Canad. Math. Bull. 2024, pp. 1–6
http://dx.doi.org/10.4153/S0008439524000742
© The Author(s), 2024. Published by Cambridge University Press on behalf of
Canadian Mathematical Society

A strengthening of McConnel's theorem on permutations over finite fields

Chi Hoi Yip

Abstract. Let p be a prime, $q = p^n$, and $D \subset \mathbb{F}_q^*$. A celebrated result of McConnel states that if D is a proper subgroup of $\mathbb{F}_q^*$, and $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function such that $(f(x) - f(y))/(x - y) \in D$ whenever $x \neq y$, then $f(x)$ necessarily has the form $ax^{p^j} + b$. In this notes, we give a sufficient condition on D to obtain the same conclusion on f. In particular, we show that McConnel's theorem extends if D has small doubling.

1 Introduction

Throughout this paper, let p be a prime. Let $q = p^n$ and $\mathbb{F}_q$ be the finite field with q elements with $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

A celebrated result of McConnel [15] states that if D is a proper subgroup of $\mathbb{F}_q^*$, and $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function such that

$$\frac{f(x) - f(y)}{x - y} \in D \tag{1.1}$$

whenever $x, y \in \mathbb{F}_q$ with $x \neq y$, then there are $a, b \in \mathbb{F}_q$ and an integer $0 \leq j \leq n-1$, such that $f(x) = ax^{p^j} + b$ for all $x \in \mathbb{F}_q$. This result was first proved by Carlitz [7] when q is odd and D consists of squares in $\mathbb{F}_q^*$, that is, D is the subgroup of index 2. Carlitz's theorem and McConnel's theorem have various connections with finite geometry, graph theory, and group theory; we refer to a nice survey by Jones [11, Section 9]. In particular, they have many applications in finite geometry; see, for example, [5, 12]. We also refer to variations of McConnel's theorem in [6, 10, 13] via tools from group theory.

One may wonder, if the assumption that D is a multiplicative subgroup plays an important role in McConnel's theorem and if it is possible to weaken this assumption. Inspired by this natural question, in this paper, we find a sufficient condition on D so that if condition (1.1) holds for a function $f : \mathbb{F}_q \to \mathbb{F}_q$, then f necessarily has the form $f(x) = ax^{p^j} + b$. In particular, our main result (Theorem 1.2) strengthens McConnel's theorem.

Before stating our results, we introduce some motivations and backgrounds from the theory of directions and their applications. Let $AG(2, q)$ denote the *affine Galois plane* over the finite field $\mathbb{F}_q$. Let U be a subset of points in $AG(2, q)$; we use Cartesian

Received by the editors July 29, 2024; accepted October 18, 2024.
AMS Subject Classification: **11T06**, 11B30.
Keywords: Finite field, linearized polynomial, direction.

coordinates in $AG(2,q)$ so that $U = \{(x_i, y_i) : 1 \le i \le |U|\}$. The set of *directions determined by* $U \subset AG(2,q)$ is

$$\mathcal{D}_U = \left\{ \frac{y_j - y_i}{x_j - x_i} : 1 \le i < j \le |U| \right\} \subset \mathbb{F}_q \cup \{\infty\},$$

where ∞ is the vertical direction. If $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function, we can naturally consider its graph $U(f) = \{(x, f(x)) : x \in \mathbb{F}_q\}$ and the set of *directions determined by* f is $\mathcal{D}_f := \mathcal{D}_{U(f)}$. Indeed, $\mathcal{D}_f$ precisely computes the set of slopes of tangent lines joining two points on $U(f)$. Using this terminology, condition (1.1) is equivalent to $\mathcal{D}_f \subset D$.

The following well-known result is due to Blokhuis, Ball, Brouwer, Storme, and Szőnyi [3, 4].

Theorem 1.1 *Let p be a prime and let $q = p^n$. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that $f(0) = 0$. If $|\mathcal{D}_f| \le \frac{q+1}{2}$, then f is a linearized polynomial, that is, there are $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q$, such that*

$$f(x) = \sum_{j=0}^{n-1} \alpha_j x^{p^j}, \quad \forall x \in \mathbb{F}_q.$$

In particular, when $q = p$ is a prime, Theorem 1.1 implies McConnel's theorem; this was first observed by Lovász and Schrijver [14]. We remark that when $q = p$ is a prime, Müller [16] showed a stronger result, namely, if D is a non-empty proper subset of $\mathbb{F}_p^*$ such that $f(x) - f(y) \in D$ whenever $x - y \in D$, then there are $a, b \in \mathbb{F}_p$ such that $f(x) = ax + b$ for all $x \in \mathbb{F}_p$. For a general prime power q, Theorem 1.1 does not imply McConnel's theorem directly. However, using the idea of directions, Muzychuk [17] provided a self-contained proof of McConnel's theorem.

