doi.org/10.1016/j.ffa.2025.102683

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of $q = p^n$ elements, where p is a prime. If f is an $\mathbb{F}_q \to \mathbb{F}_q$ function then the affine q-set $U_f := \{(x, f(x)) : x \in \mathbb{F}_q\} \subseteq \mathrm{AG}(2, q)$ is called the graph of f, the subset $D_f := \{(f(x) - f(y))/(x - y) : x, y \in \mathbb{F}_q, x \neq y\}$ of $\mathbb{F}_q$ is called the set of directions, or slopes, determined by (the graph of) f. Each $\mathbb{F}_q \to \mathbb{F}_q$ function can be uniquely represented by a polynomial of $\mathbb{F}_q[x]$ with degree at most $q - 1$, so we will consider polynomials instead of functions. For a subset A of $\mathbb{F}_q$ we will denote $A \setminus \{0\}$ by A^*.

When $d > 1$ is a divisor of $q - 1$, put

$$M_d := \{x^d : x \in \mathbb{F}_q^*\}.$$

The following result was proved first by Carlitz in the case of $d = 2$ [4] and then generalized by McConnel for other divisors d of $q - 1$ [9].

Result 1.1. If $D_f \subseteq M_d$, then f is of the form $f(x) = a + bx^{p^k}$ for some non-negative integer k, $a \in \mathbb{F}_q$, $b \in M_d$ and $(p^k - 1)$ a multiple of d.

There are several generalizations and different proofs of this result, due to Bruen and Levinger [3], Grundhöfer [6], Lenstra [8], see [7, Section 9] for a survey on these results and their relation with the Paley graph.

Since $0 \notin D_f$ yields $f(x) \neq f(y)$ for each $x \neq y$, it is obvious that only permutations can satisfy the condition $D \subseteq M_d$. This is not the case anymore if we allow $D \subseteq M_d \cup \{0\}$. In [10, pg. 114] Sziklai conjectured that $f(x) = ax^{p^k} + b$ holds also when one replaces M_d with $M_d \cup \{0\}$ in the statement of Result 1.1. To present what is known regarding this conjecture, we need to recall some definitions. An $\mathbb{F}_q \to \mathbb{F}_q$ function f is called additive if $f(a + b) = f(a) + f(b)$ for each $a, b \in \mathbb{F}_q$. Such functions correspond to polynomials $a_0 x + a_1 x^p + \cdots + a_{n-1} x^{p^{n-1}} \in \mathbb{F}_q[x]$. If f is additive and $\alpha \in \mathbb{F}_q$, then we will call $f + \alpha$ an affine polynomial. An important result on directions is the following, due to Ball, Blokhuis, Brouwer, Storme, Szőnyi [2] and Ball [1].

Result 1.2. If $|D_f| \leq (q + 1)/2$, then f is an affine polynomial.

If f is additive, then for the affine polynomial $g = f + \alpha$ it holds that $D_g = \{f(x)/x : x \in \mathbb{F}_q^*\} = D_f$. The following result is due to McGuire and Göloğlu [5].

Result 1.3. If q is odd, f is additive and $D_f \subseteq M_2 \cup \{0\}$, then $f(x) = ax^{p^k}$ for some non-negative integer k and $a \in M_2 \cup \{0\}$.

If $D_g \subseteq M_2 \cup \{0\}$, then $|D_g| \leq (q + 1)/2$ and hence by Result 1.2 $g = f + \alpha$ for some additive f with $D_f = D_g$, thus Result 1.3 proves Sziklai's conjecture in case of odd q

and even d. In [5] the authors used Gauss sums and it seems to be that their technique cannot be used to prove the conjecture when d is odd.

Our key result is Theorem 2.1. Its proof was inspired by the recent manuscript [11] of C. H. Yip who used Result 1.2 in a clever way to strengthen Result 1.1. In Corollary 2.5 we extend Yip's result to polynomials which are not necessarily permutations. Our notation is standard, if $A, B \subseteq \mathbb{F}_q$ then $A^{-1} = \{a^{-1} : a \in A^*\}$ and $AB = \{ab : a \in A, b \in B\}$. If $c \in \mathbb{F}_q$, then $A - c = \{a - c : a \in A\}$. In Theorem 2.2 and Corollary 2.3 we present conditions on the size of $D_f^{-1}D_f$ which ensure that f is a permutation. In Corollary 2.4 we prove Conjecture 18.11 from [10, pg. 114] by Sziklai:

