Additive properties of product sets in an arbitrary finite field.*

Alexey Glibichuk

Abstract

It is proved that for any two subsets $A$ and $B$ of an arbitrary finite field $\mathbb{F}_q$ such that $|A||B| > q$ the identity $16AB = \mathbb{F}_q$ holds. Moreover, it is established that for every subsets $X, Y \subset \mathbb{F}_q$ with the property $|X||Y| \geq 2q$ the equality $8XY = \mathbb{F}_q$ holds.

1 Introduction.

Let $p$ be a prime, $m$ be a natural number, $\mathbb{F}_q$ be the finite field of order $q = p^m$, and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$, so that $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. For sets $X \subset \mathbb{F}_q$, $Y \subset \mathbb{F}_q$, and for a (possibly, partial) binary operation $*: \mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{F}_q$ we let

$$X*Y = \{x* y : x \in X, y \in Y\}.$$ 

We will write $XY$ instead of $X*Y$ if $*$ is multiplication in the field; and, for an element $\lambda \in \mathbb{F}_q$, we write

$$\lambda * A = \{\lambda\}A$$

$$-A = (-1)*A = \{-a : a \in A\}.$$ 

For a set $X \subset \mathbb{F}_q$ and $k \in \mathbb{N}$ let

$$kX = \{x_1 + \cdots + x_k : x_1, \ldots, x_k \in X\},$$

*This paper was supported by National Science Foundation grant under agreement No. DMS-0635607.
\[ X^k = \{ x_1 \ldots x_k : x_1, \ldots, x_k \in X \}. \]

Let also denote the cardinality of the given set \( X \) as \( |X| \). For given natural numbers \( N \) the notation \( NXY \) should be understood as \( N \)-fold sum of the product set \( XY \). Let us consider the following definitions.

**Definition 1** The set \( X \) is said to be **symmetric** if \( X = -X \).

**Definition 2** The set \( X \) is said to be **antisymmetric** if \( X \cap (-X) = \emptyset \).

A set \( A \) is called an (additive) basis of order \( k \) (for \( \mathbb{F}_q \)) if \( kA = \mathbb{F}_q \). Observe that any basis of order \( k \) is also a basis of any order \( k' > k \). The general problem that will be discussed in this paper is whether, for given integers \( t < q, N \) and two sets \( A \) and \( B \), the set \( AB \) is a basis of order \( N \) if \( |A||B| \geq t \)?

The first machinery, allowing one to prove sum-product results on finite fields was developed in the paper of J. Bourgain, N. Katz and T. Tao(1).

The author of this paper proved the following two statements(2, Theorems 1 and 2).

**Theorem 1** Let \( A \) and \( B \) be subsets of the field \( \mathbb{F}_p \) for some prime \( p \). If the set \( B \) is antisymmetric and \( |A||B| > p \) then \( 8AB = \mathbb{F}_p \).

**Theorem 2** Let \( A \) and \( B \) be subsets of the field \( \mathbb{F}_p \) for some prime \( p \). If the set \( B \) is symmetric and \( |A||B| > p \) then \( 8AB = \mathbb{F}_p \).

In the joint paper with S.V. Konyagin(3, Lemmas 2.1 and 2.2) we established the following two results.

**Theorem 3** If \( A \subset \mathbb{F}_p, B \subset \mathbb{F}_p \) for some prime \( p \), and \( |A| \cdot \lceil |B|/2 \rceil > p \) then \( 8AB = \mathbb{F}_p \).

**Theorem 4** If \( A \subset \mathbb{F}_p, B \subset \mathbb{F}_p \) for some prime \( p \), and \( |A||B| > p \) then \( 16AB = \mathbb{F}_p \).

In this paper extensions of Theorems 1, 2 will be obtained. We shall establish the following four theorems.

**Theorem 7** If \( A \subset \mathbb{F}_q \) and \( B \subset \mathbb{F}_q \) are such that \( B \) is antisymmetric and \( |A||B| > q \) then \( 8AB = \mathbb{F}_q \).
Theorem 8 Assume that $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ are such that $B$ is symmetric. If also $|A||B| > q$ then $8AB = \mathbb{F}_q$.