While Theorem 1.1 is already quite powerful, in many applications, if some extra information on $\mathcal{D}_f$ is given, it is desirable to obtain a stronger conclusion, namely, $f(x)$ is of the form $ax^{p^j} + b$ for some j, or even $f(x)$ must have the form $ax + b$. As an illustration, we mention two recent works in applying a stronger version of Theorem 1.1 to prove analogs of the Erdős–Ko–Rado (EKR) theorem in the finite field setting [1, 2]. Asgarli and Yip [2] proved the EKR theorem for a family of pseudo-Paley graphs of square order, and their main result roughly states that if $\mathcal{D}_f$ arises from a Cayley graph with "nice multiplicative properties" on its connection set, then $f(x)$ has the form $ax + b$; see [19] for more discussions. As another example, very recently, Aguglia, Csajbók, and Weiner proved several EKR theorems for polynomials over finite fields [1]. Again, one key ingredient in their proof is a strengthening of Theorem 1.1. In [1, Theorem 2.2], they showed that if $\mathcal{D}_f$ is a proper $\mathbb{F}_p$-subspace of $\mathbb{F}_q$, then $f(x)$ has the form $ax + b$; in [1, Theorem 2.13] (see also [9]), they showed that if $\mathcal{D}_f \backslash \{0\}$ is a subset of a coset of K, where K is the subgroup of $\mathbb{F}_q^*$ with index 2, then $f(x)$ has the form $ax^{p^j} + b$ for some j.

Inspired by the connection above between the theory of directions and McConnel's theorem, we establish the following result.

https://doi.org/10.4153/S0008439524000742 Published online by Cambridge University Press

Theorem 1.2 *Let p be a prime. Let $q = p^n$ and $D \subset \mathbb{F}_q^*$. Suppose $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function such that*

$$\frac{f(x) - f(y)}{x - y} \in D$$

whenever $x, y \in \mathbb{F}_q$ with $x \neq y$. If

$$|DD^{-1}D^{-1}| \leq \frac{q+1}{2}, \tag{1.2}$$

then there are $a, b \in \mathbb{F}_q$ and an integer $0 \leq j \leq n-1$, such that $f(x) = ax^{p^j} + b$ for all $x \in \mathbb{F}_q$. In particular, if $c > 0$ is a real number such that $|DD| \leq c|D|$, and $c^3|D| \leq \frac{q+1}{2}$, then the same conclusion holds.

If D is a proper subgroup of $\mathbb{F}_q^*$, then clearly $DD^{-1}D^{-1} = D$ and thus Theorem 1.2 recovers McConnel's theorem. Indeed, in this case, the doubling constant of D is simply $|DD|/|D| = 1$. Our result shows that if the doubling constant $|DD|/|D|$ of D is small, and $|D|$ is not too large, then the analog of McConnel's theorem still holds. There are many ways to construct a set $D \subset \mathbb{F}_q^*$ with small doubling. For example, we can set $D = K \cup E$, where K is a subgroup of $\mathbb{F}_q^*$, and E is an arbitrary subset of $\mathbb{F}_q^*$ such that $|E|$ is small; alternatively, D can be taken to be the union of some cosets of a fixed subgroup K of $\mathbb{F}_q^*$.

For a linearized polynomial $f(x)$, note that $\mathcal{D}_f = \mathrm{Im}(f(x)/x)$. We refer to [8] and references therein on the study of $\mathrm{Im}(f(x)/x)$ for linearized polynomials f. In particular, it is an open question to determine all the possible sizes of $\mathrm{Im}(f(x)/x)$ among linearized polynomials f [8, Section 6]. Theorem 1.2 implies the following corollary, which partially addresses this question. It states that if D is such an image set and D satisfies inequality (1.2), then D is necessarily a coset of a subgroup of $\mathbb{F}_q^*$ with a restricted index.

Corollary 1.3 *Let p be a prime and let $q = p^n$. If $D \subset \mathbb{F}_q^*$ and $|DD^{-1}D^{-1}| \leq \frac{q+1}{2}$, then $D = \mathcal{D}_f$ for some function $f : \mathbb{F}_q \to \mathbb{F}_q$ with $f(0) = 0$ if and only if $D = aK$, where $a \in \mathbb{F}_q^*$ and K is a subgroup of $\mathbb{F}_q^*$ with index $p^r - 1$, where r is a divisor of n.*

Notations. We follow standard notations for arithmetic operations among sets. Given two sets A and B, we write $AB = \{ab : a \in A, b \in B\}$, $A^{-1} = \{a^{-1} : a \in A\}$.

2 Proofs

We start by proving Theorem 1.2. Our proof is inspired by several arguments used in [14, 17].

