

A MULTI-LINEAR GEOMETRIC ESTIMATE

CHARLOTTE ATEN AND ALEX IOSEVICH

ABSTRACT. We give a generalization of the geometric estimate used by Hart and the second author in their 2008 work on sums and products in finite fields. Their result concerned level sets of non-degenerate bilinear forms over finite fields, while in this work we prove that if $E \subset \mathbb{F}_q^d$ is sufficiently large and ϖ is a non-degenerate multi-linear form then ϖ will attain all possible nonzero values as its arguments vary over E , under a certain quantitative assumption on the extent to which E is projective. We show that our bound is nontrivial in the case that $n = 3$ and $d = 2$ and construct examples of sets to which this applies. In particular, we give conditions under which every member of \mathbb{F}_q^* belongs to $A \cdot A \cdot A + A \cdot A \cdot A \cdot A \cdot A \cdot A$ where A is a union of cosets of a subgroup of \mathbb{F}_q^* .

CONTENTS

1. Introduction	1
2. Proof of the main theorem	4
3. Examples of forms	7
4. Applicability of the main theorem	9
5. A sharp example	10
6. Examples of nontrivial bounds	11
7. Open questions and future prospects	12
References	13

1. INTRODUCTION

One of the key problems of additive number theory is the celebrated sum-product conjecture due to Erdős and Szemerédi. It says that if A is a finite subset of the integers of size n , then either the sumset $A + A := \{a + a' \mid a, a' \in A\}$ or the product set $A \cdot A := \{a \cdot a' \mid a, a' \in A\}$ has size at least $C_\epsilon n^{2-\epsilon}$ for any $\epsilon > 0$. Taking $A = \{1, 2, \dots, n\}$ or $A = \{2^1, 2^2, \dots, 2^n\}$ shows that this estimate is, in general, best possible. In the former case, the sumset is small and the product set is large. In the latter case, it is the other way around. In spite of many decades of efforts by numerous mathematicians, the conjecture is far from being solved, the best known estimate, due to Konyagin and Shkredov[5], being

$$\max(|A + A|, |A \cdot A|) \geq Cn^{\frac{4}{3}+c}$$

for any $c < \frac{5}{9813}$, improving upon a previous breakthrough due to Solymosi[6].

2020 *Mathematics Subject Classification.* 11E20.

Key words and phrases. Multi-linear forms, sum-product conjecture, finite field Fourier analysis.

This problem makes sense in any ring. For example, it has been extensively studied in the setting of finite fields. One of the key objects that arises in the study of this problem is the set

$$A \cdot A + A \cdot A = \{a \cdot a' + b \cdot b' \mid a, a', b, b' \in A\}$$

When $A \subset \mathbb{F}_q$, the finite field with q elements, it is known[4] that $A \cdot A + A \cdot A = \mathbb{F}_q$ if $|A| > q^{\frac{3}{4}}$, and $|A \cdot A + A \cdot A| > \frac{q}{2}$ if $|A| > q^{\frac{2}{3}}$. It is widely conjectured that the latter conclusion should hold if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$, but there has been no progress on this problem since 2008.

The exponents described in the previous paragraph were obtained by taking this one-dimensional problem into two dimensions by considering $E = A \times A$ with $A \subset \mathbb{F}_q$ and considering the following, higher dimensional version of the question. How large does $E \subset \mathbb{F}_q^2$ need to be to ensure that

$$\prod(E) := \{x \cdot y := x_1 y_1 + x_2 y_2 \mid x, y \in E\} = \mathbb{F}_q,$$

or, at least, that $|\prod(E)| > \frac{q}{2}$? The authors in [4] proved that the former conclusion holds if $|E| > q^{\frac{3}{4}}$ and the latter if $|E| > q^{\frac{4}{3}}$, with an additional assumption that holds, for example, if $E = A \times A$. These results can be extended to general non-degenerate quadratic forms (see e.g. [1]).

The purpose of this paper is to generalize the estimates described above to multi-linear forms. This significantly expands the range of geometric applications and allows for interesting interactions of ideas from multi-linear algebra and combinatorial geometry. As a very simple example of the setup we are going to introduce, we will be able to effectively analyze expressions of the form

$$A \cdot A \cdot A + A \cdot A \cdot A$$

along with considerably more complicated objects.

We begin by introducing some terminology pertaining to multi-linear forms.

Definition 1 (Multi-linear form). Given a vector space V over a field \mathbb{F} and some $n \in \mathbb{N}$ we refer to a linear transformation

$$\varpi: V^{\otimes n} \rightarrow \mathbb{F}$$

as a *multi-linear form* (or just as a *form*). More explicitly, we say that ϖ is an *n-linear form on V* , that ϖ has *arity n* , or that ϖ is an *n-form on V* .

Remark 1. Note the distinction between $V^{\otimes n}$, the tensor product of n copies of V , and V^n , the direct product of n copies of V . Recall that given a basis e_1, \dots, e_n of V , the n -fold tensor product of V is generated by

$$e_{i_1} \otimes e_{i_2} \otimes \dots \otimes e_{i_n},$$

where e_{i_j} is one of the basis vectors of V given above.

