Finite Fields and Their Applications 53 (2018) 140–143

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# Fourier methods and non degenerate polynomials ☆

Chun-Yen Shen

*Department of Mathematics, National Taiwan University, Taipei, 106, Taiwan*

ARTICLE INFO

*Article history:*
Received 23 September 2016
Received in revised form 2 January 2018
Accepted 9 June 2018
Available online xxxx
Communicated by S. Gao

*MSC:*
11B75

*Keywords:*
Sums
Products and expanding maps

ABSTRACT

We use Fourier methods to give a shorter proof of Vu's result and extend it to a more general setting, namely: For any non-degenerate polynomials $f(x,y) \in \mathbb{F}_q[x,y]$ and $A, B, C, D \subset \mathbb{F}_q$, either we have

$$|A+C||B+D||f(A,B)| \gtrsim |A||B|q,$$

or

$$|A+C||B+D||f(A,B)|^2 \gtrsim \frac{|A|^2|B|^2|C||D|}{q}.$$



## 1. Introduction

The sum-product problems in the finite field setting have been intensively studied since the ground breaking work [1] that if $A \subset \mathbb{F}_p$ with $p$ prime, and $p^\delta < |A| < p^{1-\delta}$, for some $\delta > 0$, then there exist $\epsilon = \epsilon(\delta) > 0$ and $c = c(\delta)$ such that

$$\max(|A+A|, |A \cdot A|) \geq c|A|^{1+\epsilon},$$

☆ C.-Y. Shen supported in part by MOST, through grant 104-2628-M-008-003-MY4.
*E-mail address:* cyshen@math.ntu.edu.tw.

https://doi.org/10.1016/j.ffa.2018.06.002
1071-5797/

where $A + A = \{a + b; a, b \in A\}$ and $A \cdot A = \{ab; a, b \in A\}$. This result has found many important applications in various areas. One of the important questions related to sum-product phenomenon is to find all two variables polynomials $f(x, y) \in \mathbb{F}_q[x, y]$ such that when $|A + A|$ is small, then $|f(A, A)|$ is large. For the case when $|A| \geq q^{1/2}$, this question was solved by Vu [6] via spectral graph theory showing that only non-degenerate polynomials (see definition for details) can do so (the same problem in real numbers was already solved by the author [3]). However as pointed out by Solymosi [4] that there are several examples to indicate that one should be able to use either Fourier methods or spectral graph theory to yield the same results. Indeed by adopting the arguments in [2] we give a simpler and shorter proof of Vu's estimates via Fourier methods and generalize it to a more general setting. Throughout this paper, the notation $M \gtrsim N$ means $M \geq cN$ for some constant $c$ that only depends on the degrees of the polynomials that may appear in the inequality.

**Theorem 1.1.** *Let $f$ be a non-degerenate polynomial in $\mathbb{F}_q[x, y]$ and $A, B, C, D$ be subsets of $\mathbb{F}_q$. Then either*

$$|A + C||B + D||f(A, B)| \gtrsim |A||B|q,$$

*or*

$$|A + C||B + D||f(A, B)|^2 \gtrsim \frac{|A|^2|B|^2|C||D|}{q},$$

## 2. Preliminaries

In this section we state the definition of degenerate polynomials and preliminary lemmas. The first two can be found in [6], the third one is the so called Schwarz–Zippel lemma, and the last one is a result of Katz [5].

**Definition 2.1.** A polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ is degenerate if it can be written as $Q(L(x, y))$ where $Q$ is an one-variable polynomial and $L$ is a linear form in $x, y$.

**Lemma 2.2.** *Given a non-degenerate polynomial $f(x, y) \in F_q[x, y]$ with degree $k$, then there are at most $k - 1$ elements $a_i$ so that $f(x, y) - a_i$ contains a linear factor.*

**Lemma 2.3.** *Let $f \in F[x_1, ..., x_n]$ be a non zero polynomial with degree $\leq k$. Then*

$$|\{x \in F^n : f(x) = 0\}| \leq k|F|^{n-1}.$$

**Lemma 2.4.** *Let $f \in \mathbb{F}_q[x, y]$ be a non zero polynomial with degree $k$ which does not contain a linear factor. Let $R$ be the set of all roots of $f$ in $\mathbb{F}_q^2$. Then for any $y \neq 0 \in F_q^2$,*