Proof (Proof of Theorem 1.2) Without loss of generality, by replacing the function $f(x)$ with $f(x) - f(0)$, we may assume that $f(0) = 0$. Since $|\mathcal{D}_f| \leq \frac{q+1}{2}$, Theorem 1.1 implies that f is linearized. Let $g(x) = 1/f(x^{-1})$ for $x \in \mathbb{F}_q \backslash \{0\}$ and set $g(0) = 0$. We claim that g is also linearized.

https://doi.org/10.4153/S0008439524000742 Published online by Cambridge University Press

Let $x, y \in \mathbb{F}_q^*$ with $x \neq y$. Then,

$$\frac{g(x)-g(y)}{x-y} = \frac{\frac{1}{f(x^{-1})} - \frac{1}{f(y^{-1})}}{x-y} = \frac{f(y^{-1})-f(x^{-1})}{(x-y)f(x^{-1})f(y^{-1})} = \frac{f(y^{-1}-x^{-1})}{(x-y)f(x^{-1})f(y^{-1})}$$

since f is linearized. It follows that

$$\frac{g(x)-g(y)}{x-y} = \frac{f(\frac{x-y}{xy})}{(x-y)f(x^{-1})f(y^{-1})} = \frac{f(\frac{x-y}{xy})}{\frac{x-y}{xy}} \cdot \frac{x^{-1}}{f(x^{-1})} \cdot \frac{y^{-1}}{f(y^{-1})} \in DD^{-1}D^{-1}.$$

On the other hand, if $x \in \mathbb{F}_q^*$, then

$$\frac{g(x)-g(0)}{x-0} = \frac{g(x)}{x} = \frac{1}{xf(x^{-1})} = \frac{x^{-1}}{f(x^{-1})} \in D^{-1}.$$

We conclude that

$$\mathcal{D}_g \subset DD^{-1}D^{-1} \cup D^{-1} = DD^{-1}D^{-1}.$$

Then inequality (1.2) implies that $|\mathcal{D}_g| \leq \frac{q+1}{2}$, and Theorem 1.1 implies that g is also linearized.

Since f and g are both linearized, we can find $\alpha_0, \beta_0, \ldots, \alpha_{n-1}, \beta_{n-1} \in \mathbb{F}_q$, such that

$$f(x) = \sum_{j=0}^{n-1} \alpha_j x^{p^j}, \quad \text{and} \quad g(x) = \sum_{j=0}^{n-1} \beta_j x^{p^j}, \quad \forall x \in \mathbb{F}_q.$$

By the definition of g, we have $f(x^{-1})g(x) = 1$ for each $x \in \mathbb{F}_q^*$, and thus $(x^{p^{n-1}} f(x^{-1}))(g(x)/x) = x^{p^{n-1}-1}$ for all $x \in \mathbb{F}_q^*$. Equivalently,

$$h(x) := \left(\sum_{j=0}^{n-1} \alpha_j x^{p^{n-1}-p^j}\right)\left(\sum_{j=0}^{n-1} \beta_j x^{p^j-1}\right) = x^{p^{n-1}-1} \tag{2.1}$$

holds for all $x \in \mathbb{F}_q^*$. Note that $h(x) - x^{p^{n-1}-1}$ is a polynomial with degree at most $2(p^{n-1}-1) \leq p^n - 1 = q-1$, and $h(x) - x^{p^{n-1}-1}$ vanishes on $\mathbb{F}_q^*$. It follows that there is a constant $C \in \mathbb{F}_q$, such that $h(x) - x^{p^{n-1}-1} = C(x^{q-1}-1)$ as polynomials. By setting $x = 0$, we get $C = 0$. Therefore, $h(x) = x^{p^{n-1}-1}$ as polynomials. In particular, $g(x)$ is a factor of $x^{p^{n-1}}$. Thus, there are $\gamma \in \mathbb{F}_q^*$ and $0 \leq j \leq n-1$ such that $g(x) = \gamma x^{p^j}$ for all $x \in \mathbb{F}_q$, and it follows that $f(x) = \gamma^{-1} x^{p^j}$ for all $x \in \mathbb{F}_q$, as required.

Finally, assume that $|DD| \leq c|D|$, and $c^3|D| \leq \frac{q+1}{2}$. Then the Plünnecke–Ruzsa inequality (see, for example, [18, Theorem 1.2]) implies that

$$|DD^{-1}D^{-1}| \leq c^3|D| \leq \frac{q+1}{2},$$

and thus the same conclusion holds. ∎

Now we use Theorem 1.2 to deduce Corollary 1.3.

https://doi.org/10.4153/S0008439524000742 Published online by Cambridge University Press