More precisely, let V and W be vector spaces over the same field. Form a vector space whose formal basis is $V \times W$ (the Cartesian product of the sets V and W). We now form a quotient where we identify (av, w) with (v, aw) , and with $a(v, w)$. The resulting vector space is the tensor product $V \otimes W$ of V and W . This yields a map $\boxtimes: V \times W \rightarrow V \otimes W$ which takes a pair (v, w) to its equivalence class, which we denote by $v \otimes w$. Similarly, given a set of vectors $E \subset V$ we may then form $E^{\boxtimes n}$, which is the image of E^n under the analogous map $V^n \rightarrow V^{\otimes n}$. Note that when the subset E is actually a subspace then both the set $E^{\boxtimes n}$ and the vector

space $E^{\otimes n}$ are defined. In this case we have that $E^{\otimes n}$ is generated by $E^{\boxtimes n}$ but in general $E^{\otimes n}$ contains many more points than $E^{\boxtimes n}$.

When doing calculations with an n -linear form $\varpi: V^{\otimes n} \rightarrow \mathbb{F}$ we often write $\varpi(x_1, \dots, x_n)$ rather than $\varpi(x_1 \otimes \dots \otimes x_n)$. Note that a multi-linear form is an element of the dual space of $V^{\otimes n}$. Multi-linear forms thus inherit the structure of a vector space.

Definition 2 (Space of multi-linear forms). Given a vector space V over a field \mathbb{F} and some $n \in \mathbb{N}$ we denote by $\text{Form}(V, n)$ the dual \mathbb{F} -vector space to $V^{\otimes n}$. That is, $\text{Form}(V, n) := \text{Hom}(V^{\otimes n}, \mathbb{F})$.

We reserve the notation V^* for the set of all nonzero vectors in V , so we will not write V^* to indicate the dual space. In the case that $V = \mathbb{F}_q^d$ for a prime power q we write $\text{Form}(q, d, n) := \text{Form}(\mathbb{F}_q^d, n)$. In this paper we primarily consider forms on finite-dimensional vector spaces over finite fields.

Definition 3 (Level set). Given an \mathbb{F} -vector space V , a form $\varpi \in \text{Form}(V, n)$, $E \subset V$, $t \in \mathbb{F}$ we define the t -level set of ϖ (with respect to E) to be

$$L_t := \left\{ (z, w) \in E^{\boxtimes(n-1)} \times E \mid \varpi(z, w) = t \right\}$$

and we define $\nu(t) := |L_t|$.

The asymmetry between $E^{\boxtimes(n-1)}$ and E in the preceding definition arises from our use of the following transformations.

Definition 4 (Evaluation map). Given a vector space V , some $n \in \mathbb{N}$, some $k \in [n]$, and subspaces $A \leq V^{\otimes(n-1)}$ and $B \leq V$ the k^{th} evaluation map on (A, B) is

$$\text{eval}_{k,A,B}: \text{Form}(V, n) \otimes B \rightarrow \text{Hom}(A, \mathbb{F})$$

is given by

$$(\text{eval}_{k,A,B}(\varpi \otimes y))(x_1, \dots, x_{n-1}) := \varpi(x_1, \dots, x_{k-1}, y, x_{k+1}, \dots, x_{n-1}).$$

We simply write eval_k rather than $\text{eval}_{k,A,B}$ in the case that $A = V^{\otimes(n-1)}$ and $B = V$. Observe that eval_k is the linear transformation given by plugging a vector y into the k^{th} slot of a form ϖ and that a general $\text{eval}_{k,A,B}$ is obtained by restricting this map appropriately. We also define the linear transformation

$$\text{eval}_{k,A,B}^{\varpi}: B \rightarrow \text{Hom}(A, \mathbb{F})$$

by $\text{eval}_{k,A,B}^{\varpi}(y) := \text{eval}_{k,A,B}(\varpi, y)$.

Definition 5 ((A, B) -non-degenerate form). Given a form $\varpi \in \text{Form}(V, n)$ and subspaces $A \leq V^{\otimes(n-1)}$ and $B \leq V$ we say that ϖ is (A, B) -non-degenerate in the k^{th} coordinate when $\text{Ker}(\text{eval}_{k,A,B}^{\varpi}) = 0$.

Example 1 (Ternary dot product). Let $V = \mathbb{F}_q^d$, $A = V^{\otimes(n-1)}$, $B = V$, $n = 3$, and

$$\varpi(x, y, z) = x_1 y_1 z_1 + x_2 y_2 z_2 + \dots + x_d y_d z_d.$$

It is not difficult to see that this form is (A, B) -non-degenerate.

If we keep B the same, change A to $W^{\otimes(n-1)}$, where

$$W = \{ x \in \mathbb{F}_q^d \mid x_1 = 0 \},$$

and use the same form as above, we get an (A, B) -degenerate form.

In the special case that $A = V^{\otimes(n-1)}$ and $B = V$ the condition for (A, B) -non-degeneracy is that $\text{Ker}(\text{eval}_k^\varpi) = 0$. We refer to a form which is $(V^{\otimes(n-1)}, V)$ -non-degenerate simply as a *non-degenerate form*. Similarly, we say that a form ϖ is *degenerate* when ϖ is not non-degenerate. A related notion of degeneracy for multi-linear forms is already present in the literature[3, p.445].

Our results depend on the following parameter measuring the extent to which a set is closed under taking scalar multiples.

