ADDITIVE AND MULTIPLICATIVE STRUCTURE IN MATRIX SPACES

[1] Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521
mcc@math.ucr.edu

Abstract. Let A be a set of N matrices. Let $g(A) := |A + A| + |A \cdot A|$, where $A+A = \{a_1+a_2 \mid a_i \in A\}$ and $A \cdot A = \{a_1a_2 \mid a_i \in A\}$ are the sumset and productset. We prove that if the determinant of the difference of any two distinct matrices in A is nonzero, then $g(A)$ cannot be bounded below by cN for any constant c. We also prove that if A is a set of $d \times d$ symmetric matrices, then there exists $\varepsilon = \varepsilon(d) > 0$ such that $g(A) > N^{1+\varepsilon}$. For the first result, we use the bound on the number of factorizations in a generalized progression. For the symmetric case, we use a technical proposition which provides an affine space V containing a large subset E of A with the property that if an algebraic property holds for a large subset of E, then it holds for V. Then we show that the system $\{a^2 : a \in V\}$ is commutative, allowing us to decompose $\mathbb{R}^d$ as eigenspaces simultaneously, so we can finish the proof with induction and a variant of Erdős-Szemerédi argument.

Introduction.

Let A be a finite subset of a ring, and let $|A|$ denote the cardinality of the set A. The *sum set* and the *product set* of A are

$$A + A := \{a_1 + a_2 \mid a_i \in A\},$$
$$A \cdot A := \{a_1a_2 \mid a_i \in A\}.$$

The study of the sizes of the sum and product sets started when Erdős and Szemerédi [ES] made their well-known conjecture for $A \subset \mathbb{Z}$ that there exists $\varepsilon > 0$ such that for

[1]partially supported by NSA grant No. MDA 904-03-1-0045.
2000 Mathematics Subject Classification. 05A99, 15A99.

$|A|$ sufficiently large,

$$|A+A|+|A\cdot A|>|A|^{2-\varepsilon}.$$

Recently a lot of work has been done in this subject. Cf [BC], [BKT], [C1]-[C5], [E], [ER], [ES], [F], [N1], [N2], [NT], [S]. All of these papers are about A being a subset of a division ring. In this paper we study the case when A is a set of matrices. The interesting point about matrices is that one can easily construct an arbitrarily large set with both sum set and product set "small". In fact, $|A+A|=|A\cdot A|=2|A|-1$, (see Remark 0.2.) We use the following

notations.

$\mathrm{Mat}(d)=\{d\times d$ matrices over $\mathbb{R}\}$ and

$\mathrm{Sym}(d)=\{d\times d$ symmetric matrices over $\mathbb{R}\}$.

We prove the following two theorems.

Theorem A. *Let $A\subset Mat(d)$ and $|A|=N$. If*

$$\det(a-a')\neq 0,\ \ \forall\, a\neq a'\in A, \tag{0.1}$$

then

$$|A+A|+|A\cdot A|>\phi(N)N,$$

where $\phi(N)\to\infty$ as $N\to\infty$.

Remark 0.1. Our hypothesis is vacuous for the case when A is contained in a division ring, because in that case, $a\neq a'$ if and only if $a-a'$ is invertible.

Theorem B. *For all d, there is $\varepsilon=\varepsilon(d)>0$ such that if $A\subset Sym(d)$ and $|A|=N$, then*

$$|A+A|+|A\cdot A|>N^{1+\varepsilon}.$$

Remark 0.2. The following set gives a counterexample for the sum-product conjecture for subsets of $\mathrm{SL}(d):=\{a:\det a=1\}$. Let

$$A=\Big\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}:k\in[1,N]\Big\}.$$

It is easy to see that $|A|=N$, $|A+A|=2N-1$ and $|A\cdot A|=2N-1$.

Roughly speaking, we prove Theorem A by assuming both $|A+A|$ and $|A\cdot A|$ are bounded by $K|A|$ with a bounded constant K. We use a bound (cf [C2]) on the number

of factorizations in a generalized progression to show that there is a large subset A_0 of A consisting of matrices with the same determinant. Then we use the fundamental theorem of algebra (see Lemma 1.2 and Proposition 1.3.) to show that there is an affine subspace V_0 containing a large subset A_1 of A_0 and that all matrices in V_0 have the same determinant. Then it is easy to see that the differences of matrices in A_1 all have determinant 0, contradicting to our hypothesis.

To prove Theorem B, we use a technical proposition (cf Proposition 2.1) under the assumption that the sumset of $A \subset \mathbb{R}^{d\times d}$ (matrix multiplication is not involved here.) is not big. The proposition provides an affine set V containing a subset E of A such that if an algebraic set Γ has sufficiently small degree and sufficiently large intersection with E, then $V \subset \Gamma$. Note that conditions on the rank of matrices and identities of matrices are all algebraic properties. Proposition 2.1 says that if a large subset of A has a certain algebraic property, then this affine subspace V has the same property. Using Proposition 2.1, we prove that $\{a^2 \colon a \in V\}$ forms a commutative multiplicative system. Therefore, we use this system to decompose $\mathbb{R}^d$ as eigen-subspaces, use regularization and use induction to finish the proof. For the initial step of the induction, we use a variant of Erdős-Szemerédi argument ([C4]). We also construct an example of a linear space $V_j \subset \mathrm{Sym}(d)$ with $\dim(V_j) = j$, for any j and with $a^2 \in \mathbb{R}\mathbf{1}$ for any $a \in V_j$. (See Remark 5.2.)

The paper is organized as follows. In Section 1, we prove Theorem A. In Section 2, we prove Proposition 2.1 which allows us to find a large subset of A with nice properties. In Section 3, we give the definition of a good pair (A, V) and prove that the cancellation law for multiplication holds for a good A. In Section 4, we show that $\{a^2 \colon a \in V\}$ is a commutative multiplicative system.

In section 5, we give the proof of Theorem B.

Notation.

$\det(A) = \{\det a : a \in A\}$, for $A \subset \mathrm{Mat}(d)$.

$p(S) = \{p(s_1, \cdots, s_m) \colon (s_1, \cdots, s_m) \in S\}$, for $S \subset \mathbb{R}^m$ and polynomial $p(x_1, \cdots, x_m)$.

$[1, J\,] = \{1, 2, \cdots, J\}$

$\log_k M = \log\log\cdots\log M$, k-fold iterated logarithm function

$d(x) \ll f(x)$ means $f(x) \geq 0$ and $|d(x)| \leq cf(x)$ for some constant c.

Section 1.

First, we will show that if a polynomial in m variables vanishes at a large subset of a generalized progression in $\mathbb{R}^m$, then it vanishes at an affine space of $\mathbb{R}^m$. (See Proposition 1.3.)

We start with a lattice version of the fundamental theorem of algebra for multivariable polynomials.