Conjecture 1.4. *If $D_f \subseteq M_d \cup \{0\}$, then f is of the form $f(x) = a + bx^{p^k}$ for some non-negative integer k, $a \in \mathbb{F}_q$, $b \in M_d \cup \{0\}$ and $(p^k - 1)$ a multiple of d.*

2. New results

Our first result shows how a simple combinatorial property of the graph of f implies an algebraic property of D_f. Recall that the graph U_f of f is a set of q points in the finite affine plane $\mathrm{AG}(2, q)$. The common points of a line ℓ of equation $y = mx + b$ and the graph U_f are exactly those points $(x, f(x))$, for which $f(x) = mx + b$. Now $f(x) - mx - b$ is either the zero polynomial, in which case $\ell = U_f$, or it has at most $\deg f$ distinct roots in $\mathbb{F}_q$. It might be that x_0 is a multiple root of $f(x) - mx - b$, but also in that case there is only one corresponding point in the intersection of the point sets U_f and ℓ, namely $(x_0, f(x_0))$, and we count this point like the others with multiplicity one. If the intersection of the point sets U_f and ℓ has size k then we will say that ℓ meets U_f in k points and this happens exactly when $\deg \gcd(f(x) - mx - b, x^q - x) = k$.

Theorem 2.1. *Assume that the line of equation $y = mx + b$ meets the graph of $f \in \mathbb{F}_q[x]$ in k points for some $1 < k < q$. Then*

$$|(D_f - m)^{-1}(D_f - m)| \geq q - k + 2.$$

Proof. Put $g(x) := f(x) - mx - b$. Then g has exactly k distinct roots in $\mathbb{F}_q$. Let a be one of them and define $h(x) := g(x + a)$. Clearly h is again a polynomial over $\mathbb{F}_q$ with exactly k distinct roots in $\mathbb{F}_q$ and 0 is one of them. Also,

$$D_h = \left\{ \frac{h(x) - h(y)}{x - y} : x, y \in \mathbb{F}_q, x \neq y \right\} =$$

$$\left\{ \frac{f(x + a) - f(y + a) - m(x - y)}{(x + a) - (y + a)} : x, y \in \mathbb{F}_q, x \neq y \right\} = D_f - m.$$

Denote by $r_1, r_2, \ldots, r_{k-1}$ the distinct non-zero roots of h in $\mathbb{F}_q$.

We claim that

$$H := \left\{ \frac{x}{x-y} : x, y \in \mathbb{F}_q,\ h(x) \neq 0,\ h(y) = 0 \right\} \subseteq D_h^{-1} D_h, \tag{1}$$

and

$$|H| \geq q - k + 1. \tag{2}$$

To prove (1) take an element $x/(x-y)$ from H (i.e., $h(x) \neq 0$, $h(y) = 0$) and put $c = x/h(x)$. Since $h(0) = 0$, we have

$$c = \frac{x}{h(x)} = \frac{x - 0}{h(x) - h(0)} \in D_h^{-1}.$$

Also, since $h(y) = 0$, we have

$$\frac{x}{x-y} = c\frac{h(x) - h(y)}{x - y} \in D_h^{-1} D_h.$$

To prove (2) first note that $0, 1 \in D_h^{-1} D_h$, $0 \notin H$ and $1 \in H$. Assume that $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ is not contained in H. Then the solutions in x of the equations

$$x/(x - r_i) = \alpha, \quad i \in \{1, 2, \ldots, k-1\}, \tag{3}$$

are in $\{r_1, r_2, \ldots, r_{k-1}\}$. If x is a solution of $x/(x - r_i) = \alpha$, then $x = r_i\alpha/(\alpha - 1)$, so if $\alpha \notin H$, then

$$\frac{\alpha}{\alpha - 1} \cdot \{r_1, r_2, \ldots, r_{k-1}\} \subseteq \{r_1, r_2, \ldots, r_{k-1}\},$$

and hence

$$\frac{\alpha}{\alpha - 1} \cdot \{r_1, r_2, \ldots, r_{k-1}\} = \{r_1, r_2, \ldots, r_{k-1}\}.$$

Put $\beta = \alpha/(\alpha - 1)$ and $R = \{r_1, r_2, \ldots, r_{k-1}\}$. Then $\beta R = R$. Clearly there are at most $k - 1$ such βs: $r_1/r_1, r_2/r_1, \ldots, r_{k-1}/r_1$, but $\beta \neq 1$ and hence there are at most $k - 2$ values of $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ for which (3) does not have a solution with $h(x) \neq 0$. It follows that $|H| \geq (q - 2) - (k - 2) + 1$ (because of $1 \in H$). Since $0 \in D_h^{-1} D_h \setminus H$, we have $|D_h^{-1} D_h| \geq |H| + 1$, which proves the assertion. $\square$