Definition 6 (Projective index). Given $E \subset \mathbb{F}_q^d$ we say that E has *projective index* α when

$$\frac{|\{(a, w) \in (\mathbb{F}_q^* \setminus \{1\}) \times \mathbb{F}_q^d \mid w, aw \in E\}|}{(q-2)|E|} \geq \alpha.$$

Note that if E has projective index 1 then E is projective in the sense that $E \cup \{0\}$ is a union of lines through the origin, while any set E has projective index 0.

We now have all the terminology needed to state our generalization of the aforementioned estimate of Hart and the second author.

Theorem 1. Suppose that $\varpi \in \text{Form}(q, d, n)$ for some $n \geq 2$, that $E \subset \mathbb{F}_q^d$, and that E has projective index α . If there exists an r -dimensional subspace A of $(\mathbb{F}_q^d)^{\otimes(n-1)}$ and a subspace B of \mathbb{F}_q^d such that

- (1) $E^{\boxtimes(n-1)} \subset A$,
- (2) $E \subset B$
- (3) ϖ is (A, B) -non-degenerate, and
- (4) $|E| > q^{\frac{r+n-1}{n}} \left(1 - \alpha \left(1 - \frac{2}{q}\right)\right)^{\frac{1}{n}}$

then $\mathbb{F}_q^* \subset \varpi(E^n)$. This bound is sharp.

The proof of the bound is located in [Section 2](#) and a sharp example is located in [Section 5](#).

2. PROOF OF THE MAIN THEOREM

Here we give the proof of [Theorem 1](#) except for the example showing that our result is sharp, which we produce in [Section 5](#).

Proof. We argue the case where ϖ is (A, B) -non-degenerate in the n^{th} coordinate, the other cases being equivalent by symmetry. Let $\chi: \mathbb{F}_q \rightarrow \mathbb{C}$ be a nontrivial additive character. We have that

$$\nu(t) = \sum_{\substack{z \in E^{\boxtimes(n-1)} \\ w \in E}} q^{-1} \sum_{s \in \mathbb{F}_q} \chi(s(\varpi(z, w) - t)).$$

This implies that

$$\nu(t) = q^{-1} |E^{\boxtimes(n-1)}| |E| + R$$

where

$$R := \sum_{\substack{z \in E^{\boxtimes(n-1)} \\ w \in E}} q^{-1} \sum_{s \in \mathbb{F}_q^*} \chi(s(\varpi(x) - t)).$$

View R as a sum in z and apply Cauchy-Schwarz. We obtain

$$\begin{aligned} R^2 &\leq \left| E^{\boxtimes(n-1)} \right| \sum_{z \in E^{\boxtimes(n-1)}} q^{-2} \sum_{s, s' \in \mathbb{F}_q^*} \sum_{w, w' \in E} \chi(s(\varpi(z, w) - t)) \chi(s'(\varpi(z, w') - t)) \\ &\leq \left| E^{\boxtimes(n-1)} \right| \sum_{z \in A} q^{-2} \sum_{s, s' \in \mathbb{F}_q^*} \sum_{w, w' \in E} \chi(s\varpi(z, w) - s'\varpi(z, w')) \chi(t(s' - s)) \\ &= \left| E^{\boxtimes(n-1)} \right| \sum_{z \in A} q^{-2} \sum_{s, s' \in \mathbb{F}_q^*} \sum_{w, w' \in E} \chi(\varpi(z, sw - s'w')) \chi(t(s' - s)). \end{aligned}$$

Define

$$U := \left| E^{\boxtimes(n-1)} \right| \sum_{z \in A} q^{-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in E \\ sw = s'w'}} \chi(\varpi(z, sw - s'w')) \chi(t(s' - s))$$

and

$$V := \left| E^{\boxtimes(n-1)} \right| \sum_{z \in A} q^{-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in E \\ sw \neq s'w'}} \chi(\varpi(z, sw - s'w')) \chi(t(s' - s)).$$

We have that $R^2 \leq U + V$.

In the case of U we have

$$\begin{aligned} U &= \left| E^{\boxtimes(n-1)} \right| q^{-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in E \\ sw = s'w'}} \chi(t(s' - s)) \sum_{z \in A} \chi(\varpi(z, 0)) \\ &= \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in \mathbb{F}_q^d \\ sw = s'w'}} \chi(t(s' - s)) E(w) E(w'), \end{aligned}$$

while in the case of V we have

$$V = \left| E^{\boxtimes(n-1)} \right| q^{-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in E \\ sw \neq s'w'}} \chi(t(s' - s)) \sum_{z \in A} \chi(\varpi(z, sw - s'w')).$$

We use the (A, B) -nondegeneracy of ϖ and orthogonality of χ to obtain $V = 0$ so we are left with $R^2 \leq U$.

We consider separately the summands in U where $s \neq s'$ and where $s = s'$.

Define

$$C := \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in \mathbb{F}_q^d \\ sw = s'w' \\ s \neq s'}} \chi(t(s' - s)) E(w) E(w')$$

and

$$D := \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{s, s' \in \mathbb{F}_q^* \\ w, w' \in \mathbb{F}_q^d \\ sw = s'w' \\ s = s'}} \chi(t(s' - s)) E(w) E(w')$$

so that $U = C + D$.

