Sums and products in finite fields: an integral geometric viewpoint

Derrick Hart and Alex Iosevich

June 15, 2007

Abstract

We prove that if $A \subset \mathbb{F}_q$ is such that

$$|A| > q^{\frac{1}{2}+\frac{1}{2d}},$$

then

$$\mathbb{F}_q^* \subset dA^2 = A^2 + \cdots + A^2 \quad d \text{ times},$$

where

$$A^2 = \{a \cdot a' : a, a' \in A\},$$

and where $\mathbb{F}_q^*$ denotes the multiplicative group of the finite field $\mathbb{F}_q$. In particular, we cover $\mathbb{F}_q^*$ by $A^2 + A^2$ if $|A| > q^{\frac{3}{4}}$. Furthermore, we prove that if

$$|A| \geq C_{size}^{\frac{1}{d}} q^{\frac{1}{2}+\frac{1}{2(2d-1)}},$$

then

$$|dA^2| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + 1}.$$

Thus dA^2 contains a positive proportion of the elements of $\mathbb{F}_q$ under a considerably weaker size assumption.

We use the geometry of $\mathbb{F}_q^d$, averages over hyper-planes and orthogonality properties of character sums.

Contents

1 Introducion

A classical problem in additive number theory is to determine, given a finite subset A of a ring, whether both $2A = \{a + a' : a, a' \in A\}$ and $A^2 = \{a \cdot a' : a, a' \in A\}$ be small in a suitable sense. A related question, posed in a finite field $\mathbb{F}_q$ with q elements, is how large $A \subset \mathbb{F}_q$ need to be to assure that $dA^2 = A^2 + A^2 + \cdots + A^2 = \mathbb{F}_q$. It is known (see e.g. [6]) that if $d = 3$ and q is prime, this conclusion is assured if $|A| \geq Cq^{\frac{3}{4}}$, with a sufficiently large constant $C > 0$. It is reasonable to conjecture that if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$, then $2A^2 = \mathbb{F}_q$. This result cannot hold, especially in the setting of general finite fields if $|A| = \sqrt{q}$ because A may in fact be a subfield. See also [1], [3], [5], [4], [8], [10], [12], [13] and the references contained therein on recent progress related to this problem and its analogs.

The purpose of this paper is to use the geometry of $\mathbb{F}_q^d$ to deduce a good lower bound on the size of A that guarantees that $dA^2 = \mathbb{F}_q$, with the possible exception of 0. Our main result is the following.

Theorem 1.1. *Let $A \subset \mathbb{F}_q$, where $\mathbb{F}_q$ is an arbitrary finite field with q elements, such that $|A| > q^{\frac{1}{2}+\frac{1}{2d}}$. Then*

$$\mathbb{F}_q^* \subset dA^2. \tag{1.1}$$

Suppose that

$$|A| \geq C_{size}^{\frac{1}{d}} q^{\frac{1}{2}+\frac{1}{2(2d-1)}}.$$

Then

$$|dA^2| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + 1}. \tag{1.2}$$

In particular, if $d = 2$,

$$\mathbb{F}_q^* \subset A^2 + A^2$$

if

$$|A| > q^{\frac{3}{4}},$$

and

$$|A^2 + A^2| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + 1}$$

if

$$|A| \geq C_{size}^{\frac{1}{2}} q^{\frac{2}{3}}.$$

Also, Theorem 1.1 gives an explicit bound for the conjecture mentioned in [6], namely that if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$, there exists $d = d(\epsilon)$ such that dA^2 covers $\mathbb{F}_q$. In view of this, we restate Theorem 1.1 as follows.

Theorem 1.2. *Let $A \subset \mathbb{F}_q$, where $\mathbb{F}_q$ is an arbitrary finite field with q elements, such that*

$$|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon},$$

for some $\epsilon > 0$. Then (1.1) holds for $d = d(\epsilon)$ equal to the smallest integer greater than or equal to $\frac{1}{2\epsilon}$. Moreover, (1.2) holds if d is equal to the smallest integer greater than or equal to $\frac{1}{2} + \frac{1}{4\epsilon}$.

Throughout the paper, $X \lesssim Y$ means that there exists a universal constant C, indepedent of q, such that $X \leq CY$, and $X \approx Y$ means that $X \lesssim Y$ and $Y \lesssim X$. In the instances when the size of the constant matters, this fact shall be mentioned explicitly.