Theorem 9 Let $A, B \subset \mathbb{F}_q$ be arbitrary subsets with $|A||B| > q$. Then we have $16AB = \mathbb{F}_q$.

Theorem 10 Let $A, B \subset \mathbb{F}_q$ be arbitrary subsets with $|A||B| \geq 2q$. Then we have $8AB = \mathbb{F}_q$.

Constant 16 in the Theorem 9 is most likely not best possible, it is demonstrated by Theorem 10 and recent result of D. Hart and A. Iosevich ([4]). They established that

Theorem 5 For every subset $A \subset \mathbb{F}_q$ such that $|A| \geq Cq^{\frac{1}{2} + \frac{1}{d}}$ for $C$ sufficiently large the identity $dA^2 = \mathbb{F}_q^*$ holds.

Applying Theorem 5 with $d = 1$ we see that the constant in the Theorem 9 can be significantly improved when $A = B$ and $|A| > Cq^2$. D. Hart and A. Iosevich in the same paper have conjectured that if $|A| > Cq^{\frac{1}{2} + \epsilon}$ for some constant $C$ and $\epsilon > 0$ then $2A^2 = \mathbb{F}_q$. However, condition $|A||B| > q$ in the Theorem 9 is sharp. Indeed, if $|A||B| = q$ then result similar to the Theorem 9 cannot hold. It is sufficient to consider sets $A = \mathbb{F}_q, B = \{0\}$ or make $A = B$ to be a subfield of order $\sqrt{q}$ when $q = p^m$ and $m$ is even, to verify this statement. To construct a less trivial counterexample let us consider two natural numbers $k$ and $l$ such that $k + l = m$. Let us take a primitive element $\xi \in \mathbb{F}_q^*$ and consider sets

\[
A = \{x_0 + x_1\xi + \ldots + x_{k-1}\xi^{k-1} : (x_0, \ldots, x_{k-1}) \in \mathbb{F}_p \times \ldots \times \mathbb{F}_p := \mathbb{F}_p^k \},
\]

\[
B = \{x_0 + x_1\xi + \ldots + x_{l-1}\xi^{l-1} : (x_0, x_1, \ldots, x_{l-1}) \in \mathbb{F}_p^l \}
\]

and

\[
C = \{x_0 + x_1\xi + \ldots + x_{m-2}\xi^{m-2} : (x_0, x_1, \ldots, x_{m-2}) \in \mathbb{F}_p^{m-1} \}
\]

where $\mathbb{F}_p \subset \mathbb{F}_q$ is a subfield of $\mathbb{F}_q$ of cardinality $p$. Then one can obviously observe that $|A||B| = q$, $AB \subset C \neq \mathbb{F}_q$ and $C$ is closed under addition.

2 Preliminary results.

Lemmas 1, 2, 3 are extensions of Lemmas 1, 2, 3 from [2]. Their proofs are due to arguments used in corresponding lemmas.
Lemma 1 Let $A \subset \mathbb{F}_q$, $B \subset \mathbb{F}_q$ be arbitrary nonempty subsets. Then there is an element $\xi \in \mathbb{F}_q^*$ such that

$$|A + \xi B| \geq \frac{|A||B|(q - 1)}{|A||B| - (|A| + |B|) + q}$$

and

$$|A - \xi B| \geq \frac{|A||B|(q - 1)}{|A||B| - (|A| + |B|) + q}. \tag{2}$$

Proof. Let us consider an arbitrary elements $\xi \in \mathbb{F}_q^*$ and $s \in \mathbb{F}_q$. Denote

$$f_\xi^+(s) = |\{(a, b) \in A \times B : a + b\xi = s\}|,$$

$$f_\xi^-(s) = |\{(a, b) \in A \times B : a - b\xi = s\}|.$$

It obviously follows that

$$\sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 = |\{(a_1, b_1, a_2, b_2) \in A \times B \times A \times B : a_1 + b_1\xi = a_2 + b_2\xi\}|$$