For C take $a := \frac{s}{s'}$ and $b := s'$ to obtain

$$\begin{aligned} C &= \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{a, b \in \mathbb{F}_q^* \\ w, w' \in \mathbb{F}_q^d \\ a \neq 1 \\ aw = w'}} \chi(tb(1-a)) E(w) E(w') \\ &= \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{(a, w) \in \mathbb{F}_q^* \times \mathbb{F}_q^d \\ a \neq 1}} E(w) E(aw) \sum_{b \in \mathbb{F}_q^*} \chi(tb(1-a)). \end{aligned}$$

From now on we assume that $t \neq 0$. By orthogonality we have that $\chi(tb(1-a)) = -1$ for each $a \in \mathbb{F}_q^*$ with $a \neq 1$ and since E has projective index α we find that

$$\begin{aligned} C &= - \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{\substack{(a, w) \in \mathbb{F}_q^* \times \mathbb{F}_q^d \\ a \neq 1}} E(w) E(aw) \\ &\leq - \left| E^{\boxtimes(n-1)} \right| |E| q^{r-1} \alpha \left(1 - \frac{2}{q} \right). \end{aligned}$$

For D we find that

$$D = \left| E^{\boxtimes(n-1)} \right| q^{r-2} \sum_{(s, w) \in \mathbb{F}_q^* \times \mathbb{F}_q^d} E(w) \leq \left| E^{\boxtimes(n-1)} \right| q^{r-2} |E| q = \left| E^{\boxtimes(n-1)} \right| |E| q^{r-1}.$$

It follows that

$$R^2 \leq U = C + D \leq \left| E^{\boxtimes(n-1)} \right| |E| q^{r-1} \left(1 - \alpha \left(1 - \frac{2}{q} \right) \right)$$

so

$$|R| \leq \left| E^{\boxtimes(n-1)} \right|^{\frac{1}{2}} |E|^{\frac{1}{2}} q^{\frac{r-1}{2}} \left(1 - \alpha \left(1 - \frac{2}{q} \right) \right)^{\frac{1}{2}}.$$

By assumption

$$|E| > q^{\frac{r+n-1}{n}} \left(1 - \alpha \left(1 - \frac{2}{q} \right) \right)^{\frac{1}{n}}$$

and it is the case that $\left| E^{\boxtimes(n-1)} \right| \geq \frac{|E|^{n-1}}{q^{n-2}}$ so we see that

$$|R| \leq \left| E^{\boxtimes(n-1)} \right|^{\frac{1}{2}} |E|^{\frac{1}{2}} q^{\frac{r-1}{2}} \left(1 - \alpha \left(1 - \frac{2}{q} \right) \right)^{\frac{1}{2}} < q^{-1} \left| E^{\boxtimes(n-1)} \right| |E|.$$

Since

$$\nu(t) = q^{-1} \left| E^{\boxtimes(n-1)} \right| |E| + R$$

it must be that $\nu(t) > 0$. Since $\nu(t)$ is the size of the set L_t we have that L_t is nonempty for each $t \neq 0$. That is, $\mathbb{F}_q^* \subset \varpi(E^n)$.

A sharp example is located in [Section 5](#). □

3. EXAMPLES OF FORMS

We provide an alternative description of (A, B) -nondegeneracy in terms of a generalized row space for forms. This will help us manufacture examples of (A, B) -non-degenerate forms. We fix a field \mathbb{F} and denote by e_1, \dots, e_d the standard basis vectors for \mathbb{F}^d .

Definition 7 ((k, A) -row space). Given a form $\varpi \in \text{Form}(\mathbb{F}^d, n)$, some $k \in \mathbb{N}$, and a subspace $A \leq (\mathbb{F}^d)^{\otimes(n-1)}$ we define the (k, A) -row space of ϖ to be

$$\text{Row}_{k,A}(\varpi) := \{ (\text{eval}_k(\varpi, e_1)(x), \dots, \text{eval}_k(\varpi, e_d)(x)) \mid x \in A \}.$$

In the situation that $A = (\mathbb{F}^d)^{\otimes(n-1)}$ we write $\text{Row}_k(\varpi)$ rather than $\text{Row}_{k,A}(\varpi)$ and refer to this space simply as the k -row space of ϖ . This generalizes the usual row space of a matrix in the following sense. Fix some $1 \leq k \leq n$ and consider $\varpi \in \text{Form}(\mathbb{F}^d, n)$. Write ϖ in coordinates as

$$\begin{aligned} \varpi(x_1, \dots, x_n) &= \sum_{i_1, \dots, i_n \in [d]} u_{i_1, \dots, i_n} x_{1, i_1} \cdots x_{n, i_n} \\ &= \sum_{i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_n \in [d]} x_{1, i_1} \cdots x_{k-1, i_{k-1}} x_{k+1, i_{k+1}} \cdots x_{n, i_n} (u_{i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_n} \cdot x_k). \end{aligned}$$

We refer to the vectors $u_{i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_n} \in \mathbb{F}^d$ as the k -rows of ϖ , for the span of these vectors is the k -row space of ϖ .