Remark 1.3. The reader can easily check that in Theorem 1.1 and Theorem 1.2, dA^2 may be easily replaced by

$$A_1 \cdot B_1 + \cdots + A_d \cdot B_d,$$

provided that

$$\Pi_{j=1}^d |A_j||B_j| \geq Cq^{d+1}$$

with a sufficiently large constant $C > 0$.

The proof of Theorem 1.1 is based on the following geometric observation that is interesting in its own right.

Theorem 1.4. *Let $E \subset \mathbb{F}_q^d$ such that $|E| > q^{\frac{d+1}{2}}$. Then*

$$\mathbb{F}_q^* \subset \{x \cdot y : x, y \in E\}.$$

To prove Theorem 1.1 we shall need the following conditional version of Theorem 1.4.

Theorem 1.5. *Let $E \subset \mathbb{F}_q^d$ such that*

$$|E \cap l_y| \leq C_{geom} q^{\frac{\alpha}{d}}$$

for some $0 \leq \alpha \leq d$, for every $y \in \mathbb{F}_q^d$, $y \neq (0, \dots, 0)$, where

$$l_y = \{ty : t \in \mathbb{F}_q\}.$$

Suppose that

$$|E| \geq C_{size} q^{\frac{d}{2}+\frac{\alpha}{2d}}.$$

Then

$$|\{x \cdot y : x, y \in E\}| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + C_{geom}}.$$

Remark 1.6. Theorem 1.5 has non-trivial applications to many other problems in additive number theory and geometric combinatorics, such as the Erdős distance problem, distribution of simplexes and others. We study these problems systematically in [7].

1.1 Integral geometric viewpoint

At the core of the proof of Theorem 1.4 and Theorem 1.5 is the $L^2(\mathbb{F}_q^d)$ estimate for the "rotating planes" operator

$$\mathcal{R}_t f(x) = \sum_{x \cdot y = t} f(y).$$

In the Euclidean space, this operator is a classical example of a phenomenon, thoroughly explored by Hormander, Phong, Stein and others (see e.g. [11]) and the references contained therein) where an operator that averages a function over a family of manifolds satisfies better than trivial bounds on $L^2(\mathbb{F}_q^d)$ provided that the family of manifolds satisfies an appropriate curvature condition. It turns out that in the finite field setting, the aforementioned operator, suitably interpreted, satisfies analogous bounds which lead to interesting arithmetic consequences.

In contrast, the authors of [8] took advantage of the $L^2(\mathbb{F}_q^d)$ mapping properties of the operator

$$H_j f(x) = \sum_{y_1 y_2 = j} f(x - y),$$

and in [9] the underlying operator is

$$A_t f(x) = \sum_{y_1^2 + \cdots + y_d^2 = t} f(x - y),$$

though in neither paper was this perspective made explicit. These examples suggest that systematic theory of Fourier Integral Operator in the setting of vector spaces over finite fields needs to be worked out and the authors shall take up this task in a subsequent paper.

1.2 Fourier analysis used in this paper

Let $f : \mathbb{F}_q^d \to \mathbb{C}$. Let χ be a non-trivial additive character on $\mathbb{F}_q$. Define the Fourier transform of f by the formula

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x)$$

for $m \in \mathbb{F}_q^d$.

The formulas we shall need are the following:

$$\sum_{t \in \mathbb{F}_q} \chi(-at) = 0 \quad \text{(orthogonality)},$$

if $t \neq 0$, and q otherwise,

$$f(x) = \sum_m \chi(x \cdot m) \widehat{f}(m) \quad \text{(inversion)},$$

$$\sum_m \widehat{f}(m)\overline{\widehat{g}(m)} = q^{-d} \sum_x f(x)g(x) \quad \text{(Plancherel/Parseval).}$$

In the case when q is a prime, one may take $\chi(t) = e^{\frac{2\pi i}{q}t}$, and in the general case the formula is only slightly more complicated.

1.3 Acknowledgements:

The authors wish to thank Moubariz Garaev, Nets Katz, Sergei Konyagin and Ignacio Uriarte-Tuero for a thorough proofreading of the earlier drafts of this paper and for many interesting and helpful remarks.