Lemma 1.1. *Let $S \subset [1, J_1] \times \cdots \times [1, J_k]$, with*

$$|S| > \frac{1}{c} J_1 \cdots J_k, \tag{1.1}$$

and let $p(x_1, \cdots, x_k)$ be a polynomial of degree D, with

$$D < \frac{J_i}{4^{k-1}c}, \forall i. \tag{1.2}$$

If $p(S) = \{0\}$, then $p \equiv 0$.

Proof. Let $S_{j_1,\cdots,j_{k-1}} = \{j_k : (j_1, \cdots, j_k) \in S\}$ be the fiber of S over $(j_1, \cdots, j_{k-1})$.

Define

$$T = \Big\{(j_1, \cdots, j_{k-1}) : |S_{j_1,\cdots,j_{k-1}}| > \frac{J_k}{2c}\Big\}. \tag{1.3}$$

A straightforward averaging argument implies that

$$|T| > \frac{J_1 \cdots J_{k-1}}{2c}.$$

We write

$$p(x_1, \cdots, x_k) = \sum_{i=0}^{d} p_i(x_1, \cdots, x_{k-1}) x_k^i.$$

For any $(j_1, \cdots, j_{k-1}) \in T$, $p(j_1, \cdots, j_{k-1}, x_k)$ is a polynomial in x_k, of degree $\leq D$, vanishing at the set $S_{j_1,\cdots,j_{k-1}}$ of size $> \frac{J_k}{2c} > D$. So its coefficients $p_i(j_1, \cdots, j_{k-1}) = 0$, i.e. $p_i(T) = \{0\}$. Applying induction on $\sum p_i^2$ (which has degree $\leq 2D < \frac{J_i}{4^{k-2}2c}$), we have $p_i \equiv 0, \forall i$. Hence $p \equiv 0$. $\square$

The next lemma is the lattice version of Proposition 1.3, our main technical tool to prove Theorem A.

Lemma 1.2. *Let $S \subset [1, J_1] \times \cdots \times [1, J_k]$, with*

$$|S| > \frac{1}{cN^{\varepsilon}} J_1 \cdots J_k,$$

and let $p(x_1, \cdots, x_k)$ be a polynomial of degree D, such that $p(S) = \{0\}$. Then there is an affine space $W \subset \mathbb{R}^k$ such that $p(W) = \{0\}$ and

$$|W \cap S| > \frac{J_1 \cdots J_k}{(cN^\varepsilon)^k D^{k-1} 2^{k(k-1)}}.$$

Proof. If $4^{k-1}(cN^\varepsilon)D < J_i$, for all i, then the lemma follows from Lemma 1.1. So we may assume

$$4^{k-1}(cN^\varepsilon)D \geq J_k. \tag{1.4}$$

Let $S_{j_k} = \{(j_1, \cdots, j_{k-1}) \colon (j_1, \cdots, j_k) \in S\}$. We fix $j_k \in [1, J_k]$ such that

$$|S_{j_k}| \geq \frac{|S|}{J_k} > \frac{1}{cN^\varepsilon} J_1 \cdots J_{k-1}.$$

The polynomial $\tilde{p} = p(x_1, \cdots, x_{k-1}, j_k)$ vanishes at S_{j_k}. Induction implies that there is an affine subspace $\widetilde{W} \subset \mathbb{R}^{k-1}$ such that $\tilde{p}(\widetilde{W}) = \{0\}$ and

$$|\widetilde{W} \cap S_{j_k}| > \frac{J_1 \cdots J_{k-1}}{(cN^\varepsilon)^{k-1} D^{k-2} 2^{(k-1)(k-2)}}. \tag{1.5}$$

Let $W = \widetilde{W} \times \{j_k\}$. Then

$$|W \cap S| \geq |\widetilde{W} \cap S_{j_k}| > \frac{J_1 \cdots J_{k-1}}{(cN^\varepsilon)^{k-1} D^{k-2} 2^{(k-1)(k-2)}} \frac{J_k}{4^{k-1}(cN^\varepsilon)D}.$$

The last inequality follows from (1.4) and (1.5). □

Let $b_1, \cdots, b_k \in \mathbb{R}^m$ be independent vectors. We have the following

Proposition 1.3. *Let $A_0 \subset P = \{j_1 b_1 + \cdots j_k b_k : j_i \in [1, J_i]\}$, where $N \leq \prod_{i=1}^k J_i \leq c_1 N$ for some $N \in \mathbb{N}$, and $|A_0| > \frac{1}{c_2} N^{1-\varepsilon}$ for some $\varepsilon \geq 0$. Let $F(x_1, \cdots, x_m) \in \mathbb{R}[x_1, \cdots, x_m]$ be a polynomial of degree D and $F(A_0) = \{0\}$. Then there is an affine space $V_0 \subset \mathbb{R}^m$ such that $F(V_0) = \{0\}$ and*

$$|V_0 \cap A_0| > \frac{1}{(c_1 c_2 D 2^{k-1})^k D^{-1}} N^{1-k\varepsilon}.$$

In particular, if $\varepsilon = 0$, then $|V_0 \cap A_0| > \frac{1}{(c_1 c_2 D 2^{k-1})^k D^{-1}} N$.

Proof. Let

$$S = \{(j_1, \cdots, j_k) \in [1, J_1] \times \cdots \times [1, J_k] : j_1 b_1 + \cdots + j_k b_k \in A_0\}.$$

Then

$$|S| = |A_0|.$$

Applying Lemma 1.2, with $c = c_1 c_2$ and $p(j_1, \cdots, j_k) = F(j_1 b_1 + \cdots + j_k b_k)$, we have $W \subset \mathbb{R}^k, p(W) = \{0\}$ and $|W \cap S| > \frac{J_1 \cdots J_k}{(cN^\varepsilon)^k D^{k-1} 2^{k(k-1)}}$. Let V_0 be the corresponding set in $\mathbb{R}^m$ of W. Then V_0 is affine, $F(V_0) = \{0\}$ and

$$|V_0 \cap A_0| = |W \cap S| > \frac{N}{(cN^\varepsilon D 2^{k-1})^k D^{-1}} = \frac{1}{(c_1 c_2 D 2^{k-1})^k D^{-1}} N^{1-k\varepsilon}. \qquad \square$$

The next two theorems will be used in the proof of Proposition 1.5.

Freiman-Ruzsa Thoerem. $[Bi], [R]$ *Let A be a set of N elements contained in a torsion-free abelian group G with $|A+A| < KN$. Then A is contained in a generalized progression in G, i.e. there are $b_1, \cdots, b_r \in G$ such that*

$$A \subset P = \{j_1 b_1 + \cdots + j_r b_r : j_i \in [1, J_i]\}, \tag{1.6}$$

$r \leq K$ and $\prod J_i = |P| < c(K)N$, where $c(K)$ is a constant depending on K.