Proposition 1. *Given a form $\varpi \in \text{Form}(\mathbb{F}^d, n)$ the following are equivalent to the (A, B) -nondegeneracy of ϖ in the k^{th} coordinate:*

- (1) $\text{Ker}(\text{eval}_{k,A,B}^\varpi) = 0$
- (2) *For each $y \in B^*$ we have that $\text{eval}_{k,A,B}^\varpi(y) \neq 0$.*
- (3) *Given $y \in B^*$ there is some $m \in \mathbb{N}$ for which there are $x_{i,j} \in (\mathbb{F}^d)^*$ for $i \in [m]$ and $j \neq k$ such that*

$$\sum_{i=1}^m \varpi(x_{i,1}, \dots, x_{i,k-1}, y, x_{i,k+1}, \dots, x_{i,n}) \neq 0$$

$$\text{and } \sum_{i=1}^m x_{i,1} \otimes \cdots \otimes x_{i,n} \in A^*.$$

- (4) $B \cap (\text{Row}_{k,A}(\varpi))^\perp = 0$

Proof. Recall that (1) was our original definition of (A, B) -nondegeneracy in coordinate k . We have that (2) is equivalent to (1) and also that (3) is equivalent to (2) by unpacking definitions. It remains to show that (2) is equivalent to (4).

Suppose that (4) holds, which means that given any $y \in B^*$ we have that $y \notin (\text{Row}_{k,A}(\varpi))^\perp$ and hence there exists some $u \in \text{Row}_{k,A}(\varpi)$ such that $u \cdot y \neq 0$. Suppose that $y = (y_1, \dots, y_d)$ and

$$u = (\text{eval}_k(\varpi, e_1)(x), \dots, \text{eval}_k(\varpi, e_d)(x))$$

where $x \in A$. We find that

$$\begin{aligned}
0 &\neq u \cdot y \\
&= \sum_{i=1}^d \text{eval}_k(\varpi, e_i)(x) y_i \\
&= \sum_{i=1}^d \text{eval}_k(\varpi, y_i e_i)(x) \\
&= \text{eval}_k(\varpi, y)(x) \\
&= \text{eval}_{k,A,B}^{\varpi}(y)(x),
\end{aligned}$$

which shows that $\text{eval}_{k,A,B}^{\varpi}(y) \neq 0$. Thus, (4) implies (2).

We show that (2) implies (4) by proving the contrapositive. Suppose that there is some $y \in B^*$ such that $y \in (\text{Row}_{k,A}(\varpi))^\perp$. This implies that for every $x \in A$ we have that

$$0 = (\text{eval}_k(\varpi, e_1)(x), \dots, \text{eval}_k(\varpi, e_d)(x)) \cdot y = \text{eval}_{k,A,B}^{\varpi}(y)(x),$$

which means that $\text{eval}_{k,A,B}^{\varpi}(y) = 0$ and hence that (2) fails. \square

We state a couple of corollaries for special cases. The first says that a form is non-degenerate precisely when its row space spans and the second says that a form ϖ is $(A, \text{Row}_{k,A}(\varpi))$ -non-degenerate when the restriction of the usual dot product to $\text{Row}_{k,A}(\varpi)$ is itself a non-degenerate bilinear form.

Corollary 1. *A form $\varpi \in \text{Form}(\mathbb{F}^d, n)$ is non-degenerate in coordinate k if and only if $\text{Row}_k(\varpi) = \mathbb{F}^d$.*

Corollary 2. *Given a form $\varpi \in \text{Form}(\mathbb{F}^d, n)$ and a subspace $A \leq (\mathbb{F}^d)^{\otimes(n-1)}$ we have that ϖ is $(A, \text{Row}_{k,A}(\varpi))$ -non-degenerate if and only if for each $x \in (\text{Row}_{k,A}(\varpi))^*$ we have that there exists some $y \in \text{Row}_{k,A}(\varpi)$ such that $x \cdot y \neq 0$.*

We can obtain forms from n -ary relations on a finite set.

Definition 8 (Form of a relation). Given a relation $\theta \subset S^n$ on a finite set S and a field \mathbb{F} the \mathbb{F} -form of θ , which is $\theta_{\mathbb{F}} \in \text{Form}(\mathbb{F}^S, n)$, is given by

$$\theta_{\mathbb{F}}(x_1, \dots, x_n) := \sum_{s_1, \dots, s_n \in S} 1_{\theta}(s_1, \dots, s_n) x_{1,s_1} \cdots x_{n,s_n}$$

where $1_{\theta}: S^n \rightarrow \mathbb{F}$ is the indicator function of θ .

Of course, given a bijection between S and $[d]$ we can always think of $\theta_{\mathbb{F}}$ as living in $\text{Form}(\mathbb{F}^d, n)$. For forms of the form $\theta_{\mathbb{F}}$ we have an alternative way to check for (A, B) -degeneracy in a component.

Proposition 2. *Given a relation $\theta \subset [d]^n$ we have that if $\theta_{\mathbb{F}}$ is (A, B) -non-degenerate in the k^{th} coordinate and $B \supset \langle e_k \rangle$ then $\pi_k: \theta \rightarrow [d]$ is surjective, where π_k is the k^{th} coordinate projection map.*

Proof. Suppose that π_k is not surjective with $\alpha \in [d] \setminus \text{Im}(\pi_k)$. Consider a k -row $u = u_{i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_n}$. Observe that for any pure tensor $x_1 \otimes \cdots \otimes x_{n-1}$ we have that $\text{eval}_k(\theta_{\mathbb{F}}, \alpha)(x_1, \dots, x_{n-1}) = 0$, from which it follows that $\text{eval}_k(\theta_{\mathbb{F}}, \alpha) = 0$. This implies that $\langle e_k \rangle \in (\text{Row}_{A,k}(\theta_{\mathbb{F}}))^\perp$. Thus, if $B \supset \langle e_k \rangle$ then we have that $B \cap (\text{Row}_{A,k}(\theta_{\mathbb{F}}))^\perp \neq 0$, which by the previous proposition shows that $\theta_{\mathbb{F}}$ is not (A, B) -non-degenerate in coordinate k , establishing the contrapositive of our claim. \square

Note that the preceding result places no restriction on A whatsoever.

