Pairs of Dot Products in Finite Fields and Rings

David Covert and Steven Senger

Abstract We obtain bounds on the number of triples that determine a given pair of dot products arising in a vector space over a finite field or a module over the set of integers modulo a power of a prime. More precisely, given $E \subset \mathbb{F}_q^d$ or $\mathbb{Z}_q^d$, we provide bounds on the size of the set

$$\{(u, v, w) \in E \times E \times E : u \cdot v = \alpha, u \cdot w = \beta\}$$

for units α and β.

Keywords Dot-product sets · Sum-product problem · Finite fields

1 Introduction

For a subset of a ring, $A \subset R$, the sumset and productset of A are defined as $A + A = \{a + a' : a, a' \in A\}$ and $A \cdot A = \{a \cdot a' : a, a' \in A\}$, respectively. The sum-product conjecture asserts that when $A \subset \mathbb{Z}$, then either $A + A$ or $A \cdot A$ is of large cardinality. For example, if we take $A \subset \mathbb{Z}$ to be a finite arithmetic progression of length n, you achieve $|A + A| = 2n - 1$, whereas $|A \cdot A| \geq cn^2/((\log n)^\delta \cdot (\log\log n)^{3/2})$ for some constant $c > 0$ and $\delta = 0.08607\ldots$ [7]. When $A \subset \mathbb{Z}$ is a geometric progression of length n, we have $|A \cdot A| = 2n - 1$, and yet it is easy to show that $|A + A| = \binom{n+1}{2}$. For subsets of integers, the following conjecture was made in [6].

Conjecture 1 *Let $A \subset \mathbb{Z}$ with $|A| = n$. For every $\epsilon > 0$, there exists a constant $C_\epsilon > 0$ so that*

$$\max(|A + A|, |A \cdot A|) \geq C_\epsilon n^{2-\epsilon}.$$

D. Covert (✉)
University of Missouri, Saint Louis, USA
e-mail: covertdj@umsl.edu

S. Senger
Missouri State University, Springfield, USA

M. B. Nathanson (ed.), *Combinatorial and Additive Number Theory II*,
Springer Proceedings in Mathematics & Statistics 220,
https://doi.org/10.1007/978-3-319-68032-3_8

Much progress has been made on the sum-product problem. The best result to date belongs to Konyagin and Shkredov [11], wherein they demonstrated that for a sufficiently large constant C, we have the bound

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

for any $c < \frac{5}{9813}$, whenever A is a set of real numbers with cardinality n. Work has also been done on analogues of the sum-product problem for general rings [12]. For example, the authors in [8] showed that if $E \subset \mathbb{F}_q^d$ is of sufficiently large cardinality, then we have

$$|\{(x, y) \in E \times E : x \cdot y = \alpha\}| = \frac{|E|^2}{q}(1 + \underline{o}(1)),$$

for any $\alpha \in \mathbb{F}_q^*$. Here, $\mathbb{F}_q$ is the finite field with q elements, $\mathbb{F}_q^d$ is the d-dimensional vector space over $\mathbb{F}_q$, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. As a corollary, they showed that $|dA^2| := |A \cdot A + \cdots + A \cdot A| \supset \mathbb{F}_q^*$, whenever $A \subset \mathbb{F}_q$ is such that $|A| \geq q^{\frac{1}{2}+\frac{1}{2d}}$. Much work has also been done to give such results when E has relatively small cardinality. See, for example, [10] and the references contained therein.

In [3], the second listed author and Daniel Barker studied pairs of dot products determined by sets $P \subset \mathbb{R}^2$. In addition to the applications toward the sum-product problem above, the problem of pairs of dot products has applications in coding theory, graph theory, and frame theory, among others [1, 2, 4]. The main results from [3] are as follows.

