An improved estimate on sums of product sets

Misha Rudnev*

May 17, 2008

Abstract

In a recent paper [2] A. Glibichuk proved that if $A, B$ are subsets of an arbitrary finite filed $\mathbb{F}_q$, such that $|A||B| > q$, then $16AB = \mathbb{F}_q$. We improve this to $10AB = \mathbb{F}_q$.

Let $\mathbb{F}_q$ be a finite field of $q$ elements. As usual, for $A, B \subseteq \mathbb{F}_q$, $\xi \in \mathbb{F}_q^*$, where $\mathbb{F}_q^*$ stands for the multiplicative group of $\mathbb{F}_q$, we denote

$$A + B = \{a + b : a \in A, b \in B\}, \quad AB = \{ab : a \in A, b \in B\},$$

$$\xi B = \{\xi b : b \in B\}, \quad -A = \{-1\}A, \quad dA = A + \ldots + A, \quad \text{d times}$$

for $d \in \mathbb{N}$. The main results of this note are as follows.

**Theorem 1** Let $A, B \subseteq \mathbb{F}_q$, such that the product of their cardinalities $|A||B| > q$. Then $10AB = \mathbb{F}_q$.

Theorem [1] is an improvement on a recent result of Glibichuk [2] who showed $16AB = \mathbb{F}_q$ as a consequence of a stronger claim $8AB = \mathbb{F}_q$ if one of the sets $A, B$ is symmetric or antisymmetric (which also implies that $8AB = \mathbb{F}_q$ as long as $|A||B| \geq 2q$.) Our claim is based on one simple observation and a slightly more elaborate use of symmetry. The constant 10 regarding $10AB = \mathbb{F}_q$ is unlikely to be optimal. A more general question is: under the assumption $|A||B| > (1 + c)q$, what is the smallest integer $d(c)$ so that $dAB$ cover a fraction $\frac{1}{c(1)}$ of elements of $\mathbb{F}_q^*$? One is tempted to believe that $d = 2$ should not generally suffice for $c = o(1), C = O(1)$ yet we are unaware of constructive evidence to this. D. Hart and A. Iosevich [3] conjectured that in the case $A = B$, the condition $|A| \geq C_0q^{2+c}$ should suffice for $2A^2$ to cover the whole of $\mathbb{F}_q$.

Geometrically the integer $d$ has the meaning of the dimension, so that $d$-dimensional Cartesian products $A_d, B_d$ of $A$ and $B$, respectively, with itself generate sufficiently many distinct dot products $a \cdot b = a_1b_1 + \ldots + a_db_d$, where $a = (a_1, \ldots, a_d) \in A_d, \ b = (b_1, \ldots, b_d) \in B_d$. This geometric interpretation of the arithmetic problem was used quite elegantly in [3] by way of Fourier analysis; it also puts this problem under the shibboleth of “hard Erdős problems” and arguably distinguishes the sum $AB + AB + \ldots$, within the more general case when some of the plus signs are replaces by minuses. It follows in particular from Theorem [1] that in $d = 10$ the set of dot products of elements of $A_d$ with itself is the whole field $\mathbb{F}_q$, as long as $|A_d| > q^\frac{1}{2}$, quite in the spirit of, say, the Erdős-Falconer distance problem. (In the case $A = B$, the following proof can be interpreted that there exists $a_s \in A_d$, such that dot products with $a_s$ cover $\mathbb{F}_q$.)

The proof of Theorem [1] follows from massaging the results of Lemmas 1, 2, and 4 in [2], which we formulate in a form suitable for immediate use in the sequel. The following lemma the key point of the argument. It has recently appeared in arithmetic combinatorics literature on numerous occasions, following up on a “statement about generic projections” by Bourgain, Katz, and Tao [1, Lemma 2.1].

By default, the sets $A, B$ in the sequel always satisfy the conditions of Theorem [1]

**Lemma 2** ([2], Lemmas 1,2) There exists $\xi \in \mathbb{F}_q^*$, such that

---

AMS subject classification 11T, 52C

*University of Bristol, Bristol BS8 1TW UK, m.rudnev@bris.ac.uk

May 17, 2008
Lemma 5

Theorem 1 follows if there exists a non-trivial $a$ for some $(\xi, a)$. In the sequel, a pair of those sets means a pair of the four sets $A$, $B$, $C$, and $D$.