The converse to this proposition is false in general. Take $A \leq (\mathbb{F}^d)^{\otimes(n-1)}$, take $B \leq \mathbb{F}^d$ with $B \cap \langle(1, \dots, 1)\rangle^\perp \neq 0$, and consider the relation $\theta = [d]^n$. Although $\pi_k: \theta \rightarrow [d]$ is indeed surjective we have that $\text{Row}_{k,A}(\varpi) \leq \langle(1, \dots, 1)\rangle$ so $(\text{Row}_{k,A}(\varpi))^\perp \geq \langle(1, \dots, 1)\rangle^\perp$. This implies that $B \cap (\text{Row}_{k,A}(\varpi))^\perp \neq 0$ so we find that ϖ is (A, B) -degenerate. We do have a partial converse, however.

Proposition 3. *Given a relation $\theta \subset [d]^n$ we have that if $\pi_k: \theta \rightarrow [d]$ is a bijection and for each $\alpha \in [d]$ the subspace $A \leq (\mathbb{F}^d)^{\otimes(n-1)}$ contains*

$$e_{i_1} \otimes \dots \otimes e_{i_{k-1}} \otimes e_{i_{k+1}} \otimes \dots \otimes e_{i_n}$$

when $(i_1, \dots, i_{k-1}, \alpha, i_{k+1}, \dots, i_n) = \pi_k^{-1}(\alpha)$ then $\theta_{\mathbb{F}}$ is (A, B) -non-degenerate in the k^{th} coordinate.

Proof. It suffices to show that $\text{Row}_{k,A}(\theta_{\mathbb{F}})$ contains each standard basis element e_α for $\alpha \in [d]$. Let $(i_1, i_2, \dots, i_{k-1}, i_{k+1}, \dots, i_n) = \pi_k^{-1}(\alpha)$. It follows that $\text{Row}_{k,A}(\theta_{\mathbb{F}})$ contains

$$(\text{eval}_k(\theta_{\mathbb{F}}, e_1)(\pi_k^{-1}(\alpha)), \dots, \text{eval}_k(\theta_{\mathbb{F}}, e_d)(\pi_k^{-1}(\alpha))) = e_\alpha$$

as desired. \square

Note that the preceding result places no restriction on B whatsoever.

4. APPLICABILITY OF THE MAIN THEOREM

Although the statement of [Theorem 1](#) refers to a wide range of possible arities n and dimensions d , we will see that this result is vacuous in a nontrivial way for many values of n and d .

Proposition 4. *Consider the case of our [Theorem 1](#) when $\dim(\text{Span}(E)) = \ell$ and $r = \ell^{n-1}$. We have that [Theorem 1](#) is vacuously true unless*

- (1) $\ell = 1$,
- (2) $n = 2$, or
- (3) $n = 3$ and $\ell = 2$.

Proof. Suppose that $B = \text{Span}(E)$, $A = B^{\otimes(n-1)}$, and $\dim(B) = \ell$. We have that $|E| \leq q^\ell$ since $E \subset B \cong \mathbb{F}_q^\ell$. If the estimate in [Theorem 1](#) holds then then

$$q^{\frac{\ell^{n-1} + n - 1}{n}} \left(1 - \alpha \left(1 - \frac{2}{q}\right)\right)^{\frac{1}{n}} < |E| \leq q^\ell.$$

This implies that

$$\ell^{n-1} - n\ell + n < 2 - \log_q(q - \alpha(q - 2)).$$

It is only the case that $\ell^{n-1} - n\ell + n < 2$ when

- (1) $\ell = 1$,
- (2) $n = 2$, or
- (3) $n = 3$ and $\ell = 2$.

Otherwise, the result is vacuously true since no set $E \subset \mathbb{F}_q^d$ can satisfy the relevant bound. \square

By restricting the form ϖ to $B^{\otimes n}$ the preceding proposition effectively says that the only cases of interest are when $d = 1$ (which is relatively trivial), $n = 2$ (for which we give a result which is basically that of Hart and the second author[4] incorporating the projective index α), and $n = 3$ and $d = 2$.

In this last case it is certainly possible for a set $E \subset \mathbb{F}_q^2$ to fail to satisfy the bound in question, as the following example shows.

Example 2. Let A be the subgroup of \mathbb{F}_q^* of order $\frac{q-1}{2}$ and take $E := A^2$. We have that $|E| = \frac{1}{4}(q-1)^2$ and that E has projective index $\frac{q-3}{2(q-2)}$. We would have that $\varpi(E^3) \supset \mathbb{F}_q^*$ for any non-degenerate form ϖ if

$$\frac{1}{64}(q-1)^6 = |E|^3 > q^6 \left(1 - \frac{q-3}{2(q-2)} \left(1 - \frac{2}{q}\right)\right) = \frac{1}{2}q^6 + \frac{3}{2}q^5.$$

When $n = 3$ and $d = 2$ our theorem applies only for

$$\alpha > \frac{q^6 - |E|^3}{q^6 - 2q^5}$$

and hence only for sets $E \subset \mathbb{F}_q^2$ with $|E| > \sqrt[3]{2}q^{\frac{5}{3}}$. That is, **Theorem 1** cannot say anything about sets E with $|E| \leq \sqrt[3]{2}q^{\frac{5}{3}}$, independent of the projective index α .