Theorem 1 *Suppose that $P \subset \mathbb{R}^2$ is a finite point set with cardinality $|P| = n$. Then, the set*

$$\Pi_{\alpha,\beta}(P) := \{(x, y, z) \in P \times P \times P : x \cdot y = \alpha, x \cdot z = \beta\}$$

satisfies the upper bound $|\Pi_{\alpha,\beta}(P)| \lesssim n^2$ whenever α and β are fixed, nonzero real numbers.

Note 1 Here and throughout, we use the notation $X \lesssim Y$ to mean that $X \leq cY$ for some constant $c > 0$. Similarly, we use $X \gtrsim Y$ for $Y \lesssim X$, and we use $X \approx Y$ if both $X \lesssim Y$ and $X \gtrsim Y$. Finally, we write $X \gtrapprox Y$ if for all $\epsilon > 0$, there exists a constant $C_\epsilon > 0$ such that $X \gtrapprox C_\epsilon q^\epsilon Y$.

Theorem 1 is sharp, as shown in an explicit construction [3]. Additionally, they showed the following:

Theorem 2 *Suppose that $P \subset [0, 1]^2$ is a set of n points that obey the separation condition*

$$\min(|p - q| : p, q \in P, p \neq q) \geq \epsilon.$$

Then, for $\epsilon > 0$ and fixed $\alpha, \beta \neq 0$, we have

$$|\Pi_{\alpha,\beta}(P)| \lesssim n^{4/3}\epsilon^{-1} \log\left(\epsilon^{-1}\right).$$

The purpose of this article is to study finite field and finite ring analogues of the results from [3]. Our main results are as follows.

Theorem 3 *Given a set, $E \subset \mathbb{F}_q^2$ or $\mathbb{Z}_q^d$, $|E| = n$, and fixed units α, β, we have the bound*

$$|\Pi_{\alpha,\beta}(E)| \lesssim n^2.$$

In general, for a set of n points, $E \subset \mathbb{F}_q^2$, one cannot expect to get an upper bound better than Theorem 3, as we will show via an explicit construction in Proposition 1. This proof and construction are similar to their analogues in [3]. However, if we view the separation condition from Theorem 2 as it relates to density (as is often the case for translating such results, such as in [9]), the previous proof techniques yield very little. It turns out that a discrepancy theoretic approach gives more information, as our second main result is for general subsets of $\mathbb{F}_q^d$, for $d \geq 2$, as opposed to just $d = 2$.

Theorem 4 *Let $d \geq 2$, $E \subset \mathbb{F}_q^d$, and suppose that $\alpha, \beta \in \mathbb{F}_q$. Then, we have the bound*

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E|^3}{q^2}(1 + \underline{o}(1)),$$

for $|E| \gtrapprox q^{\frac{d+1}{2}}$ when $\alpha, \beta \in \mathbb{F}_q^*$, and for $|E| \gtrapprox q^{\frac{d+2}{2}}$ otherwise.

Note that Theorem 4 gives a quantitative version of Theorem 3 at least for sets $E \subset \mathbb{F}_q^2$ in the range $|E| \gtrapprox q^{3/2}$.

The proof of Theorem 4 relies on adapting the exponential sums found in the study of single dot products [8]. Since the results from [8] were extended to general rings $\mathbb{Z}_q^d$ in [5], Theorem 4 also easily extends to rings. Here and throughout, $\mathbb{Z}_q$ denotes the set of integers modulo q, $\mathbb{Z}_q^\times$ is the set of units in $\mathbb{Z}_q$, and $\mathbb{Z}_q^d = \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$ is the d-rank free module over $\mathbb{Z}_q$. For $E \subset \mathbb{Z}_q^d$, we define $\Pi_{\alpha,\beta}(E)$ exactly as before.

Theorem 5 *Suppose that $E \subset \mathbb{Z}_q^d$, where $q = p^\ell$ is the power of a prime $p \geq 3$. Then for units $\alpha, \beta \in \mathbb{Z}_q^\times$, we have*

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E|^3}{q^2}(1 + \underline{o}(1))$$

whenever $|E| \gtrapprox q^{\frac{d(2\ell-1)}{2\ell} + \frac{1}{2\ell}}$. In particular,

$$|\Pi_{\alpha,\beta}(E)| \lesssim |E|^2$$

for sets $E \subset \mathbb{Z}_q^2$ of sufficiently large cardinality.