2 Proof of the basic geometric estimate (Theorem 1.4)

Let
$$\nu(t) = |\{(x,y) \in E \times E : x \cdot y = t\}|.$$

We have
$$\nu(t) = \sum_{x,y \in E} q^{-1} \sum_{s \in \mathbb{F}_q} \chi(s(x \cdot y - t)),$$
where χ is a non-trivial additive character on $\mathbb{F}_q$. It follows that
$$\nu(t) = |E|^2 q^{-1} + R,$$
where
$$R = \sum_{x,y \in E} q^{-1} \sum_{s \neq 0} \chi(s(x \cdot y - t)).$$

Viewing R as a sum in x, applying the Cauchy-Schwartz inequality and dominating the sum over $x \in E$ by the sum over $x \in \mathbb{F}_q^d$, we see that
$$R^2 \leq |E| \sum_{x \in \mathbb{F}_q^d} q^{-2} \sum_{s,s' \neq 0} \sum_{y,y' \in E} \chi(sx \cdot y - s'x \cdot y')\chi(t(s'-s)).$$

Orthogonality in the x variable yields
$$= |E| q^{d-2} \sum_{\substack{sy = s'y' \\ s,s' \neq 0}} \chi(t(s'-s))E(y)E(y').$$

If $s \neq s'$ we may set $a = s/s', b = s'$ and obtain
$$|E| q^{d-2} \sum_{\substack{y \neq y' \\ ay = y' \\ a \neq 1, b}} \chi(tb(1-a))E(y)E(y')$$

$$= -|E|q^{d-2} \sum_{y \neq y', a \neq 1} E(y)E(ay),$$

and the absolute value of this quantity is

$$\leq |E|q^{d-2} \sum_{y \in E} |E \cap l_y|$$

$$\leq |E|^2 q^{d-1},$$

since

$$|E \cap l_y| \leq q$$

by the virtue of the fact that each line contains exactly q points.

If $s = s'$ we get

$$|E|q^{d-2} \sum_{s,y} E(y) = |E|^2 q^{d-1}.$$

It follows that

$$\nu(t) = |E|^2 q^{-1} + R(t),$$

where

$$R^2(t) \leq -Q(t) + |E|^2 q^{d-1},$$

with

$$Q(t) \geq 0.$$

It follows that

$$R^2(t) \leq |E|^2 q^{d-1},$$

so

$$|R(t)| \leq |E| q^{\frac{d-1}{2}}. \tag{2.1}$$

We conclude that

$$\nu(t) = |E|^2 q^{-1} + R(t)$$

with $|R(t)|$ bounded as in (2.1).

This quantity is strictly positive if $|E| > q^{\frac{d+1}{2}}$ with a sufficiently large constant $C > 0$. This completes the proof of Theorem 1.4. Theorem 1.1 follows from Theorem 1.4 by simply setting $E = A \times A \times \cdots \times A$.

3 Proof of the enhanced geometric estimate (Theorem 1.5)

Assume throughout the argument, without loss of generality,that E does not contain the origin. Applying Cauchy-Schwartz as above we see that

$$\nu(t) \le |E| \sum_{x \in E} \sum_{y,y' \in E} q^{-2} \sum_{s,s'} \chi(x \cdot (sy - s'y'))\chi(t(s'-s)).$$

It follows that

$$\sum_t \nu(t) \le |E| q^{d-1} \sum_{s \ne 0} \sum_m \widehat{E}(sm) \sum_{y-y'=m} E(y)E(y')$$

$$= |E| q^{d-1} \sum_s \sum_m \widehat{E}(ms) E * E(m)$$

$$= |E| q^{d-1} \sum_m \left(\sum_s \widehat{E}(sm) \right) E * E(m). \tag{3.1}$$

Now,

$$\sum_s \widehat{E}(ms) = \sum_s q^{-d} \sum_x E(x)\chi(-x \cdot ms)$$

$$= q^{-(d-1)} \sum_{x \cdot m = 0} E(x).$$

Inserting this it into (3.1) we get

$$|E| \sum_m \left(\sum_{x \cdot m = 0} E(x) \right) \cdot E * E(m). \tag{3.2}$$

Let

$$F(m) = \sum_{x \cdot m = 0} E(x), \quad G(m) = E * E(m).$$

By a direct calculation,

$$\widehat{G}(k) = q^d |\widehat{E}(k)|^2.$$

On the other hand,

$$\widehat{F}(k) = q^{-d} \sum_m \chi(-m \cdot k) \sum_{x \cdot m = 0} E(x)$$

$$= q^{-d} q^{-1} \sum_{m,x} \sum_s \chi(-m \cdot k + sx \cdot m) E(x)$$

$$= q^{-d}q^{-1}\sum_{m,x}\sum_{s\neq 0}\chi(-m\cdot k+sx\cdot m)E(x)$$

$$= q^{-1}\sum_{s\neq 0}E(s^{-1}k)$$

$$= q^{-1}\sum_{s\neq 0}E(sk) = q^{-1}|E\cap l_k|,$$

if $k\neq(0,\dots,0)$ and

$$q^{-1}|E|,$$

if $k=(0,\dots,0)$.