Proof (Proof of Corollary 1.3) Assume that $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function such that $f(0) = 0$ and $\mathcal{D}_f = D$. Since $D \subset \mathbb{F}_q^*$ and $|DD^{-1}D^{-1}| \leq \frac{q+1}{2}$, Theorem 1.2 implies that there exist $a \in \mathbb{F}_q^*$ and an integer $0 \leq j \leq n-1$, such that $f(x) = ax^{p^j}$ for all $x \in \mathbb{F}_q$. Therefore, $D = \mathcal{D}_f = \{ax^{p^j-1} : x \in \mathbb{F}_q^*\}$. Note that

$$\gcd(p^j - 1, q - 1) = \gcd(p^j - 1, p^n - 1) = p^{\gcd(j,n)} - 1.$$

It follows that

$$D = \{ax^{p^{\gcd(j,n)}-1} : x \in \mathbb{F}_q^*\} = aK,$$

where K is the subgroup of $\mathbb{F}_q^*$ with index $p^{\gcd(j,n)} - 1$.

Conversely, let r be a divisor of n and $a \in \mathbb{F}_q^*$. Let $f(x) = ax^{p^r}$ for all $x \in \mathbb{F}_q$. Then we have $\mathcal{D}_f = \{ax^{p^r-1} : x \in \mathbb{F}_q^*\} = aK$, where K is the subgroup of $\mathbb{F}_q^*$ with index $p^r - 1$. ■

Acknowledgments The author thanks Bence Csajbók for helpful discussions. The author is also grateful to anonymous referees for their valuable comments and suggestions.

References

[1] A. Aguglia, B. Csajbók, and Z. Weiner, *Intersecting families of graphs of functions over a finite field*. Ars Math. Contemp. **24**(2024), no. 1, Article no. 4, 22 pp.
[2] S. Asgarli and C. H. Yip, *Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*. J. Combin. Theory Ser. A **192**(2022), Article no. 105667, 23 pp.
[3] S. Ball, *The number of directions determined by a function over a finite field*. J. Combin. Theory Ser. A **104**(2003), no. 2, 341–350.
[4] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, and T. Szőnyi, *On the number of slopes of the graph of a function defined on a finite field*. J. Combin. Theory Ser. A **86**(1999), no. 1, 187–196.
[5] A. Blokhuis, A. Seress, and H. A. Wilbrink, *Characterization of complete exterior sets of conics*. Combinatorica **12**(1992), no. 2, 143–147.
[6] A. Bruen and B. Levinger, *A theorem on permutations of a finite field*. Canad. J. Math. **25**(1973), 1060–1065.
[7] L. Carlitz, *A theorem on permutations in a finite field*. Proc. Amer. Math. Soc. **11**(1960), 456–459.
[8] B. Csajbók, G. Marino, and O. Polverino, *A Carlitz type result for linearized polynomials*. Ars Math. Contemp. **16**(2019), no. 2, 585–608.
[9] F. Göloğlu and 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.
[10] T. Grundhöfer, *Über Abbildungen mit eingeschränktem Differenzenprodukt auf einem endlichen Körper*. Arch. Math. (Basel) **37**(1981), no. 1, 59–62.
[11] G. A. Jones, *Paley and the Paley graphs*. In: G. A. Jones, I. Ponomarenko, J. Širáň, (eds.), Isomorphisms, symmetry and computations in algebraic graph theory, Springer Proceedings of Mathematics and Statistics, 305, Springer, Cham, 2020, pp. 155–183.
[12] N. Knarr and M. Stroppel, *Polarities and unitals in the Coulter-Matthews planes*. Des. Codes Cryptogr. **55**(2010), no. 1, 9–18.
[13] H. W. Lenstra, Jr, *Automorphisms of finite fields*. J. Number Theory **34**(1990), no. 1, 33–40.
[14] L. Lovász and A. Schrijver, *Remarks on a theorem of Rédei*. Studia Sci. Math. Hungar. **16**(1983), nos. 3–4, 449–454.
[15] R. McConnel, *Pseudo-ordered polynomials over a finite field*. Acta Arith. **8**(1962/63), 127–151.
[16] P. Müller, *Permutation groups of prime degree, a quick proof of Burnside's theorem*. Arch. Math. (Basel) **85**(2005), no. 1, 15–17.

[17] M. E. Muzychuk, *Automorphism groups of Paley graphs and cyclotomic schemes*. In: G. A. Jones, I. Ponomarenko, J. Širáň, (eds.), Isomorphisms, symmetry and computations in algebraic graph theory, Springer Proceedings of Mathematics and Statistics, 305, Springer, Cham, 2020, pp. 185–194.
[18] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*. Combinatorica **32**(2012), no. 6, 721–733.
[19] C. H. Yip, *Erdős–Ko–Rado theorem in Peisert-type graphs*. Canad. Math. Bull. **67**(2024), no. 1, 176–187.

School of Math, Georgia Institute of Technology, Atlanta, GA, United States
e-mail: cyip30@gatech.edu