5. A SHARP EXAMPLE

We show that **Theorem 1** gives a sharp bound by considering a non-degenerate form $\varpi \in \text{Form}(q, d, n)$ and $E \subset \mathbb{F}_q^d$ with $E^{\boxtimes(n-1)} \subset A$, $E \subset B$, and $|E| \approx q^{\frac{r+n-1}{n}}$ such that $\varpi(E^{\boxtimes n}) \not\supset \mathbb{F}_q^*$. That is, considering the projective index α to be a constant independent of q we have that the factor $1 - \alpha \left(1 - \frac{2}{q}\right) = O(1)$ so we can absorb it as a constant.

Let $n = 3$ and $d = 2$ and fix $s \in \mathbb{N}$. Take q as large as possible so that $s \mid (q-1)$ and not every element of \mathbb{F}_q^* can be written as a sum of two nonzero s^{th} powers. Let Γ be the multiplicative subgroup of \mathbb{F}_q^* of order $\frac{q-1}{s}$ and note that since Γ consists of the nonzero s^{th} powers in \mathbb{F}_q we have that $\Gamma + \Gamma \not\supset \mathbb{F}_q^*$ where

$$\Gamma + \Gamma := \{ \gamma_1 + \gamma_2 \mid \gamma_1, \gamma_2 \in \Gamma \}.$$

Define $E := \Gamma^2$. We have that $r = \dim((\mathbb{F}_q^2)^{\otimes(3-1)}) = 4$ so

$$|E| = \left(\frac{q-1}{s}\right)^2 \approx q^2 = q^{\frac{4+3-1}{3}} = q^{\frac{r+n-1}{n}}$$

Take $\theta := \{(1, 1, 1), (2, 2, 2)\} \subset [2]^3$ and define $\varpi := \theta_{\mathbb{F}_q}$. We have that ϖ is non-degenerate in coordinate 3, yet

$$\varpi(E^{\boxtimes 3}) = \Gamma + \Gamma \not\supset \mathbb{F}_q^*,$$

demonstrating that **Theorem 1** is sharp. This is really little more than the assertion that up to the highest-order term the bound in our main theorem for the case $n = 3$ and $d = 2$ cannot be improved beyond the trivial bound of “approximately all of \mathbb{F}_q^2 ”. However, in the preceding section we give examples of nontrivial application of our theorem when taking the term $1 - \alpha \left(1 - \frac{2}{q}\right)$ into account.

6. EXAMPLES OF NONTRIVIAL BOUNDS

We consider the following family of sets in this section.

Definition 9 (Omphalos). We say that a set $E \subset \mathbb{F}_q^2$ is a (q, k, ℓ) -omphalos when

$$E = \bigcup_{h \in H} E_h$$

where H is a set of k distinct lines through the origin in \mathbb{F}_q^2 and each E_h consists of exactly ℓ nonzero points from h .

Our bound for the $n = 3$ and $d = 2$ case may be made more succinct when E is a (q, k, ℓ) -omphalos.

Proposition 5. *Suppose that E is a (q, k, ℓ) -omphalos and that ϖ is a non-degenerate ternary form on \mathbb{F}_q^2 . If*

$$k^3 \ell^3 > q^6 - (\ell - 1)q^5$$

then $\varpi(E^2) \supset \mathbb{F}_q^$.*

Proof. Apply [Theorem 1](#) to E in the case that

$$\alpha := \frac{\ell - 1}{q - 2}.$$

Since $|E| = k\ell$ cubing the bound

$$|E| > q^2 \left(1 - \alpha \left(1 - \frac{2}{q} \right) \right)^{\frac{1}{3}}$$

yields the desired inequality. \square

Omphaloi may be constructed from cosets of multiplicative subgroups of \mathbb{F}_q^* .

Example 3. Let Γ be a subgroup of \mathbb{F}_q^* of order $\frac{q-1}{s}$ and take $H \subset \mathbb{F}_q^*$ where $|H| = r$ and if $h_1, h_2 \in H$ with $h_1 \neq h_2$ then $h_1\Gamma \neq h_2\Gamma$. That is, let H consist of representatives of r distinct cosets of Γ . Define

$$E := \{ x(1, y) \in \mathbb{F}_q^2 \mid x, y \in H\Gamma \}.$$

Note that Γ is a (q, k, l) -omphalos where

$$k = l = \frac{r(q-1)}{s}.$$

As a corollary to [Proposition 5](#) we have the special case where E is as in the above example.

Corollary 3. *Taking E from [Example 3](#) we have that if*

$$(q-1)^6 r^6 + (q-1)s^5 q^5 r - s^6(q^6 + q^5) > 0$$

and ϖ is a non-degenerate ternary form on \mathbb{F}_q^2 then $\mathbb{F}_q^ \subset \varpi(E^3)$.*

We illustrate the application of this corollary in our last example. Further discussion of this particular case appears in the subsequent section.