Remark 1 Notice that the proofs of Theorems 4 and 5 provide both a lower and upper bounds on the cardinality of $\Pi_{\alpha,\beta}(E)$, though we could achieve the upper bound $|\Pi_{\alpha,\beta}(E)| \lesssim q^{-2}|E|^3$ if we relaxed the condition $|E| \gtrapprox q^{\frac{d+1}{2}}$ to simply $|E| \gtrsim q^{\frac{d+1}{2}}$, for example.

2 Explicit Constructions

2.1 *Sharpness of Theorem 3*

We construct explicit sharpness examples for $\mathbb{F}_q^2$. The same constructions can be modified to yield sharpness in $\mathbb{Z}_q^2$ as well.

Proposition 1 *Given a natural number $n \lesssim q$ and elements $\alpha, \beta \in \mathbb{F}_q^*$, there is a set, $E \subset \mathbb{F}_q^2$ for which $|E| = n$ and*

$$|\Pi_{\alpha,\beta}(E)| \approx n^2.$$

Proof Let u be the point with coordinates $(1, 1)$. Now, distribute up to $\lceil \frac{n-1}{2} \rceil$ points along the line $y = \alpha - x$, and distribute the remaining up to $\lfloor \frac{n-1}{2} \rfloor$ points along the line $y = \beta - x$. If there are any points left over, put them anywhere not yet occupied.[1] Clearly, there are at least $|E|^2$ pairs of points (b, c), where q is chosen from the first line and r is chosen from the second. Notice that u contributes a triple to $\Pi_{\alpha,\beta}(E)$ for each such pair, giving us

$$|\Pi_{\alpha,\beta}(E)| \approx n^2.$$

2.2 *The Special Case $\alpha = \beta = 0$, $D = 2$*

Proposition 2 *There exists a set $E \subset \mathbb{F}_q^2$ of cardinality $|E| = n < 2q$ for which*

$$|\Pi_{0,0}(P)| \approx n^3.$$

Proof Select $\lceil \frac{n}{2} \rceil$ points with zero x-coordinate, and $\lfloor \frac{n}{2} \rfloor$ points with zero y-coordinate. Now, for each of the points with zero x-coordinate, there are about $\binom{\frac{n}{2}}{2}$ pairs of points with zero y-coordinate. Notice that any point chosen with zero x-coordinate will have dot product zero with each point from the pair chosen with zero y-coordinate. Therefore, each of these $\frac{1}{8}n^3$ triples will contribute to $\Pi_{0,0}(E)$.

We can get just as many triples that contribute to $\Pi_{0,0}(E)$ by taking single points with zero y-coordinate and pairs of points with zero x-coordinate. In total, we get

$$|\Pi_{0,0}(P)| \approx \frac{1}{8}n^3 + \frac{1}{8}n^3 \approx n^3.$$

[1]This is just in the case that $(1, 1)$ is on one of the lines or $\alpha = \beta$.

3 Proofs of Main Results

3.1 Proof of Theorem 3

This proof is a modified version of the proof of Theorem 1 in [3], to which we refer to the reader for a more detailed exposition.

Proof We will simultaneously prove this for $E \subset \mathbb{F}_q^2$ and $E \subset \mathbb{Z}_q^2$. Here, we will use R_q to denote either $\mathbb{F}_q$ or $\mathbb{Z}_q$, and we will be more specific when necessary.