Factorization Theorem. $[C2]$ *Let P be a generalized progression as in (1.6), and let $J = \max J_i$. Then $\forall n \in \mathbb{C} \setminus \{0\}$, the number of factorizations of n with factors in P is $< J^{\frac{c}{\log_2 J}}$, where $c = c(r, J)$ is a constant depending on r, J.*

Lemma 1.4. *Let $A \subset Mat(d)$ with $|A| = N$.*

If

$$|A + A| < KN,$$

then $\det(A)$ *is contained in a generalized progression Q with* $\dim Q \leq \binom{d+K-1}{d}$ *and* $|Q| \leq N^{d\binom{d+K-1}{d}}$.

Proof. Freiman-Ruzsa Theorem implies that there are $b_1, \cdots, b_r \in Mat(d)$ such that A is contained in a generalized progression P generated by $b_1, \cdots, b_r$, with r and $|P|$ bounded. Let $b_{i[k,j]}$ be the (k,j)-entry of matrix b_i. Then

$$\begin{aligned} \det\Big(\sum_{i=1}^{r} j_i b_i\Big) &= \sum_{\pi \in S_d} (-1)^{\sigma(\pi)} \prod_{k=1}^{d} \Big(\sum_i j_i b_i\Big)_{[k,\pi(k)]} \\ &= \sum_{\pi \in S_d} (-1)^{\sigma(\pi)} \prod_{k=1}^{d} \Big(\sum_i j_i b_{i[k,\pi(k)]}\Big), \end{aligned}$$

where S_d is the symmetric group on d letters.

We view $\det(\sum_{i=1}^r j_i b_i)$ as a homogeneous polynomial in $j_1 \cdots j_r$,

$$\det\Big(\sum_{i=1}^{r} j_i b_i\Big) = \sum_{\alpha_1+\cdots+\alpha_r=d} j_1^{\alpha_1}\cdots j_r^{\alpha_r}\gamma_\alpha,$$

where γ_α is a linear combination of the products of d of the entries $b_{i[k,\pi(k)]}$. Therefore, $\det(A)$ is contained in the progression Q generated by the γ_α's, and $\dim Q \le \binom{d+K-1}{d}$, $|Q| \le N^{d\binom{d+K-1}{d}}$ $\square$

Proposition 1.5. *Let $A \subset \mathrm{GL}(d)$ with $|A| = N$.*

If

$$|A + A| < KN \tag{1.7}$$

and

$$|A \cdot A| < KN, \tag{1.8}$$

then there is $\beta \in \mathbb{R}$ and $A_0 \subset A$ with $|A_0| > \frac{1}{K} N^{1-\frac{c}{\log_2 N}}$, such that $\det(A_0) = \{\beta\}$.

Proof. Inequality (1.8) implies that there is $b \in A \times A$ such that

$$|\{(a_1, a_2) \in A \times A : b = a_1 a_2\}| > \frac{N}{K}.$$

We consider the composite map $A \times A \to \det(A) \times \det(A) \to \det(A) \cdot \det(A)$ given by $(a_1, a_2) \to (\det a_1, \det a_2) \to \det a_1 \det a_2$, and look at the fiber at $\beta := \det b \in \det(A) \cdot \det(A)$. The lemma follows from applying the Factorization Theorem on the generalized progression Q gotten in Lemma 1.4 with $n = \det a$ for any $a \in A$.

Proposition 1.6. *Let $A_0 \subset Mat(d)$. Suppose A_0 is contained in a generalized progression as in* (1.6) *and $|A_0| > \frac{1}{c_2} N^{1-\varepsilon}$ for some $\varepsilon \ge 0$. If $\det(A_0) = \{\rho\}$, then there is a linear space $V \subset Mat(d)$, and $A_1 \subset A_0$ with $|A_1| > \frac{1}{c} N^{1-r\varepsilon}$, such that $\det(V) = \{0\}$ and $a - a' \in V$ for $a, a' \in A_1$. Here $c = c(c(K), c_2, d, r)$.*

Proof. Let $F = \det - \beta$. i.e.

$$F(x_{11}, \cdots, x_{dd}) = \sum_{\pi \in S_d} (-1)^{\sigma(\pi)} x_{1,\pi(1)} \cdots x_{d,\pi(d)} - \beta.$$

Then Lemma 1.3 applied to F gives the existence of $V_0 \subset Mat(d)$, such that $\det(V_0) = \{\beta\}$ and $|V_0 \cap A_0| > \frac{1}{c} N^{1-r\varepsilon}$, where $c = c(c(K), c_2, r, d)$.

Write $V_0 = a_0 + V$, where V is a linear space. Then $\forall\ a \in V$ and $\forall\ t \in \mathbb{R}$, $\det(a_0 + ta) = \beta$. Therefore, $\det a = 0$. i.e. $\det(V) = \{0\}$.

Let $A_1 = V_0 \cap A_0$. Then $|A_1| \gtrsim N^{1-r\varepsilon}$ and $a - a' \in V, \forall\ a, a' \in A_1$. $\square$

Proof of Theorem A. We assume that there is a constant K such that (1.7) and (1.8) hold. Freiman-Ruzsa Theorem provides the existence of a generalized progression P as in (1.6) which contains any subset of A. Then we use Proposition 1.6 to get a contradiction to hypothesis (0.1).

Case 1. $|A \cap \mathrm{GL}(d)| > \frac{N}{2}$.

We apply Propositions 1.5 and 1.6 to $\widetilde{A} = A \cap \mathrm{GL}(d)$ and note that $|2\widetilde{A}| < 2K|\widetilde{A}|$ and $|\widetilde{A}^2| < 2K|\widetilde{A}|$.

Case 2. $|A \cap \mathrm{GL}(d)| \leq \frac{N}{2}$.

We let

$$A_0 = \{a \in A \colon \det a = 0\}.$$

Then

$$|A_0| > \frac{N}{2},$$

and we apply Proposition 1.6 directly on A_0. $\square$

Our goal in the rest of the paper is to prove Theorem B.

Section 2.

In this section we will prove the following technical proposition.