Rewriting (3.2) and applying the Parseval identity we get

$$|E|\sum_m F(m)G(m) = |E|q^d\sum_k \widehat{F}(k)\overline{\widehat{G}(k)}$$

$$= |E|q^{2d-1}\sum_{k\neq(0,\dots,0)}|E\cap l_k||\widehat{E}(k)|^2 + |E|q^{2d-1}\cdot|E|\cdot q^{-2d}|E|^2$$

$$\leq C_{geom}|E|q^{2d-1}q^{\frac{\alpha}{d}}q^{-d}|E| + |E|^4q^{-1}C_{geom}|E|^2q^{d-1+\frac{\alpha}{d}} + |E|^4q^{-1}.$$

Since

$$|E|^4 = \left(\sum_t \nu(t)\right)^2 \leq |\{x\cdot y : x,y\in E\}|\cdot\sum_t \nu^2(t)$$

$$\leq |\{x\cdot y : x,y\in E\}|\left(C_{geom}|E|^2q^{d-1+\frac{\alpha}{d}} + |E|^4q^{-1}\right),$$

it follows that

$$|\{x\cdot y : x,y\in E\}| \geq q\cdot\frac{|E|^2}{C_{geom}q^{d+\frac{\alpha}{d}}+|E|^2} = r_q\cdot q. \tag{3.3}$$

Suppose that

$$|E|\geq C_{size}q^{\frac{d}{2}+\frac{\alpha}{2d}}.$$

It follows that

$$r_q \geq \frac{C_{size}^2}{C_{size}^2+C_{geom}},$$

as desired.

4 Proof of the main arithmetic result (Theorem 1.1)

Let $E = A \times A \times \cdots \times A$. The proof of the first part of Theorem 1.1 follows instantly. To prove the second part observe that

$$|E \cap l_y| \leq |A| = |E|^{\frac{1}{d}}$$

for every $y \in E$.

Then the line (3.3) takes the form

$$|\{(x \cdot y : x, y \in E\}| \geq q \cdot \frac{|E|^2}{q^d \cdot |E|^{\frac{1}{d}} + |E|^2}.$$

The proof of Theorem 1.5 tells us at this point that

$$|\{x \cdot y : x, y \in E\}| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + 1}$$

if

$$|E| \geq C_{size} q^{\frac{d}{2} + \frac{d}{2(2d-1)}}.$$

It follows that if

$$|A| \geq C_{size}^{\frac{1}{d}} q^{\frac{1}{2} + \frac{1}{2(2d-1)}},$$

then

$$|dA^2| \geq q \cdot \frac{C_{size}^2}{C_{size}^2 + 1}$$

as desired. This completes the proof of Theorem 1.1.

References

[1] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), 380-398.

[2] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Func. Anal. **14** (2004) 27-57.

[3] E. Croot, *Sums of the Form* $1/x_1^k + \dots 1/x_n^k$ *modulo a prime*, Integers **4** (2004).

[4] M. Garaev, *The sum-product estimate for large subsets of prime fields*, (preprint), (2007).

[5] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erds-Graham problem*, Mat. Zametki, **79** (2006), 384-395; translation in: Math. Notes **79** (2006), 356-365.

[6] A. Glibichuk and S. Konyagin, *Additive properties of product sets in fields of prime order*, Centre de Recherches Mathematiques, Proceedings and Lecture Notes, (2006).

[7] D. Hart, A. Iosevich and M. Rudnev, *Erdős distance problem on arithmetic varieties and connection with sums and products in finite fields*, in preparation, (2007).

[8] D. Hart, A. Iosevich and J. Solymosi, *Sums and products in finite fields via Kloosterman sums*, IMRN (to appear), (2007).

[9] A. Iosevich and M. Rudnev, *Erdös distance problem in vector spaces over finite fields*, TAMS, (to appear), (2007).

[10] Nets Hawk Katz and Chun-Yen Shen, *Garaev's Inequality in finite fields not of prime order*, (preprint), (2007).

[11] E. Stein, *Harmonic Analysis*, Princeton University Press, (1993).

[12] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press, (2006).

[13] V. Vu, *Sum-Product estimates via directed expanders*, (preprint), (2007).