$$= |A||B| + |\{(a_1, b_1, a_2, b_2) \in A \times B \times A \times B : a_1 \neq a_2, a_1 + b_1\xi = a_2 + b_2\xi\}|,$$

$$\sum_{s \in \mathbb{F}_q} (f_\xi^-(s))^2 = |\{(a_1, b_1, a_2, b_2) \in A \times B \times A \times B : a_1 - b_1\xi = a_2 - b_2\xi\}|$$

$$= |A||B| + |\{(a_1, b_1, a_2, b_2) \in A \times B \times A \times B : a_1 \neq a_2, a_1 - b_1\xi = a_2 - b_2\xi\}|.$$

Therefore, $\sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 = \sum_{s \in \mathbb{F}_q} (f_\xi^-(s))^2$, and it is enough to consider only sum with values of $f_\xi^+(s)$. It is easy to see that for every $a_1, a_2 \in A$ and $b_1, b_2 \in B$ with $a_1 \neq a_2$ there is only one element $\eta \neq 0$ such that $a_1 + b_1\eta = a_2 + b_2\eta$. Thus,

$$\sum_{\xi \in \mathbb{F}_q^*} \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 = |A||B|(q - 1) + |A||B|(|A| - 1)(|B| - 1).$$

Therefore, there is $\xi \in \mathbb{F}_q^*$ such that

$$\sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 \leq |A||B| + \frac{|A||B||A| - 1(|B| - 1)}{q - 1}. \tag{3}$$
By Cauchy-Schwartz
\[
\left( \sum_{s \in \mathbb{F}_q} f_\xi^+(s) \right)^2 \leq |A + \xi B| \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2, \quad (4)
\]
\[
\left( \sum_{s \in \mathbb{F}_q} f_\xi^-(s) \right)^2 \leq |A - \xi B| \sum_{s \in \mathbb{F}_q} (f_\xi^-(s))^2. \quad (5)
\]
Moreover, it obviously follows that
\[
\sum_{s \in \mathbb{F}_q} f_\xi^+(s) = |A||B|,
\]
\[
\sum_{s \in \mathbb{F}_q} f_\xi^-(s) = |A||B|.
\]
Now from (3), (4) and (5) one can deduce a desired inequality:
\[
|A + \xi B| \geq \frac{|A|^2|B|^2}{|A||B| + \frac{|A||B|(|A|-1)(|B|-1)}{q-1}} = \frac{|A||B|(q-1)}{|A||B| - (|A| + |B|) + q}
\]
and
\[
|A - \xi B| \geq \frac{|A||B|(q-1)}{|A||B| - (|A| + |B|) + q}.
\]
Lemma 1 is proved. ■

**Lemma 2** Let \( A \) and \( B \) be subsets of field \( \mathbb{F}_q \) with \( |A||B| > q \). Then there is \( \xi \in \mathbb{F}_q^\ast \) such that
\[
|A + \xi B| > \frac{q}{2}, \quad (6)
\]
and
\[
|A - \xi B| > \frac{q}{2}. \quad (7)
\]

**Proof.** Let us apply Lemma 1. It states that there is \( \xi \in \mathbb{F}_q^\ast \) such that (1) and (2) hold. Clearly, we have
\[
\frac{|A||B|(q-1)}{|A||B| - (|A| + |B|) + q} \geq \frac{|A||B|(q-1)}{|A||B| + (q-2)}.
\]
Let us consider the difference
\[ s = \frac{|A||B|(q - 1)}{|A||B| + (q - 2)} - \frac{q}{2} = \frac{(q - 2)(|A||B| - q)}{2(|A||B| + (q - 2))}. \]
It is clear that \( s > 0 \) when \( |A||B| > q \) and \( q \neq 2 \). If \( q = 2 \) then the condition \( |A||B| > q \) implies that at least one of the subsets \( A \) or \( B \) is equal to \( \mathbb{F}_q \). Lemma \( \square \) is proved.