Proof: Suppose, there is a non-trivial $a$ for some $(\xi, a)$. Then

$$x = a_1 + \xi b_1 = -a_2 - \xi b_2,$$

for some $(a_1, b_1, a_2, b_2) \in A \times B \times A \times B$, and $b \neq b_2$. So

$$\xi = \frac{a_1 + a_2}{b_1 + b_2}.$$
with non-zero denominator. Hence, by Lemma 2 (ii), the set

\[(b_1 + b_2)C_\xi^+ = \{(b_1 + b_2)a + (a_1 + a_2)b : (a, b) \in A \times B\}\]

has cardinality in excess of \(\frac{q}{4}\) and is clearly a subset of \(4AB\); then Lemma 3 ensures that \(8AB\) covers \(\mathbb{F}_q\).

Suppose now a non-trivial \(x\) lives in \(C_\xi^+ \cap C_\xi^-\). Then

\[x = a_1 + \xi b_1 = a_2 - \xi b_2,\]

for some \((a_1, b_1, a_2, b_2) \in A \times B \times A \times B\), and \(b \neq -b_2\). So

\[\xi = \frac{a_2 - a_1}{b_1 + b_2} = \frac{a_2 + a_3 + a_4}{b_1 + b_2},\]

for some \(a_3, a_4 \in A\) (by the assumption \(\bar{A} \subseteq A + A\)) and with non-zero denominator. Hence, by Lemma 2 (ii), the set

\[(b_1 + b_2)C_\xi^+ = \{(b_1 + b_2)a + (a_1 + a_2 + a_3)b : (a, b) \in A \times B\}\]

has cardinality in excess of \(\frac{q}{2}\) and is clearly a subset of \(5AB\); by Lemma 3 now \(10AB\) covers \(\mathbb{F}_q\).

Similarly, if a non-trivial \(x\) lives in \(C_\xi^+ \cap -C_\xi^-\), we have

\[x = a_1 + \xi b_1 = -a_2 + \xi b_2\]

for some \((a_1, b_1, a_2, b_2) \in A \times B \times A \times B\), and \(b_1 \neq b_2\). So

\[\xi = \frac{a_1 + a_2}{b_2 − b_1} = \frac{a_1 + a_2}{b_2 + b_3 + b_4},\]

for some \(b_3, b_4 \in B\) (by the assumption \(\bar{B} \subseteq B + B\)) and with non-zero denominator. Hence, by Lemma 2 (ii), the set

\[(b_2 + b_3 + b_4)C_\xi^+ = \{(b_2 + b_3 + b_4)a + (a_1 + a_2)b : (a, b) \in A \times B\}\]

has cardinality in excess of \(\frac{q}{2}\) and is clearly a subset of \(5AB\); by Lemma 3 now \(10AB\) covers \(\mathbb{F}_q\).

Other three pairs out of the four sets \(C_\xi^\pm, -C_\xi^\pm\) are clearly amenable to one of the three cases above. \(\square\)

It remains to establish that a non-trivial \(x\) exists. Let \(\tilde{A}\) denote a symmetric part of \(A\) and \(\tilde{A}\) its antisymmetric part. I.e.

\[\tilde{A} = \{a \in A : -a \in A\}, \quad \tilde{A} = A \setminus \tilde{A},\]

the same for \(B\). Suppose, a non-trivial \(x\) does not exist. This entails two consequences. Firstly, all the sets

\[\tilde{A} + \xi \tilde{B}, \quad \tilde{A} - \xi \tilde{B}, \quad -\tilde{A} + \xi \tilde{B}, \quad -\tilde{A} - \xi \tilde{B},\]

\[\tilde{A} + \xi \tilde{B}, \quad \tilde{A} - \xi \tilde{B}, \quad \tilde{A} + \xi \tilde{B}, \quad -\tilde{A} + \xi \tilde{B},\]