Proposition 2.1. *Let $A \subset \mathbb{R}^m$ be a finite set, $|A| = N$ and*

$$|A + A| < KN \tag{2.1}$$

with

$$\log K \ll \log N.$$

Then there is $E \subset A$ and an affine space $V \subset \mathbb{R}^m$ such that

(*i*) $\frac{|E|}{|A|} = \delta > K^{-c}$, *where* $c = c(m)$

(*ii*) $E \subset V$

(*iii*) *If $\Gamma \subset \mathbb{R}^m$ is algebraic of degree $< m^{10}$ and*

$$|\Gamma \cap E| > \delta^{10} K^{-10} |E|, \tag{2.2}$$

then

$$V \subset \Gamma.$$

Before we give the proof, we will recall some definitions and facts about algebraic sets. A set $\Gamma \subset \mathbb{R}^m$ is *algebraic*, if it is the common zero sets of a collection of polynomials. We say Γ is *irreducible*, if it cannot be expressed as the union $\Gamma = \Gamma_1 \cup \Gamma_2$ of two proper algebraic subsets. We define the *dimension* of Γ to be the maximum of all integers n such that there exists a chain $\Gamma_0 \subset \Gamma_1 \subset \ldots \subset \Gamma_n$ of distinct irreducible algebraic subsets of Γ. The *degree* of Γ is the number of points of intersection of Γ with a sufficiently general linear space L of dimension $m - \dim \Gamma$. An irreducible linear space either is contained in Γ or intersects Γ at no more than $\deg \Gamma$ many points.

Proof of Proposition 2.1. There are two steps in the proof. Assumption (2.1) will only be used in the second step.

Step 1. We start by proving a weaker version of the theorem, in which an algebraic set W is obtained instead of an affine set V. An additional argument using the small doubling property will allow us to deduce that W can in fact be taken to be affine. Therefore, we will first construct $E \subset A$ satisfying (i) and an algebraic set $W \supset E$ (cf (ii)) such that

(iii') $\deg W < m^{10}$ and $W \subset \Gamma$ for any algebraic set $\Gamma \subset \mathbb{R}^m$, with $\deg \Gamma < m^{10}$, satisfying (2.2).

This construction is straightforward and by induction.

For $i = 0$, we take $E_0 = A, W_0 = \mathbb{R}^m$. Hence $\delta_0 = 1$. If (iii$'$) does not hold, there is a Γ_0 algebraic such that

$$\deg \Gamma_0 < m^{10}, \tag{2.3}$$

$$|\Gamma_0 \cap E_0| > \delta_0^{10} K^{-10} |E_0| \,, \tag{2.4}$$

and

$$W_0 \not\subset \Gamma_0. \tag{2.5}$$

Note the fact that $W_0 = \mathbb{R}^m$ and (2.5) imply

$$\dim \Gamma_0 < m. \tag{2.6}$$

Let W_1 be an irreducible component of $\Gamma_0 = \Gamma_0 \cap W_0$ such that

$$\begin{aligned} |W_1 \cap E_0| &\geq \frac{1}{\deg \Gamma_0 \cap W_0} \, |(\Gamma_0 \cap W_0) \cap E_0| \\ &> \frac{1}{\deg \Gamma_0} \, K^{-10} |E_0| \\ &> m^{-10} K^{-10} |E_0|. \end{aligned} \tag{2.7}$$

The last two inequalities follow from (2.3) and (2.4).

Take $E_1 = W_1 \cap E_0$. Inequalities (2.6) and (2.7) give $m_1 := \dim W_1 \leq \dim \Gamma_0 < m$, and $\delta_1 := \frac{|E_1|}{N} > m^{-10}K^{-10}$. If (iii′) fails again, there is $\Gamma_1 \not\supset W_1$, with $\deg \Gamma_1 < m^{10}$ so that

$$|\Gamma_1 \cap E_1| > \delta_1^{10} K^{-10} |E_1|.$$

Similarly, let W_2 be an irreducible component of $\Gamma_1 \cap W_1$ such that

$$\begin{aligned} |W_2 \cap E_1| &\geq \frac{1}{\deg(\Gamma_1 \cap W_1)} \, |(\Gamma_1 \cap W_1) \cap E_1| \\ &> \frac{1}{\deg \Gamma_1} \, |\Gamma_1 \cap E_1| \\ &> m^{-10} \delta_1^{10} K^{-10} |E_1|. \end{aligned} \tag{2.7}$$

The fact that $W_2 \subset \Gamma_1 \cap W_1 \neq W_1$ implies

$$m_2 := \dim W_2 < \dim W_1 = m_1.$$

Take $E_2 = W_2 \cap E_1$. Then

$$\delta_2 := \frac{|E_2|}{N} = \frac{|E_2|}{|E_1|} \, \delta_1 > m^{-10} \, \delta_1^{11} K^{-10}.$$

The process terminates after $s < m$ steps, and we obtain $E = E_s, W = W_s$, such that $W \subset \Gamma$ for all Γ algebraic,with $\deg \Gamma < m^{10}$, satisfying (2.2).

Also

$$\delta = \delta_s := \frac{|E_s|}{N} = \frac{|E_s|}{|E_{s-1}|} \, \delta_{s-1} > m^{-10} \delta_{s-1}^{11} K^{-10}. \tag{2.8}$$

Step 2.

Now we will show that W obtained in Step 1 is an affine space.

We define

$$r(\xi) = |\{(a_1, a_2) \in E \times E : \xi = a_1 - a_2\}| = |E \cap (E + \xi)|. \tag{2.9}$$

Then

$$|E|^2 = \sum_{\xi \in E - E} r(\xi) = \sum |E \cap (E + \xi)|. \tag{2.10}$$

The first equality and Cauchy-Schwartz imply that

$$\sum_{\xi\in E-E} r(\xi)^2 \geq \frac{|E|^4}{|E-E|}. \tag{2.11}$$

Let

$$B = \{\xi \in E-E:\ r(\xi) > \frac{|E|^2}{2|E-E|}\} \subset E \setminus E. \tag{2.12}$$

Therefore,

$$\sum_{\xi\in (E-E)\setminus B} r(\xi)^2 \leq \Big(\frac{|E|^2}{2|E-E|}\Big)^2 |E-E|. \tag{2.13}$$

Putting (2.11) and (2.13) together, we have

$$|B|\ |E|^2 \geq \sum_{\xi\in B} r(\xi)^2 > \frac{3|E|^4}{4|E-E|}.$$

Hence

$$|B| > \frac{3|E|^2}{4|E-E|}\ . \tag{2.14}$$

On the other hand, from (2.1) and (i), we have

$$|E+E| \leq |A+A| < KN = K\delta^{-1}|E|.$$

Applying Theorem 8.4 in [N3], we get

$$|E-E| < (K\delta^{-1})^2|E|. \tag{2.15}$$

Both (2.14) and (2.15) will be used in the proof of Claim 3 later.

Claim 1. *$W = W+\xi$, for all $\xi \in B$.*

Proof of Claim 1. Let $\xi \in B$ and let $\Gamma = W \cap (W+\xi)$. Then the fact that $W \supset E$ and (2.9), (2.12), (2.15) give

$$\begin{aligned} |\Gamma \cap E| = |E \cap W \cap (W+\xi)| &\geq |E \cap (E+\xi)| \\ &= r(\xi) > \frac{|E|^2}{2|E-E|} > \frac{\delta^2}{2K^2}|E|. \end{aligned}$$

Therefore, $W \subset \Gamma$ by (iii′). Namely,

$$W \subset W+\xi.$$

On the other hand, $-B = B$ implies that

$$W \subset W-\xi.$$

Hence $W = W+\xi$. $\square$

Claim 2. $W = W + \langle B\rangle$.