Our basic idea is to consider pairs of points $(v, w) \in E \times E$ and obtain a bound on the number of possible candidates for u to contribute a triple of the form (u, v, w) to $\Pi_{\alpha,\beta}(E)$. Consider $a = (a_x, a_y) \in R_q^2$, and notice that for a point $v \in E$, the set of points $L_\alpha(v)$ that determine the dot product α with v forms a line.

$$L_\alpha(v) = \left\{(x, y) \in R_q^2 : xv_x + yv_y = \alpha\right\}. \tag{1}$$

Also, v lies on a unique line containing the origin. We similarly define $L_\beta(v)$. Now, consider a second point $w \in E$. It is easy to see that if $|L_\alpha(v) \cap L_\beta(w)| > 1$, then v and w lie on the same line through the origin which implies that if v and w are on different lines through the origin, then $|L_\alpha(v) \cap L_\beta(w)| \leq 1$. We will use this dichotomy to decompose $E \times E$ into two sets:

$$\begin{aligned}
A &= \{(v, w) \in E \times E : |L_\alpha(v) \cap L_\beta(w)| \leq 1, |L_\alpha(w) \cap L_\beta(v)| \leq 1\} \\
B &= (E \times E) \setminus A.
\end{aligned}$$

Given $(v, w) \in A$, the pair can only be the last pair of at most one triple in $\Pi(E)$. This is of course only if $L_\alpha(v) \cap L_\beta(w)$ is a point in E. As there are no more than $|E|^2$ choices for pairs $(v, w) \in A$, the contribution to $\Pi(E)$ by point pairs in A is at most $|E|^2$

The analysis on the set of pairs in B is a bit more delicate. Consider an arbitrary pair, $(v, w) \in B$. Without loss of generality (possibly exchanging v with w or α with β) suppose $|L_\alpha(v) \cap L_\beta(w)| > 1$. Then, we get that

$$\begin{aligned}
|L_\alpha(v) \cap L_\beta(w)| &> 1 \\
\left|\left\{(x, y) \in R_q^2 : xv_x + yv_y = \alpha\right\} \cap \left\{(x, y) \in R_q^2 : xw_x + yw_y = \beta\right\}\right| &> 1 \\
\left|\left\{(x, y) \in R_q^2 : xv_x + yv_y = \alpha \text{ and } xw_x + yw_y = \beta\right\}\right| &> 1.
\end{aligned}$$

Namely, there will be more than one point with coordinates $(x, y) \in R_q^2$ satisfying

$$xv_x + yv_y = \alpha\left(\frac{xw_x + yw_y}{\beta}\right) = \frac{\alpha}{\beta}(xw_x + yw_y). \tag{2}$$

Note that β is a unit, and hence the quantity α/β is well defined. This restriction tells us that if $|L_\alpha(v) \cap L_\beta(w)| > 1$, then $|L_\alpha(v) \cap L_\beta(w')| = 0$, for any $w' \neq w$. This should not be surprising for if $\alpha = \beta$, then $L_\alpha(v) = L_\beta(w)$ forces $v = w$.

We pause for a moment to introduce an equivalence relation, say $\sim$, on the set of lines. Two lines $L_\alpha(v)$ and $L_\beta(w)$ are equivalent under $\sim$ if one can be translated to become a (possibly improper) subset of the other. It is clear that if $|L_\alpha(v) \cap L_\beta(w)| > 1$, then $L_\alpha(v) \sim L_\beta(w)$. The equivalence classes of $\sim$ keep track of the different "directions" that lines can have. So we can easily see that $L_\alpha(v) \sim L_\beta(v)$. Take note that if $R_q = \mathbb{Z}_q$, it is possible for two distinct lines to intersect in more than one point.

If $|L_\alpha(v) \cap L_\beta(w)| > 1$, then the pair (v, w) have no more than $\min\{|L_\alpha(v)|, |L_\beta(w)|\}$ possible choices for u to contribute a triple of the form (u, v, w) to $\Pi_{\alpha,\beta}(E)$. Now, we see that any other pair of points, say (v', w'), with $|L_\alpha(v') \cap L_\beta(w')| > 1$ and with $L_\alpha(v) \sim L_\alpha(v')$, will have $L_\alpha(v) \cap L_\alpha(v') = \emptyset$, and $L_\beta(w) \sim L_\beta(w')$, will have $L_\beta(w) \cap L_\beta(w') = \emptyset$. So any point u that contributes to a triple of the form $(u, v, w) \in \Pi_{\alpha,\beta}(E)$ can only contribute to a triple with a single pair (v, w) when $L_\alpha(v) \sim L_\beta(w)$.