\[\tilde{A} + \xi \tilde{B}\]

must be pairwise-disjoint, or there would exist a non-trivial \(x\). Secondly, the diophantine equation (11) restricted to any one of the last five of these sets may not have any involved solutions. Indeed, if one of these two conditions failed, then using \(\tilde{A} \cap A = \emptyset\), as well as \(\tilde{A} \cap \tilde{A} = \emptyset\), and \(\tilde{A} = -\tilde{A}\), the same for \(B\), it would be possible to express \(\xi\) unambiguously in the form either \(\frac{a_1 + a_2}{b_1 + b_2}\), or \(\frac{a_1 - a_2}{b_1 + b_2}\), or \(\frac{a_1 + a_2}{b_1 - b_2}\) and then repeat the reasoning inside the proof of Lemma 3. The only doubling, i.e. the existence of involved solutions of (11), may occur when \(a_1, a_2, b_1, b_2\) appearing therein are restricted to one of the first four sets on the disjoint list (2). The fact that \(x\) is involved would then yield an unambiguous expression \(\xi = \frac{a_1 - a_2}{b_1 - b_2}\), but the latter defies the argument inside the proof of lemma 5 (i.e. the same argument would only result in \(12AB = \mathbb{F}_q\)).

It remains to bring the reasoning to absurd. Let \(|\tilde{A}| = u|A|, |\tilde{B}| = v|B|\) for some \(u, v \in (0, 1)\). (If one of the sets is symmetric or antisymmetric, i.e. \(u\) or \(v\) is 0 or 1, then by Glischuk’s result (2) \(8AB\) covers \(\mathbb{F}_q\).)
Let us estimate from below the size of the first four sets on the list (2). Lemma 2 (i) provides the upper estimate for the total number of solutions of the equation (1) on a pair of sets $A$ and $B$, which is clearly valid if one restricts the equation to their subsets. Hence, by Cauchy-Schwartz inequality and Lemma 2 (i), we have

$$|	ilde{A} + \xi \tilde{B}| > \frac{q}{2} \left( \frac{||\tilde{A}||B}{||A||B} \right)^2 = \frac{q}{2}(uv)^2,$$

and the same estimate for all the four first sets on the list (2). Furthermore, if there is no doubling in the last five sets and all the nine sets are disjoint, the cardinality of the union of them all, using

$$q < |A||B| = |\tilde{A}||\tilde{B}| + |\tilde{A}||\tilde{B}| + |\tilde{A}||\tilde{B}|,$$

is greater than

$$2q(2uv)^2 + |A||B|(2u(1-v) + 2v(1-u) + (1-u)(1-v)) > q(2(2uv)^2 + (u + v) - 3uv + 1).$$

It is easy to see that for $u, v \in (0, 1)$,

$$f(u, v) = 2(2uv)^2 + (u + v) - 3uv \geq 0.$$

Indeed, $f(u, v)$ is non-negative on the boundary of the above domain for $(u, v)$ and has a single critical point $u = v = \frac{1}{2}$ inside, where $f(\frac{1}{2}, \frac{1}{2}) = \frac{3}{8} > 0$. (At a critical point we have

$$4uv^3 - 3v + 1 = 0 \quad \text{and} \quad u = v.$$

The function $4v^3 - 3v + 1 > 0$ on $(0, 1)$ attains its absolute minimum, equal to zero, at $v = \frac{1}{2}$.)

Thus, assuming that all the sets (2) are disjoint and there is no doubling within the last five leads to an absurd statement that their union has size greater than $q$. The alternative to this is that there exists a non-trivial $x$ in some pair-wise intersection of the sets $C_{\xi}^\pm, -C_{\xi}^\pm$. Lemma 5 now kicks in and completes the proof of Theorem 1. □

References

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

[2] A. Glibichuk. Additive properties of product sets in an arbitrary finite field. Arxiv: 0801.2021 preprint 2008.

[3] D. Hart, A. Iosevich. Sums and products in finite fields: an integral geometric viewpoint. To appear in Radon transforms, geometry, and wavelets: A special volume of Contemporary Mathematics 2007.