Proof of Claim 2. It follows from Claim 1 that

$$W = W + r\xi, \forall r \in \mathbb{Z}.$$

Since $W - W$ is algebraic, the line $\langle\xi\rangle$ either is contained in $W - W$ or intersects $W - W$ no more than $\deg W - W$ many points. Therefore $\langle\xi\rangle \subset W - W$. Namely,

$$W = W + \langle\xi\rangle,\ \forall\xi \in B.$$

Hence $W = W + \langle B\rangle$. $\square$

Claim 3. *There is an $x_0 \in E \subset W$ such that*

$$|(E - x_0) \cap B| > \frac{|E|}{4(K')^4} = \frac{3\delta^4}{8K^4}|E|.$$

Proof of Claim 3. This is because of the following estimate

$$\begin{aligned}\sum_{x\in E} |(E-x)\cap B| &= \sum_{\xi\in B} |\{(x', x)\colon x' - x = \xi\}| \\ &= \sum_{\xi\in B} r(\xi) \\ &> \frac{|E|^2}{2|E-E|}|B| \\ &> \frac{3|E|^4}{8|E-E|^2} \\ &> \frac{3\delta^4|E|^2}{8K^4}\end{aligned}$$

The last two inequalities are by (2.14) and (2.15). $\square$

Let $V = x_0 + \langle B\rangle$, where x_0 is as in Claim 3. Note that as an algebraic set, $\deg V = 1$. Claim 2 implies that $V \subset W$. To see that $W \subset V$, we use Step 1. Inequality (2.2) in (iii′) is satisfied because

$$|E \cap V| > |E \cap (x_0 + B)| > \frac{3\delta^4}{8K^4}|E|.$$

Hence $W = V$, an affine space.

This completes the proof of Proposition 2.1. $\square$

Section 3.

We will show that cancellation law for multiplication holds for A satisfying (1)-(3) below. (See the definition of *good pair*.)

Recall (cf [BC]) that for a set A with $|A| = N$, the *doubling constants* for addition and multiplication are

$$K_+(A) = \frac{|A+A|}{N}, \quad K_\times(A) = \frac{|A \cdot A|}{N}.$$

Let $A \subset Sym(d)$ and assume $\log[K_+(A) + K_\times(A)] \ll \log N$.

Applying Proposition 2.1 to the set A with

$$K = d^{1+\frac{1}{10}}\big(K_+(A) + K_\times(A)\big), \tag{3.0}$$

we obtain $E \subset A$ and an affine space V satisfying (i)-(iii).

Since by (i), $K_+(E) < \delta^{-1}K_+(A)$ and $K_\times(E) < \delta^{-1}K_\times(A)$, (iii) implies that if $\Gamma \subset \mathrm{Mat}(d)$ is algebraic of $\deg \Gamma < d^{20}$ and satisfies

$$|\Gamma \cap E| > \frac{|E|}{d^{11}[K_+(E) + K_\times(E)]^{10}}, \tag{3.1}$$

then $\Gamma \supset V$.

Let

$$E = \bigcup_{r=1}^{d} E_r, \text{ with } E_r = \{a \in E\colon \operatorname{rank} a = r\}.$$

Fix $r \le d$ such that

$$|E_r| \ge \frac{|E|}{d} = \frac{\delta N}{d}. \tag{3.2}$$

Assume $r < d$.

Let $D_{I,J}(a)$ be the determinant of the $(r+1) \times (r+1)$ matrix obtained by deleting $d-(r+1)$ rows I and $d-(r+1)$ columns J from a. Then rank $a \le r$ if and only if

$$F(a) := \sum_{I,J} D_{I,J}(a)^2 = 0.$$

$F = F(x_{11}, \cdots, x_{dd})$ is a polynomial on $\mathbb{R}^{d\times d}$ of degree $2(r+1)$. Let $(F)_0$ be the zero set of F. Since

$$|(F)_0 \cap E| \geq |E_r| \geq \frac{|E|}{d},$$

Proposition 2.1 holds. Cf (3.1). Therefore

$$V \subset (F)_0,$$

meaning that

$$\operatorname{rank} a \leq r \text{ for all } a \in V.$$

We will work on E_r instead of A. The inequality in (3.2) implies that

$$K_*(E_r) < d\, K_*(E), \tag{3.3}$$

where $K_* = K_+$ or $K_\times$.

Inequality (2.2) may be replaced by

$$|\Gamma \cap E_r| > \frac{|E_r|}{|(K_+(E_r) + K_\times(E_r))^{10}},$$

because (3.1), (3.2) and (3.3) hold.

Definition. *The pair (A, V) is called good, if the following hold.*

(1) *$A \subset V \subset$ Sym(d), A finite, and V is affine*

(2) *rank $a \leq r, \forall a \in V$, and rank $a = r, \forall a \in A$ for some $r \leq d$*

(3) *for any algebraic set $\Gamma \subset \mathbb{R}^{d\times d}$ with $\deg \Gamma < d^{20}$, if*

$$|\Gamma \cap A| > \frac{|A|}{|(K_+(A) + K_\times(A))^{10}},$$

then $\Gamma \supset V$.

$\big(K_+(A)$ and $K_\times(A)$ are the doubling constants of $A.\big)$

For the rest of the paper, we work on a good pair A, V.

Proposition 3.1. *Let A be as above and let $a, b, c \in A$. If $b \neq c$, then $ab \neq ac$.*

Proof. If $r = d$, the statement is obvious. Assume $r < d$.

Let o be the orthogonal matrix formed by the orthonormal eigenvectors of a such that

$$o^{-1}ao = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & \mathbf{0} & \\ & & \lambda_r & & & \\ & & & 0 & & \\ & \mathbf{0} & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

where $\lambda_1 \cdots \lambda_r \neq 0$.

Since $A \subset V = v_0 + V_0, V_0$ being linear,

$$w := b - c \in V_0, \text{ and } a + tw \in V \text{ for } t \in \mathbb{R}.$$

Let $(w_{i,j}) = o^{-1}wo$.