**Definition 3** For two subsets \( A \subset \mathbb{F}_q, B \subset \mathbb{F}_q \) denote
\[ I(A, B) = \{(b_1 - b_2) \cdot a_1 + (a_2 - a_3) \cdot b_3 : a_1, a_2, a_3 \in A, b_1, b_2, b_3 \in B\}. \]

**Lemma 3** Consider two subsets \( A \subset \mathbb{F}_q \) and \( B \subset \mathbb{F}_q \). If for some \( \xi \in \mathbb{F}_q^* \)
\[ |A + \xi B| < |A||B| \]
then
\[ |I(A, B)| \geq |A + \xi B|. \]

**Proof.** If \( |A + \xi B| < |A||B| \) then there are elements \( a_1, a_2 \in A \) and \( b_1, b_2 \in B \) such that \( (a_1, b_1) \neq (a_2, b_2) \) and
\[ (a_1 - a_2) + (b_1 - b_2) \cdot \xi = 0. \tag{8} \]
It is clear that \( b_1 \neq b_2 \). Let us consider the set
\[ S = (b_1 - b_2) \cdot (A + \xi B) = \{(b_1 - b_2) \cdot b : b \in A + \xi B\}. \]
It is obviously follows that \( |S| = |A + \xi B| \) and every element of \( S \) can be rewritten in the form
\[ s = (b_1 - b_2) \cdot a + (b_1 - b_2) \cdot b \xi \]
with \( a \in A \) and \( b \in B \). From \( \square \) one can easily deduce that
\[ s = (b_1 - b_2) \cdot a + (a_2 - a_1) \cdot b. \]
Therefore, \( S \subset I(A, B) \) and lemma follows. \( \square \)

**Lemma 4** Assume that \( X \subset \mathbb{F}_q \) with \( |X| > \frac{q}{2} \), then \( X + X = \mathbb{F}_q \).
Proof. Let us take an arbitrary element $x \in \mathbb{F}_q$ and consider a set $x - X$. From $|x - X| = |X| > \frac{q}{2}$ one can obviously prove that sets $x - X$ and $X$ have nonempty intersection, so there are elements $x_1, x_2 \in X$ such that $x - x_1 = x_2 \iff x = x_1 + x_2$. Lemma now follows. ■

Lemma 5. Let $A$ be any subset of $\mathbb{F}_q$. If $|A| \not\equiv 2 \pmod{3}$ then there is a symmetric or antisymmetric subset $S \subset A$ with $|S| \geq \frac{2}{3}|A|$. If $|A| \equiv 2 \pmod{3}$ then one can find either symmetric or antisymmetric subset $S \subset A$ with $|S| \geq \frac{2}{3}|A| - \frac{1}{3}$.

Proof. Let us define a set $A_1 = \{x \in A : -x \notin A\}$. It is an antisymmetric subset of $A$. Consider a set of subsets $\mathcal{S} = \{\{a_1, a_2\} : a_1 \in A, a_2 \in A, a_1 = -a_2\}$. It is clear that one can choose one element from each of the sets from $\mathcal{S}$ and form a new set $A_2$ from those elements. It is easy to observe that $A_2 \cap A_1 = \emptyset$, $0 \in A_2$ if $0 \in A$ and $A_2 \setminus \{0\}$ is antisymmetric. Let us define a subset $A_3 = A \setminus (A_1 \cup A_2)$. It is an antisymmetric subset of $A$ with cardinality $|A_3| = |A_2| - 1$ if $0 \in A$ and $|A_3| = |A_2| - 1$ otherwise, such that $0 \notin A_3$ and $A_2 \cup A_3$ is the maximal symmetric subset of $A$. We have split the set $A$ into three nonintersecting parts: $A = A_1 \cup A_2 \cup A_3$.

If $|A| < \frac{1}{3}|A|$ then $|A_2 \cup A_3| \geq \frac{2}{3}|A|$ and Lemma 5 follows with symmetric $S = A_2 \cup A_3$.