Therefore, given any single equivalence class of $\sim$, there can be no more than $|E|$ choices for u to contribute a triple of the form (u, v, w) to $\Pi_{\alpha,\beta}(E)$ with $(v, w) \in B$. As there are no more than $|E|$ possible choices for equivalence classes of $L_\alpha(v)$ (as each point has only one associated equivalence class of $\sim$), there are no more than $|E|^2$ triples of the form $(u, v, w) \in \Pi_{\alpha,\beta}(E)$ with $(v, w) \in B$.

3.2 Proof of Theorem 4

Proof Let χ denote the canonical additive character of $\mathbb{F}_q$. By orthogonality, we have

$$\begin{aligned}
|\Pi_{\alpha,\beta}(E)| &= |\{(x, y, z) \in E \times E \times E : x \cdot y = \alpha, x \cdot z = \beta\}| \\
&= q^{-2} \sum_{s,t \in \mathbb{F}_q} \sum_{x,y,z \in E} \chi(s(x \cdot y - \alpha))\chi(t(\beta - x \cdot z)) \\
&= q^{-2} \sum_{s,t \in \mathbb{F}_q} \sum_{x,y,z \in E} \chi(s\alpha)\chi(-t\beta)\chi(x \cdot (sy - tz)) \\
&:= I + II + III,
\end{aligned}$$

where I is the term with $s = t = 0$, II is the term with exactly one of s or t equal to zero, and III is the term with s and t both nonzero. Clearly

$$I = q^{-2} \sum_{s=t=0} \sum_{x,y,z \in E} \chi(s\alpha)\chi(-t\beta)\chi(x \cdot (sy - tz)) = |E|^3 q^{-2}.$$

For the second and third sums, we need the following known results.

Lemma 1 [8] *For any set $E \subset \mathbb{F}_q^d$, we have the bound*

$$\sum_{s\neq 0}\sum_{x,y\in E}\chi(s(x\cdot y-\gamma)) \leq |E|q^{\frac{d+1}{2}}\lambda(\gamma), \tag{3}$$

where $\lambda(\gamma) = 1$ for $\gamma \in \mathbb{F}_q^*$ and $\lambda(0) = \sqrt{q}$. Furthermore, we have

$$\sum_{s,s'\neq 0}\sum_{\substack{y,y'\in E\\ sy=s'y'}}\chi(\alpha(s'-s)) \leq |E|q\lambda(\gamma). \tag{4}$$

Note that the quantities in the above Lemma can be shown to be real numbers, so there is no need for absolute values. Now, separating the II term into two sums, each with exactly one of s or t zero,

$$II = q^{-2}|E|\left(\sum_{s\neq 0}\sum_{x,y\in E}\chi(s(x\cdot y-\alpha)) + \sum_{t\neq 0}\sum_{x,z\in E}\chi(t(x\cdot z-\beta))\right)$$

From (3), it follows that $|II| \leq |E|^2 q^{\frac{d-3}{2}}(\lambda(\alpha)+\lambda(\beta))$. Finally, by the triangle-inequality, dominating a nonnegative sum over $x \in E$ by the same nonnegative sum over $x \in \mathbb{F}_q^d$, and applying Cauchy–Schwarz, we have