Claim 1. *$w_{k,\ell} = 0$ for all $k, \ell \in \{r+1, \ldots, d\}$*

Proof of Claim. We note that rank $(a + tw) \leq r$ implies that

$$\text{rank} \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & \mathbf{0} & \\ & & \lambda_r & & & \\ & & & 0 & & \\ & \mathbf{0} & & & \ddots & \\ & & & & & 0 \end{pmatrix} + t(w_{i,j}) \leq r.$$

Let $D^{k,\ell}$ be the determinant of the $(r+1) \times (r+1)$ submatrix of $o^{-1}(a+tw)o$ obtained by deleting the p-th rows for all $p \in \{r+1, \cdots, d\} \setminus \{k\}$ and q-th columns for all $q \in \{r+1, \cdots, d\} \setminus \{\ell\}$. So $D^{k,\ell}$ is a polynomial in t vanishing identically. In particular, the coefficient of t is zero. i.e.

$$w_{k\ell} \prod_{i=1}^{r} \lambda_i = 0.$$

Therefore, $w_{k,\ell} = 0$. $\square$

If $aw = 0$, then

$$o^{-1}(aw)o = (o^{-1}ao)(o^{-1}wo) = (\lambda_i w_{i,j}) = 0.$$

Since $\prod_{i=1}^{r} \lambda_i \neq 0$,, we have $w_{i,j} = 0$ for $i = 1, \cdots, r$ and for all j. Now the proposition follows from Claim 1 and a being symmetric. $\square$

Section 4.

In this section we will study the multiplicative structure of V. Our goal is to prove the following

Proposition 4.1. *Let $A \subset V$ be a good pair. Then*

$$\{a^2 : a \in V\}$$

is commutative under multiplication.

The proof will use Proposition 2.1 several times.

Lemma 4.2. *Let*

$$S_0 = \{(a_1, a_2, a_3) \in A \times A \times A : a_1a_2a_3 \in a_3Aa_3\}.$$

Then

(a) $|S_0| > \frac{N^3}{K_\times(A)}$

(b) $\forall (a_1, a_2, a_3) \in S_0, a_1a_2a_3 = a_3a_2a_1$

Proof. Part (b) is obvious. To show (a), we note that by Proposition 3.1, there is a one-to-one correspondence between S_0 and

$$T = \{(a_1, a_2, a_3, a_4) \in A \times \cdots \times A : \ a_1a_2 = a_3a_4\}.$$

So we will bound $|T|$ instead.

Let $r(n) = |\{(a_1, a_2) : n = a_1a_2\}|$. Then

$$\sum_{n \in A \cdot A} r(n) = N^2, \qquad |T| = \sum_{n \in A \cdot A} r(n)^2$$

and Cauchy-Schwartz imply $|T| \geq \frac{N^4}{|A \cdot A|} = \frac{N^3}{K_\times(A)}$. $\square$

We will work on

$$S = \{(a_1, a_2, a_3) \in A \times A \times A : a_1a_2a_3 = (a_1a_2a_3)^T\}.$$

By Lemma 4.2,

$$|S| \geq \frac{N^3}{K_\times(A)}.$$

Lemma 4.3. *For $a_2, a_3 \in A$, let*

$$\begin{aligned}\Gamma_{a_2,a_3} &= \langle a : aa_2a_3 = a_3a_2a\rangle,\\ S(a_2,a_3) &= \{a_1 \in A\colon (a_1,a_2,a_3) \in S\},\\ S_{2,3} &= \big\{(a_2,a_3) \in A\times A|\ |S(a_2,a_3)| > \frac{N}{2K_\times(A)}\big\}.\end{aligned}$$

Then

(a) $|S_{2,3}| > \frac{N^2}{2K_\times(A)}$

(b) $S(a_2,a_3) = A \cap \Gamma_{a_2,a_3}$

(c) $V \subset \Gamma_{a_2,a_3}, \forall (a_2,a_3) \in S_{2,3}$.

Proof. (a) follows from a straightforward averaging argument. (b) is obvious. (c) holds, because of (b) and that (A,V) being a good pair.

Remark 4.3.1. The meaning of (c) is that $a_1a_2a_3 = a_3a_2a_1$ holds for all $a_1 \in V$, $(a_2,a_3) \in S_{2,3}$.

Lemma 4.4. *Let*

$$\begin{aligned}S_{2,3}(a_3) &= \{a_2 \in A :\ (a_2,a_3) \in S_{2,3}\}\\ S_3 &= \big\{a_3 \in A :\ |S_{2,3}(a_3)| > \frac{N}{4K_\times(A)}\big\}\\ \Gamma^{a_1}_{a_3} &= \langle a :\ a_1aa_3 = a_3aa_1\rangle,\ \textit{for } a_3 \in S_3, a_1 \in V.\end{aligned}$$

Then

(a) $|S_3| > \frac{N}{4K_\times(A)}$

(b) $S_{2,3}(a_3) \subset A \cap \Gamma^{a_1}_{a_3}$

(c) $V \subset \Gamma^{a_1}_{a_3}$.

Proof. Same reasoning as in the proof of Lemma 4.3.

Remark 4.4.1. The meaning of (c) is that $a_1a_2a_3 = a_3a_2a_1$ holds for all $a_1, a_2 \in V$, $a_3 \in S_3$.

Proof of Proposition 4.1. For $a_1, a_2 \in V$, define

$$\Gamma^{a_1,a_2} = \langle a :\ a_1a_2a = aa_2a_1\rangle.$$

Then $S_3 \subset A \cap \Gamma^{a_1 \cdot a_2}$.

(A, V) being a good pair and Lemma 4.4 (a) imply $V \subset \Gamma_3$, i.e.

$$a_1 a_2 a_3 = a_3 a_2 a_1, \text{ for all } a_1, a_2, a_3 \in V. \tag{4.5}$$

In particular

$$a_1^2 a_2 = a_2 a_1^2 \tag{4.6}$$

$$a_1^2 a_2^2 = a_2^2 a_1^2 \tag{4.7}$$

for all $a_1, a_2 \subset V$.

Thus $\{a^2 | a \in V\}$ are commutative symmetric matrices. $\square$

Section 5.

In this section we will conclude the proof of Theorem B. Let

$$\mathbb{R}^d = \oplus H_\alpha$$

be the eigenspace decomposition by the commutative system $\{a^2 : a \in V\}$ such that if $a \in V, x \in H_\alpha$, then

$$a^2(x) = \lambda_\alpha(a) x$$

with $\lambda_\alpha(a) \in \mathbb{R}$ and also, if $\alpha \neq \beta$, then

$$\lambda_\alpha(a) \neq \lambda_\beta(a) \text{ for some } a \in V. \tag{5.1}$$

Returning to (4.6), we have for $x \in H_\alpha$

$$a_1^2(a_2 x) = \lambda_\alpha(a_1)(a_2 x)$$

so that

$$a_2 x \in \underset{\lambda_\beta(a_1) = \lambda_\alpha(a_1)}{\oplus} H_\beta. \tag{5.2}$$

Since (5.2) holds for all $a_2 \in V$ and (5.1) holds, necessarily

$$a_2 x \in H_\alpha, \qquad \forall x \in H_\alpha, \forall a_2 \in V.$$

Thus H_α is invariant for all $a \in V$.