If $0 \notin A$ and $|A_1| \geq \frac{1}{3}|A|$ then $|A_2| = |A_3|$ and $|A_3| < \frac{1}{3}|A|$. Assuming $S$ to be an antisymmetric subset $A_1 \cup A_2$ we complete the proof of Lemma 5.

Assume that $|A_1| > \frac{1}{3}|A|$ and $0 \in A$. If $|A_3| \geq \frac{1}{3}|A|$ then $|A_1 \cup A_3| \geq \frac{2}{3}|A|$ and Lemma 5 is proved by letting $S$ be antisymmetric subset $A_1 \cup A_3$.

It is left to prove Lemma 5 when

$$|A_1| \geq \frac{1}{3}|A|, \quad (9)$$

$$|A_3| < \frac{1}{3}|A| \quad (10)$$

and $0 \in A$. Let us consider three cases.

Case 1. $|A| = 3k$ for some natural $k$. Taking into account (9) and (10) one can see that $|A_3| \leq k - 1$ and therefore $|A_1 \cup A_2| \geq 2k + 1$. By defining $S = (A_1 \cup A_2) \setminus \{0\}$ ($S$ is antisymmetric) we complete the proof of Lemma 5.

Case 2. $|A| = 3k + 1$ for some natural $k$. Again, using (9) and (10) one can deduce that $|A_3| \leq k$. If $|A_3| \leq k - 1$ then assuming $S = (A_1 \cup A_2) \setminus \{0\}$
we get a required antisymmetric subset. If $|A_3| = k$ then $|A_2| = k + 1$ and $|A_1| = k$. Note that the identity $|A_1| = k$ contradicts inequality (9). We are done.

Case 3. $|A| = 3k + 2$ for some natural $k$. Using (9) and (10) one can easily deduce that $|A_3| \leq k$ and $|A_1| \geq k + 1$. If $|A_3| \leq k - 1$ then $|A_1 \cup A_2| = |A \setminus A_3| \geq 2k + 3$. Letting $S$ to be an antisymmetric subset $(A_1 \cup A_2) \setminus \{0\}$ we observe that $|S| \geq 2k + 2 > \frac{1}{3}|A|$ and we are done with better bound on $|S|$. In case when $|A_3| = k$ it is easy to see that $|A_2| = k + 1$ and $|A_1| = k + 1$. Assuming $S$ to be a symmetric subset $A_2 \cup A_3$ we complete the proof of Lemma 5. ■

Definition 4 For every subset $X \subset \mathbb{F}_q$ its symmetry group (it is denoted as $\text{Sym}_1(X)$) is defined by the identity

$$\text{Sym}_1(X) = \{h : \{h\} + X = X\}.$$  

We shall use the following theorem (see [6], theorem 5.5 or [5]).

Theorem 6 (Kneser) For every subsets $X, Y \subset \mathbb{F}_q$ we have

$$|X + Y| \geq |X + \text{Sym}_1(X + Y)| + |Y + \text{Sym}_1(X + Y)| - |\text{Sym}_1(X + Y)| \geq$$

$$\geq |X| + |Y| - |\text{Sym}_1(X + Y)|.$$  

Lemma 6 Given a subset $X \subset \mathbb{F}_q$. Let us take any subgroup $G$ of the group $\text{Sym}_1(X)$. Then $X$ is a union of additive cosets of $G$.

Proof. One can easily observe that $\text{Sym}_1(X)$ is an additive subgroup. It is sufficient to prove that every coset of the subgroup $G$ either is a subset of $X$ or has an empty intersection with $X$. Suppose that some coset $x + G$ has nonempty intersection with $X$. Let us take an arbitrary element $y \in X \cap (x + G)$. By definition of $y$ a coset $y + G = x + G$, but from symmetry of $X$ it follows that $y + G \subset X$. Lemma 6 is proved. ■

Lemma 7 Let $B$ be an arbitrary subset of $\mathbb{F}_q$ such that $|B| \geq 2$. Then one of the following two alternatives holds

(i) $|B + B| \geq \frac{3}{2}|B|$, 

(ii) there is an additive subgroup $G \subset \mathbb{F}_q$ such that $B \subset b + G$ for some $b \in B$ and $|B| > \frac{2}{3}|G|$. Moreover, in this case $B + B = 2b + G$.  