$$\begin{aligned}
|III| &\leq q^{-2}\sum_{x\in E}\left|\sum_{s\neq 0}\sum_{y\in E}\chi(s(x\cdot y-\alpha))\right|\left|\sum_{t\neq 0}\sum_{z\in E}\chi(t(x\cdot z-\beta))\right| \\
&\leq q^{-2}\sum_{x\in \mathbb{F}_q^d}\left|\sum_{s\neq 0}\sum_{y\in E}\chi(s(x\cdot y-\alpha))\right|\left|\sum_{t\neq 0}\sum_{z\in E}\chi(t(x\cdot z-\beta))\right| \\
&\leq q^{-2}\left(\sum_{x\in \mathbb{F}_q^d}\left|\sum_{s\neq 0}\sum_{y\in E}\chi(s(x\cdot y-\alpha))\right|^2\right)^{1/2} \\
&\quad\cdot\left(\sum_{x\in \mathbb{F}_q^d}\left|\sum_{t\neq 0}\sum_{z\in E}\chi(t(x\cdot z-\beta))\right|^2\right)^{1/2} \\
&=: q^{-2}III_\alpha\cdot III_\beta.
\end{aligned}$$

Now,

$$\begin{aligned} III_\alpha^2 &= \sum_{x\in\mathbb{F}_q^d}\left|\sum_{s\neq 0}\sum_{y\in E}\chi(s(x\cdot y-\alpha))\right|^2 \\ &= \sum_x \sum_{s,s'\neq 0}\sum_{y,y'\in E}\chi(s(x\cdot y-\alpha))\chi(-s'(x\cdot y'-\alpha)) \\ &= \sum_x \sum_{s,s'\neq 0}\sum_{y,y'\in E}\chi(\alpha(s'-s))\chi(x\cdot(sy-s'y')) \\ &= q^d \sum_{s,s'\neq 0}\sum_{\substack{y,y'\in E\\ sy=s'y'}}\chi(\alpha(s'-s)) \\ &\leq q^{d+1}|E|\lambda(\alpha)^2, \end{aligned}$$

by (4). Similarly, we have $III_\beta \leq \sqrt{q^{d+1}|E|}\lambda(\beta)$. Combining these estimates yields

$$|III| \leq q^{d-1}|E|\lambda(\alpha)\lambda(\beta).$$

This completes the proof as we have

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E|^3}{q^2} + R_{\alpha,\beta},$$

where

$$|R_{\alpha,\beta}| \leq |E|^2 q^{\frac{d-3}{2}}(\lambda(\alpha)+\lambda(\beta)) + q^{d-1}|E|\lambda(\alpha)\lambda(\beta).$$

3.3 Proof of Theorem 5

The proof will imitate that of Theorem 4, so we omit some of the details. Let $\chi(\sigma) = \exp(2\pi i\sigma/q)$ be the canonical additive character of $\mathbb{Z}_q$, and identify E with its characteristic function. We use the following known bounds for dot-product sets in $\mathbb{Z}_q^d$.

Lemma 2 [5] *Suppose that $E \subset \mathbb{Z}_q^d$, where $q = p^\ell$ is the power of an odd prime. Suppose that $\gamma \in \mathbb{F}_q^\times$ is a unit. Then, we have the following upper bounds.*

$$\sum_{j\in\mathbb{Z}_q\setminus\{0\}}\sum_{x,y\in E}\chi(j(x\cdot y-\gamma)) \leq 2|E|q^{\left(\frac{d-1}{2}\right)\left(2-\frac{1}{\ell}\right)+1} \tag{5}$$

and

$$\sum_{s,s'\in\mathbb{Z}_q\setminus\{0\}}\sum_{\substack{y,y'\in E\\ sy=s'y'}}\chi(\gamma(s'-s)) \leq 2|E|q^{\frac{\ell d-d+1}{\ell}} \tag{6}$$

Note 2 The authors in [5] actually gave a slightly different bound than those in Lemma 2. For example in (5), they showed

$$\sum_{j\in\mathbb{Z}_q\setminus\{0\}}\sum_{x,y\in E}\chi(j(x\cdot y-\gamma))\leq\sum_{i=0}^{\ell-1}|E|q^{\left(\frac{d-1}{2}\right)\left(1+\frac{i}{\ell}\right)}\leq\ell|E|q^{\left(\frac{d-1}{2}\right)\left(2-\frac{1}{\ell}\right)+1}.$$

However, summing the geometric series removes the factor of ℓ in the estimate. Likewise, a factor of ℓ can be removed from the estimate in (6).