Let $d_\alpha = \dim H_\alpha$, with $\sum d_\alpha \leq d$, we get a decomposition

$$a = \underset{\alpha}{\oplus} a^{(\alpha)}, \quad a^{(\alpha)} \in \text{ Sym}(d_\alpha) \cap \text{ GL}(d_\alpha).$$

At this point, we distinguish 2 cases.

1. $d_\alpha < d$ for all α. In this situation, we use the induction hypothesis.

2. There is a unique invariant space $H_\alpha = \mathbb{R}^d$ and

$$a^2 = \lambda(a)\mathbf{1} \text{ for all } a \in V \supset A.$$

In this situation, we will use a variant of the Erdös-Szemerédi argument.

Case 1.

Thus all $d_\alpha < d$. We will use induction.

We may assume

$$A \subset \mathrm{Sym}(d_1) \times \mathrm{Sym}(d_2)$$

and theorem holds for each $\mathrm{Sym}(d_i)$. We need to establish a sum-product theorem for $\mathrm{Sym}(d_1) \times \mathrm{Sym}(d_2)$.

Let π be the projection $\mathrm{Sym}(d_1) \times \mathrm{Sym}(d_2) \to \mathrm{Sym}(d_1)$. For $x \in \pi(A) \subset \mathrm{Sym}(d_1)$, denote the fiber of A at x by

$$A(x) = \{y \in \mathrm{Sym}(d_2) : (x, y) \in A\}.$$

We perform the usual regularization of the graph using the additive doubling constant. Let

$$\begin{aligned} M_1 &= |\pi(A)| \\ M_2 &= \max_{x \in \pi(A)} |A(x)| = |A(\bar{x})| \,. \end{aligned} \tag{5.3}$$

Thus

$$M_1 M_2 \geq N. \tag{5.4}$$

Let

$$K = K_+(A) + K_\times(A).$$

Then

$$\begin{aligned} K \sum_{x \in \pi(A)} |A(x)| &= K|A| \\ &\geq K_+(A)|A| = |A + A| \\ &\geq \sum_{x \in \pi(A)} |A(x) + A(\bar{x})| \\ &\geq |\pi(A)| \; |A(\bar{x})| = M_1 M_2. \end{aligned}$$

Let

$$B = \{x \in \pi(A) : |A(x)| > \frac{M_2}{2K}\}. \tag{5.5}$$

A straightforward averaging argument implies that

$$|B| > \frac{M_1}{2K}\ . \tag{5.6}$$

Induction on $B \subset \mathrm{Sym}(d_1)$ implies that there is $\varepsilon_1 = \varepsilon_1(d_1)$ such that

$$|B+B| + |B \cdot B| > |B|^{1+\varepsilon_1} > \left(\frac{M_1}{2K}\right)^{1+\varepsilon_1}.$$

The last inequality is by (5.6).

Assume

$$|B+B| > \frac{1}{2}\left(\frac{M_1}{2K}\right)^{1+\varepsilon_1}. \tag{5.7}$$

Then by (5.7), (5.5) and (5.4),

$$KN > |A+A| \geq |B+B| \min_{x,x' \in B} |A(x)+A(x')| > \frac{1}{2}\left(\frac{M_1}{2K}\right)^{1+\varepsilon_1} \frac{M_2}{2K} > \frac{N}{K^3} M_1^{\varepsilon_1}. \tag{5.8}$$

Hence

$$K > M_1^{\frac{\varepsilon_1}{4}}. \tag{5.9}$$

Assume

$$|B \cdot B| > \frac{1}{2}\left(\frac{M_1}{2K}\right)^{1+\varepsilon_1}.$$

Similarly,

$$KN > |A \cdot A| \geq |B \cdot B| \min_{x,x' \in B} |A(x) \cdot A(x')| > \frac{1}{2}\left(\frac{M_1}{2K}\right)^{1+\varepsilon_1} \frac{M_2}{2K} > \frac{N}{K^3} M_1^{\varepsilon_1}.$$

This is because of the following

Claim. *For any $y \in A(x)$, $|\, y \cdot A(x')| = |A(x')| > \frac{M_2}{2K}$.*

Proof. This follows from the fact that the map

$$A(x') \to yA(x') : z \mapsto yz \text{ is one-to-one.}$$

Indeed, if $z_1 \neq z_2$ in $A(x')$, then $(x', z_1) \neq (x', z_2)$ are distinct elements of A satisfying Proposition 3.1. Thus

$$(x, y) \cdot (x', z_1) \neq (x, y) \cdot (x', z_2) \Rightarrow y.z_1 \neq y.z_2. \quad \square$$

Hence, in either case (5.9) holds.

Let $\varepsilon_2 = \varepsilon_2(d_2)$ be provided by the induction hypothesis for $\{\bar{x}\} \times A(\bar{x}) \subset \mathrm{Sym}(d_2)$. If $M_1^{\frac{\varepsilon_1}{4}} \geq N^{\frac{\varepsilon_1\varepsilon_2}{9}}$, then (5.9) implies the theorem. So we assume

$$M_1^{\frac{\varepsilon_1}{4}} < N^{\frac{\varepsilon_1\varepsilon_2}{9}}. \tag{5.10}$$

Note that (5.10) is equivalent to

$$N^{\varepsilon_2} M_1^{-2} > N^{\frac{\varepsilon_2}{9}}. \tag{5.11}$$

The sum-product theorem for $\{\bar{x}\} \times A(\bar{x})$ gives

$$KN > |A + A| + |A.A| \geq |A(\bar{x}) + A(\bar{x})| + |A(\bar{x}) \cdot A(\bar{x})| > M_2^{1+\varepsilon_2} > \left(\frac{N}{M_1}\right)^{1+\varepsilon_2}.$$

The last inequality is by (5.4). Hence

$$K > N^{\varepsilon_2} M_1^{-1-\varepsilon_2} > N^{\varepsilon_2} M_1^{-2}. \tag{5.12}$$

Combining (5.11) and (5.12), we obtain

$$K > N^{\frac{\varepsilon_2}{9}} > N^{\frac{\varepsilon_1\varepsilon_2}{9}}.$$

Therefore, we may take

$$\varepsilon = \frac{\varepsilon_{d_1}\varepsilon_{d_2}}{9} \tag{5.13}$$

and claim

$$|A + A| + |A \cdot A| > |A|^{1+\varepsilon} \tag{5.14}$$

for $A \subset \mathrm{Sym}(d_1) \times \mathrm{Sym}(d_2)$.

This concludes Case 1.

Case 2. $d_\alpha = d$.