8
Proof. Application of Theorem 6 for sets $X = Y = B$ implies
\[ |B + B| \geq 2|B + \text{Sym}_1(B + B)| - |\text{Sym}_1(B + B)| \geq 2|B| - |\text{Sym}_1(B + B)|. \tag{11} \]

Since $\text{Sym}_1(B + B)$ is an additive subgroup of $\mathbb{F}_q$ then there is an integer $0 \leq l \leq n$ such that $|\text{Sym}_1(B + B)| = p^l$. Observe that $\text{Sym}_1(B + B) \subset \text{Sym}_1(B + \text{Sym}_1(B + B))$. Now from Lemma 6 clearly follows that $|B + \text{Sym}_1(B + B)| = mp^l$ for some natural $m$. Again, using (11) we can see that
\[ |B + B| \geq (2m - 1)p^l. \tag{12} \]

Assume that the inequality $|B + B| < \frac{3}{2}|B|$ holds. Then we deduce from (11) that
\[ \frac{3}{2}|B| > 2|B| - |\text{Sym}_1(B + B)| \Leftrightarrow |B| < 2p^l \]
and therefore $|B + B| < \frac{3}{2} \cdot 2p^l = 3p^l$. Combining the last inequality with (12) we obtain the condition $2m - 1 < 3$ and therefore $m$ can take on one value: $m = 1$. When $m = 1$ one can observe that $|B + \text{Sym}_1(B + B)| = |\text{Sym}_1(B + B)| = p^l$. Take an arbitrary element $b \in B$ and consider the set $B' = B - b$. It is clear, that $B' + \text{Sym}_1(B + B) = \text{Sym}_1(B + B)$ and therefore $B' \subset \text{Sym}_1(B + B)$. Recalling definition of $B'$ we obtain a relation $B \subset b + \text{Sym}_1(B + B)$. By (12) one can deduce the inequality $|B + B| \geq p^l$. Observing that $B + B \subset 2b + \text{Sym}_1(B + B)$ we can obtain the relation $|B + B| = |\text{Sym}_1(B + B)| = p^l$. Now it is clear that if $|B| \leq \frac{2}{3}p^l$ then the inequality $|B + B| \geq \frac{2}{3}|B|$ holds, otherwise we get the alternative $(ii)$. To finish the proof of the Lemma 7 we need to observe that according to Lemma 4 $B + B = 2b + \text{Sym}_1(B + B)$ when $|B| > \frac{2}{3}p^l$. Lemma 7 now follows. \[ \blacksquare \]

3 Proofs of theorems 7-10.

Theorem 7 If $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ are such that $B$ is antisymmetric and $|A||B| > q$ then $8AB = \mathbb{F}_q$.

Proof. Let us apply Lemma 2. It states that there is an element $\xi \in \mathbb{F}_q^*$ such that (9) and (7) hold. From (6) one can easily derive that $(A + \xi b) \cap (-A - \xi B) \neq \emptyset$ and, therefore, there are elements $a_1, a_2 \in A, b_1, b_2 \in B$ with $a_1 + b_1 \xi = -(a_2 + b_2 \xi)$. Thus,
\[ \xi = -\frac{a_1 + a_2}{b_1 + b_2}. \tag{13} \]
The expression (13) is correct because \( B \cap (-B) = \emptyset \) and denominator of the fraction in this formula is not equal to zero. From (7) it follows that

\[
\left| \left\{ a_3 + \frac{a_1 + a_2}{b_1 + b_2} b_3 : a_3 \in A, b_3 \in B \right\} \right| > \frac{q}{2} \iff \\
\left| \{a_3(b_1 + b_2) + b_3(a_1 + a_2) : a_3 \in A, b_3 \in B\} \right| > \frac{q}{2}.
\]

Therefore, \(|4AB| > \frac{q}{2}\) and Lemma 4 gives us the desired statement. ■

**Theorem 8** Assume that \( A \subset \mathbb{F}_q \) and \( B \subset \mathbb{F}_q \) are such that \( B \) is symmetric. If also \(|A||B| > q\) then \( 8AB = \mathbb{F}_q \).