We proceed as before. Write

$$|\Pi_{\alpha,\beta}|=\frac{|E|^3}{q^2}+II+III,$$

where

$$II:=|E|q^{-2}\left(\sum_{s\neq 0}\sum_{x,y\in E}\chi(s\cdot(x\cdot y-\alpha))+\sum_{t\neq 0}\sum_{x,z\in E}\chi(s\cdot(x\cdot z-\beta))\right)$$

and

$$III:=q^{-2}\sum_{x\in E}\left(\sum_{s\neq 0}\sum_{y\in E}\chi(-s\alpha)\chi(s(x\cdot y))\right)\left(\sum_{t\neq 0}\sum_{z\in E}\chi(-t\beta)\chi(t(x\cdot z))\right).$$

Applying Lemma 2, we see that

$$|II|\leq 4|E|^2q^{-2}q^{\frac{d(2\ell-1)+1}{2\ell}},$$

while

$$\begin{aligned}|III|&\leq q^{-2}\left(\sum_{x\in\mathbb{F}_q^d}\left|\sum_{s\neq 0}\sum_{y\in E}\chi(-s\alpha)\chi(s(x\cdot y))\right|^2\right)^{1/2}\\&\cdot\left(\sum_{x\in\mathbb{F}_q^d}\left|\sum_{t\neq 0}\sum_{z\in E}\chi(-t\beta)\chi(t(x\cdot z))\right|^2\right)^{1/2}\\&\leq 2|E|q^{-2}q^{\frac{\ell d-d+1}{\ell}}\leq 2|E|q^{-2}q^{\frac{d(2\ell-1)}{\ell}+\frac{1}{\ell}},\end{aligned}$$

where in the last line, we reason as in the proof of Theorem 4, except with Lemma 2 in place of Lemma 1. This completes the proof.

References

1. J.A. Alvarez-Bermejo, J.A. Lopez-Ramos, J. Rosenthal, D. Schipani, Managing key multicasting through orthogonal systems. J. Discrete Math. Sci. Cryptogr
2. P. Bahls, Channel assignment on Cayley graphs. J. Graph Theory **67**, 169–177 (2011), https://doi.org/10.1002/jgt.20523
3. D. Barker, S. Senger, Upper bounds on pairs of dot products. J. Comb. Math. Comb. Comput
4. J.J. Benedetto, M. Fickus, Finite normalized tight frames. Adv. Comput. Math. **18**, 357–385 (2003)
5. D. Covert, A. Iosevich, J. Pakianathan, Geometric configurations in the ring of integers modulo p^{ℓ}. Indiana Univ. Math. J. **61**, 1949–1969 (2012)
6. P. Erdős, E. Szemerédi, in *On Sums and Products of Integers*. Studies in Pure Mathematics (Birkhäuser, Basel, 1983), pp. 213–218
7. K. Ford, Integers with a divisor in an interval. Ann. Math. **168**(2), 367–433 (2008)
8. D. Hart, A. Iosevich, D. Koh, M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture. Trans. Am. Math. Soc. **363**(6), 3255–3275 (2011)
9. A. Iosevich, S. Senger, Orthogonal systems in vector spaces over finite fields. Electron. J. Comb. **15** (2008)
10. N.H. Katz, C.Y. Shen, A slight improvement to Garaev's sum product estimate. Proc. Am. Math. Soc. **136**(137), 2499–2504 (2008)
11. S.V. Konyagin, I.D. Shkredov, New results on sums and products in $\mathbb{R}$. Proc. Steklov Inst. Math. **294**, 78 (2016), https://doi.org/10.1134/S0081543816060055
12. T. Tao, The sum-product phenomenon in arbitrary rings. Contrib. Discrete Math. **4**(2), 59–82 (2009)