Thus $A \subset V \subset \mathrm{Sym}(d)$ and

$$a^2 = \lambda(a)\mathbf{1}, \text{ for all } a \in V = v_0 + V_0, \tag{5.15}$$

where V_0 is a linear space.

Claim. *$a^2 = \lambda(a)\mathbf{1}$, for all $a \in \langle v_0, V_0\rangle$.*

Proof. Let $w \in V_0, t \in \mathbb{R}$. Then $v_0 + tw \in V$, hence

$$v_0^2 + t(v_0 w + w v_0) + t^2 w^2 \in \mathbb{R}\mathbf{1} \text{ for all } t.$$

Therefore, for all $w \in V_0$

$$w^2, v_0 w + w v_0 \in \mathbb{R}\mathbf{1} \quad \square$$

Therefore, we may assume $A \subset V$, a linear space and $a^2 = \lambda(a)\mathbf{1}$, for all $a \in V$. For a matrix $a = (a_{i,j})$, let

$$|\, a \,| = \big(\sum_{i,j=1}^{d} a_{ij}^2 \big)^{1/2},$$

the Hilbert-Schmidt norm.

Since $V \subset \mathrm{Sym}(d)$, the Claim above and orthonormal diagonalization for symmetric matrices give the following properties for $a, b \in V$:

$$|\, a| = \sqrt{\lambda(a) d}. \tag{5.16}$$

$$\lambda(ab) = \lambda(a)\lambda(b) \tag{5.17}$$

$$|\, ab \,| = d^{-\frac{1}{2}} |\, a \,|\, |\, b \,| \tag{5.18}$$

The proof is completed by noting that this case follows from

Proposition. (Theorem 3 in [C4]) *Let $\{\mathbb{R}^m, +, *\}$ be an $\mathbb{R}$-algebra with $+$ the componentwise addition. For $a = (a_1, \cdots, a_m)$, let $|a| = \sqrt{(\sum a_i^2)}$ be the Hilbert-Schmidt norm, and let $V \subset \mathbb{R}^m$ such that*

1. $\exists\ c = c(m)$, $\forall a, b \in V$, $|\, a * b| = c|\, a|\, |\, b|$

2. for any $a \in V \setminus \{0\}, a^{-1}$ exists (in a possibly larger field).

Then for any $A \subset V$, $|A + A| + |AA| > |A|^{1+\delta}$.

Remark 5.1 Recall however that the set A here is a subset A' of the original set A, obtained by applying first Proposition 2.1 and making next the rank specification. Cf (i) and (3.2). If N is the size of the original set A, from (i), (3.0), (3.4), the size of A' here satisfies

$$|A'| > \frac{1}{d} K^{-C_d} N > d^{-1-C_d} [K_+(A) + K_\times(A)]^{-C_d} N. \tag{5.19}$$

Hence

$$\begin{aligned}[K_+(A)+K_\times(A)]N &= |A+A|+|A\cdot A| \\ &\geq |A'+A'|+|A'\cdot A'| > |A'|^{1+\varepsilon} \\ &> d^{-(1+C_d)(1+\varepsilon)}[K_+(A)+K_\times(A)]^{-C_d(1+\varepsilon)}N^{1+\varepsilon},\end{aligned}$$

which gives

$$K_+(A)+K_\times(A) > \left(\frac{1}{d}\right)^{1+\varepsilon/(1+C_d(1+\varepsilon))} N^{\varepsilon/(1+C_d(1+\varepsilon))}. \tag{5.20}$$

We may therefore take $\varepsilon_d = \frac{\varepsilon}{1+C_d(1+\varepsilon)}$, with ε obtained by A'.

Remark 5.2. Concerning Case 2, there exists indeed linear space V_j of symmetric matrices a such that $a^2 \in \mathbb{R}\mathbf{1}$ for any $a \in V_j$, and $\dim V_j = j$ for any j.

Take $V_1 = \mathbb{R}$.

Let $d_j = 2^{j-1}$ and assume V_j is a subspace of $\mathrm{Sym}(d_j)$ with the above properties. Let V_{j+1} consist of the $(2^j \times 2^j)$-matrices

$$b = \begin{pmatrix} \lambda_{j+1}\mathbf{1} & \mathbf{a} \\ \mathbf{a} & -\lambda_{j+1}\mathbf{1} \end{pmatrix}$$

where $\lambda_{j+1} \in \mathbb{R}$ and $\mathbf{a} \in V_j$. It is easy to see that $b^2 = (\lambda_1^2 + \cdots + \lambda_{j+1}^2)\mathbf{1}$, and $\dim V_{j+1} = \dim V_j + 1 = j+1$.

Acknowledgement. *The author would like to thank W. Raskind for his hospitality.*

References

[Bi]. Y. Bilu, *Structure of sets with small sumset*, in 'Structure Theory of Set Addition', Astérisque 258 (1999), 77-108.

[BC]. J. Bourgain, M.-C. Chang, *On the size of k-fold sum and product sets of integers*, JAMS Vol. 17, No. 2, (2004), 473-497.

[BKT]. J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, preprint.

[C1]. M.-C. Chang, *Erdös-Szemeredi problem on sum set and product set*, Annals of Math. 157 (2003), 939-957.

[C2]. ———, *Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems*, GAFA Vol. 113, (2002), 399-419.

[C3]. ———, *On sums and products of distinct numbers*, J. of Combinatorial Theory, Series A 105, (2004), 349-354.

[C4]. ———, *A sum-product estimate in algebraic division algebras over* $\mathbb{R}$, Israel J. of Math. (to appear).

[C5]. ———, *A sum-product theorem in semi-simple commutative Banach algebras*, J.Funct Anal, 212, (2004), 399-430..

[E]. G. Elekes, *On the number of sums and products*, Acta Arithmetica 81, Fase 4 (1997), 365-367.

[ER]. G. Elekes, I.Z. Ruzsa, *Product sets are very large if sumsets are very small*, preprint.

[ES]. P. Erdős and E. Szemerédi, *On sums and products of integers*, in Studies in Pure Mathematics, Birkhauser, Basel, 1983, pp. 213-218.

[F]. K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan J. **2** (1998), 59-66.

[N1]. M.B. Nathanson, *The simplest inverse problems in additive number theory*, in Number Theory with an Emphasis on the Markoff Spectrum (A. Pollington and W. Moran, eds.), Marcel Dekker, 1993, pp. 191–206.

[N2]. ———, *On sums and products of integers*, Proc. Amer. Math. Soc. **125** (1997), 9-16.

[N3]. ———, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer (1996).

[NT]. M. Nathanson and G. Tenenbaum, in Structure Theory of Set Addition, Astérisque 258 (1999).

[R]. I.Z. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. 65 (1994), no 4, 379-388.

[S]. J. Solymosi, *On the number of sums and products,*, (preprint) (2003).