**Proof.** Applying Lemma 2 one can find an element \( \xi \in \mathbb{F}_q^* \) such that \(|A + \xi B| > \frac{q}{2}\). Moreover, from restrictions on sets \( A \) and \( B \) one can see that \(|A + \xi B| \leq q < |A||B|\) and we can apply Lemma 3 that gives us the following:

\[ |I(A, B)| \geq |A + \xi B| > \frac{q}{2}. \]

Taking into account that \( B = -B \) one can derive that \( I(A, B) \subset 4AB \) and \(|4AB| > \frac{q}{2}\). Now Theorem 8 follows from Lemma 4. ■

**Theorem 9** Let \( A, B \subset \mathbb{F}_q \) be arbitrary subsets with \(|A||B| > q\). Then we have \( 16AB = \mathbb{F}_q \).

**Proof.** Let us apply Lemma 7 for the set \( B \). If (ii) holds then \( B + B = 2b + G \) for some \( b \in B \) and an additive subgroup \( G \subset \mathbb{F}_q \). It is easy to see that every coset of an additive subgroup is an antisymmetric or a symmetric subset. Then application of Theorem 7 or Theorem 8 for sets \( A \) and \( B + B \) gives us Theorem 9.

Assume now that

\[ |B + B| \geq \frac{3}{2}|B| \tag{14} \]

i. e. alternative (i) holds. If \(|B + B| \not\equiv 2 \pmod{3}\) then application of Lemma 5 gives us a subset \( S \subset B + B \) such that \(|S| \geq \frac{3}{3}|B + B|\) and \( S \) is either symmetric or antisymmetric. By (14) we observe that \(|S| \geq |B|\). Application of Theorem 7 or Theorem 8 for sets \( A \) and \( S \) allows one deduce Theorem 9.

It is left to consider the case when \(|B + B| \equiv 2 \pmod{3}\) and the inequality (14) holds. Assume that \(|B + B| = 3k + 2\) for some natural \( k \). Lemma 5
states that there is either symmetric or antisymmetric subset $S \subset B + B$ with $|S| \geq \frac{2}{3}|B + B| - \frac{1}{3} = 2k + 1$. Moreover, by (14) we can deduce that $2k + 1 \geq |B| - \frac{1}{3}$ and, therefore $|B| \leq 2k + 1$. Now it is easy to see that $|S| \geq 2k + 1 \geq |B|$. Using Theorem 7 or Theorem 8 for sets $A$ and $S$ we complete the proof of Theorem 9. ■

**Theorem 10** Let $A, B \subset \mathbb{F}_q$ be arbitrary subsets with $|A||B| \geq 2q$. Then we have $8AB = \mathbb{F}_q$.

**Proof.** Our aim is to extract from the set $B$ a sufficiently large symmetric or antisymmetric subset $S \subset B$. Lemma 5 states that there is a symmetric or antisymmetric subset $S \subset B$ with $|S| \geq \frac{2}{3}|B| - \frac{1}{3}$. Let us notice that the equality $|B| = 2$ holds when $|A||B| = 2q$ and, therefore, $A = \mathbb{F}_q$, so we can assume that $|B| > 2$. Observe that in this case $\frac{2}{3}|B| - \frac{1}{3} > \frac{1}{2}|B|$ and we have $|A||S| > \frac{1}{2}|A||B| \geq q$ and Theorem 10 now follows from Theorems 7 and 8. ■

**References**

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

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

[3] A. A. Glibichuk, S.V. Konyagin, *Additive properties of product sets in fields of prime order*, Centre de Recherches Mathématiques Proceedings and Lecture Notes, vol. 43, pp. 279-286.

[4] D.Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, preprint.

[5] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Z., vol. 58, 1953, pp. 459–484.

[6] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Univ. Press, Cambridge, 2006.