Corollary 2.2. *Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree k for some $0 < k < q$. If $|D_f^{-1} D_f| < q - k + 2$, then f is a permutation of $\mathbb{F}_q$.*

Proof. If $k = 1$, then f is a permutation. Assume $k > 1$. If f was not a permutation, then there would be a line with slope 0 meeting U_f in at least two and at most k points (since $f(x) = c$ has at most $\deg f$ roots for each $c \in \mathbb{F}_q$). By Theorem 2.1 it follows that $|D_f^{-1}D_f| \geq q - k + 2$, contradicting the assumption. □

Corollary 2.3. *If $|D_f^{-1}D_f| \leq (q+1)/2$ holds for some $\mathbb{F}_q \to \mathbb{F}_q$ non-constant function f, then f permutes $\mathbb{F}_q$.*

Proof. f is non-constant, hence there is a non-zero element in D_f, so $D_f^{-1} \neq \emptyset$ and $|D_f| \leq |D_f^{-1}D_f|$. By Result 1.2 f can be represented by an affine polynomial of degree at most $q/p \leq q/2$. Then

$$|D_f^{-1}D_f| \leq \frac{q+1}{2} < q - q/2 + 2 \leq q - \deg f + 2,$$

and the result follows from Theorem 2.2. □

The next result proves Conjecture 18.11 from [10, pg. 114].

Corollary 2.4. *If $D_f \subseteq M_d \cup \{0\}$, then f is of the form $f(x) = a + bx^{p^k}$ for some non-negative integer k, $a \in \mathbb{F}_q$, $b \in M_d \cup \{0\}$ and $(p^k - 1)$ a multiple of d.*

Proof. $D_f^{-1}D_f \subseteq M_d^{-1}(M_d \cup \{0\}) = M_d \cup \{0\}$ and hence $|D_f^{-1}D_f| \leq |M_d| + 1 \leq (q+1)/2$. By Corollary 2.3 f is a constant function (that is, $b = 0$), or it is a permutation and hence $0 \notin D_f$. The assertion follows from Result 1.1. □

The next result weakens the condition on f from [11, Theorem 1.2], since we do not require f to be a permutation.

Corollary 2.5. *If for some $\mathbb{F}_q \to \mathbb{F}_q$ function f it holds that $|D_f^{-1}D_f D_f^{-1}| \leq (q+1)/2$, then $f(x) = a + bx^{p^k}$.*

Proof. For each subset D_f of $\mathbb{F}_q$ it holds that $|D_f^{-1}D_f| \leq |D_f^{-1}D_f D_f^{-1}|$, thus by Corollary 2.3 f is a constant function or a permutation. In the former case the result trivially holds, in the latter case the statement follows from [11, Theorem 1.2]. □

Data availability

No data was used for the research described in the article.

References

[1] S. Ball, The number of directions determined by a function over a finite field, J. Comb. Theory, Ser. A 104 (2) (2003) 341–350.

[2] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, J. Comb. Theory, Ser. A 86 (1) (1999) 187–196.
[3] A. Bruen, B. Levinger, A theorem on permutations of a finite field, Can. J. Math. 25 (1973) 1060–1065.
[4] L. Carlitz, A theorem on permutations in a finite field, Proc. Am. Math. Soc. 11 (1960) 456–459.
[5] F. Göloğlu, G. McGuire, On theorems of Carlitz and Payne on permutation polynomials over finite fields with an application to $x^{-1} + L(x)$, Finite Fields Appl. 27 (2014) 130–142.
[6] T. Grundhöfer, Über Abbildungen mit eingeschränktem Differenzenprodukt auf einem endlichen Körper, Arch. Math. (Basel) 37 (1) (1981) 59–62.
[7] G.A. Jones, Paley and the Paley graphs, in: Isomorphisms, Symmetry and Computations in Algebraic Graph Theory, in: Springer Proc. Math. Stat., vol. 305, Springer, Cham, 2020, pp. 155–183.
[8] H.W. Lenstra Jr., Automorphisms of finite fields, J. Number Theory 34 (1) (1990) 33–40.
[9] R. McConnel, Pseudo-ordered polynomials over a finite field, Acta Arith. 8 (1963) 127–151.
[10] P. Sziklai, Polynomials in finite geometry, https://www.academia.edu/69422637/Polynomials_in_finite_geometry, 2008.
[11] C.H. Yip, A strengthening of McConnel's theorem on permutations over finite fields, Can. Math. Bull. (2024) 1–6, https://doi.org/10.4153/S0008439524000742. Published online.