Example 4. Consider the set $E \subset \mathbb{F}_q^2$ from [Example 3](#) where $q = 160001$, $s = 20$, and $r = 16$ and take ϖ to be the ternary dot product from [Example 1](#). Since

$$(q-1)^6 r^6 + (q-1)s^5 q^5 r - s^6(q^6 + q^5) > 0$$

in this case and ϖ is non-degenerate we have that every nonzero member of \mathbb{F}_q^* may be written as

$$\varpi(h_1\gamma_1(1, h_2\gamma_2), h_3\gamma_3(1, h_4\gamma_4), h_5\gamma_5(1, h_6\gamma_6))$$

where the h_i are from a fixed set H consisting of $r = 16$ coset representatives of the subgroup Γ of \mathbb{F}_q^* of order $\frac{q-1}{s} = 8000$ and the γ_i are members of Γ . Thus, each member of \mathbb{F}_q^* is of the form

$$h_1 h_3 h_5 \psi_1 (1 + h_2 h_4 h_6 \psi_2)$$

where ψ_1 and ψ_2 are 20^{th} powers in \mathbb{F}_q and the h_i belong to H . This also implies that each member of \mathbb{F}_q^* can be written as

$$h_1\gamma_1 h_3\gamma_3 h_5\gamma_5 + h_1\gamma_1 h_2\gamma_2 h_3\gamma_3 h_4\gamma_4 h_5\gamma_5 h_6\gamma_6$$

and hence that

$$A \cdot A \cdot A + A \cdot A \cdot A \cdot A \cdot A \cdot A \supset \mathbb{F}_q^*$$

when $A = H\Gamma$.

7. OPEN QUESTIONS AND FUTURE PROSPECTS

In this section we describe some open problems that arose from this paper and some possible extensions of these results.

- In [Section 4](#) we note that the only nontrivial cases in which our result can apply are the cases where $n = 2$ or when both $n = 3$ and $d = 2$. What further assumptions on E or ϖ might yield nontrivial bounds for other values of n and d ? Are there useful applications of our stronger result in the $n = 2$ along the lines of what was done in [\[4\]](#)?
- A natural multi-linear form that falls within the scope of our results is $\det(x^1, x^2, \dots, x^d)$ where $x^j \in \mathbb{F}_q^d$. This form was studied systematically in [\[2\]](#) under a variety of structural assumptions on the underlying set E . Using the main result of this paper, we obtain similar exponents under different structural assumptions having to do with tensor products. It would be very interesting to reconcile and unify these results, particularly in the context of a regime that takes us beyond the $n = 3$ and $d = 2$ case.
- Although [Section 5](#) shows that in general [Theorem 1](#) gives us a bound on the order of q^2 in the case that $n = 3$ and $d = 2$, it is natural to wonder whether the bound given in [Corollary 3](#) is the best possible. That is, given a prime q and $s \mid q-1$ let $f(q, s)$ be the least $r \in \mathbb{N}$ such that

$$(q-1)^6 r^6 + (q-1)s^5 q^5 r - s^6(q^6 + q^5) > 0$$

and let $g(q, s)$ be the least r such that for any non-degenerate ternary form ϖ on \mathbb{F}_q^2 we have that $\mathbb{F}_q^* \subset \varpi(E^3)$ where E is as in [Example 3](#) for any possible choice of coset representative H of size r . Necessarily we have that $f(q, s) \geq g(q, s)$, but how much smaller can $g(q, s)$ be in general?

REFERENCES

- [1] Michael Bennett et al. “Group actions and geometric combinatorics in \mathbb{F}_q^d ”. In: *Forum Math.* 29.1 (2017), pp. 91–110. ISSN: 0933-7741.
- [2] David Covert et al. “Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields”. In: *European J. Combin.* 31.1 (2010), pp. 306–319. ISSN: 0195-6698.
- [3] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. 233 Spring Street, New York, NY 10013, USA: Birkhäuser Boston, 2008. ISBN: 978-0-8176-4770-4.
- [4] Derrick Hart and Alex Iosevich. “Sums and products in finite fields: an integral geometric viewpoint”. In: *Radon transforms, geometry, and wavelets*. Vol. 464. Contemp. Math. Providence, RI: Amer. Math. Soc., 2008, pp. 129–135.
- [5] S. V. Konyagin and I. D. Shkredov. “New results on sums and products in \mathbb{R} ”. In: *Tr. Mat. Inst. Steklova* 294. Sovremennye Problemy Matematiki, Mekhaniki i Matematicheskoi Fiziki. II (2016). English version published in Proc. Steklov Inst. Math. 294 (2016), no. 1, 78–88, pp. 87–98. ISSN: 0371-9685.
- [6] József Solymosi. “Bounding multiplicative energy by the sumset”. In: *Adv. Math.* 222.2 (2009), pp. 402–408. ISSN: 0001-8708.

MATHEMATICS DEPARTMENT, UNIVERSITY OF ROCHESTER, ROCHESTER 14627, USA
 URL: <http://aten.cool>
 Email address: charlotte.aten@rochester.edu

MATHEMATICS DEPARTMENT, UNIVERSITY OF ROCHESTER, ROCHESTER 14627, USA
 URL: <https://people.math.rochester.edu/faculty/iosevich/>
 Email address: alex.iosevich@rochester.edu