Combinatorics/Number Theory

Some consequences of the Polynomial Freiman–Ruzsa Conjecture

Mei-Chu Chang

Department of Mathematics, University of California, Riverside, CA 92521, USA

Received 25 December 2008; accepted after revision 2 April 2009

Presented by Jean Bourgain

Abstract

Assuming the Weak Polynomial Freiman–Ruzsa Conjecture, we derive some consequences on sum-products and the growth of subsets of $\text{SL}_3(\mathbb{C})$. To cite this article: M.-C. Chang, C. R. Acad. Sci. Paris, Ser. I 347 (2009).

Résumé


Version française abrégée

Soit $A$ un sous-ensemble fini d’un espace vectoriel $V$ et notons $A + A = \{x + y : x, y \in A\}$ l’ensemble somme (de même, $nA = (n - 1)A + A$). Un lemme dû à Freiman affirme que si $|A + A| < K|A|$ et $|A| > cK^2$, l’espace $(A)$ engendré par $A$ est de dimension inférieure à $K$.

La conjecture polynomiale faible de Freiman–Ruzsa (WPFRC) est l’énoncé suivant : Si $A$ satisfait $|A + A| < K|A|$, il existe un sous-ensemble $A_1$ de $A$ tel que $|A_1| > K^{-c}|A|$ avec $A_1 \subset \mathbb{Z}\xi_1 + \cdots + \mathbb{Z}\xi_d$, $\xi_i \in V$ et $d < c \log K$ où $c$ est une constante absolue.


Théorème 1. Supposons WPFRC. Étant donné $n \in \mathbb{Z}_+$ et $\varepsilon > 0$, il existe $\delta > 0$ tel que si $A \subset \mathbb{C}^*$ est un ensemble fini et $|AA| < |A|^{1+\delta}$ (en supposant $|A|$ suffisamment grand), on a $|nA| > |A|^{n(1-\varepsilon)}$.

On a également la propriété suivante pour la croissance d’ensembles finis dans un groupe linéaire:

E-mail address: mcc@math.ucr.edu.
Théorème 2. Supposons WPFRC. Si $A \subset SL_3(\mathbb{C})$ satisfait $|AA| < K|A|$ ($|A|$ fini et suffisamment grand), il existe un sous-ensemble $A'$ de $A$ tel que $|A'| > K^{-c}|A|$ avec $A'$ contenu dans une classe d’un sous-groupe nilpotent ($c$ est une constante absolue).

D’autre part nous mentionnons certains résultats plus faibles, qui ne dépendent pas de cette conjecture.

1. Notations

The $n$-fold sum set and the $n$-fold product set of $A$ are $nA = A + \cdots + A = \{a_1 + \cdots + a_n : a_1, \ldots, a_n \in A\}$ and $A^n = A \cdot \cdots \cdot A = \{a_1 \cdots a_n : a_i \in A\}$ respectively. The inverse set $A^{-1}$ can be defined similarly. Let further $A[n] = (\{1\} \cup A \cup A^{-1})^n$. The notation $A^n$ is also used for the $n$-fold Cartesian product, when there is no ambiguity.

2. Freiman’s theorem and related conjectures

One way to formulate the Polynomial Freiman–Ruzsa Conjecture is as follows: Let $V$ be a $\mathbb{Z}$-module and $A \subset V$ a finite set satisfying

\[|A + A| < K|A|.\] (1)

Then there exist a positive integer $d \in \mathbb{Z}_+$, a subset $A_1 \subset A$, a convex subset $B \subset \mathbb{R}^d$ and a group homomorphism $\phi : \mathbb{Z}^d \to V$ such that

\[d < c \log K,\] (2)

\[|A_1| > K^{-c}|A|,\] (3)

\[\phi(B \cap \mathbb{Z}^d) \supset A_1,\] (4)

\[|B \cap \mathbb{Z}^d| < K^{-c}|A|.\] (5)

Here $c$ is an absolute constant.

Recall that if $A$ satisfies (1) and $cK^2 < |A|$, then $A \subset \phi(B \cap \mathbb{Z}^d)$ with $d \leq K$ and $B \subset \mathbb{R}^d$ a box satisfying $|B| < \exp(cK^2 \log^3 K)|A|$. (Quantitative version of Freiman’s theorem from [4].)

More relevant in this note is the much simpler Freiman Lemma, stating that if (1) holds and $|A| > cK^2/\varepsilon$, then $A \subset \phi(\mathbb{Z}^d)$ with $d \leq [K - 1 + \varepsilon]$.

The Polynomial Freiman–Ruzsa Conjecture implies, in particular, the following weaker conjecture, which is all we will use:

Weak Polynomial Freiman–Ruzsa Conjecture (WPFRC): If $A \subset V$ satisfies $|A + A| < K|A|$, then there exist a subset $A_1 \subset A$ with $|A_1| > K^{-c}|A|$, and elements $\xi_1, \ldots, \xi_d \in V$ with $d < c \log K$, so that $A_1 \subset \mathbb{Z}\xi_1 + \cdots + \mathbb{Z}\xi_d$, where $c$ is an absolute constant.

Note that if $A \subset \mathbb{R}_+$ is finite satisfying

\[|AA| < K|A|\] (6)

and considering the set $\log A \subset \mathbb{R} =: V$, one would derive that there are elements $\eta_1, \ldots, \eta_d \in \mathbb{R}^*$ with $d < c \log K$ such that

\[|A \cap G| > K^{-c}|A|,\] (7)

where $G < \mathbb{R}^*$ denotes the multiplicative group generated by $\eta_1, \ldots, \eta_d$.

The analogous statement would hold equally well for a finite subset $A \subset \mathbb{C}^*$ satisfying (6).

3. Sets with small product sets

We recall the deep theorem of Evertse–Schlickewei–Schmidt ([7], Theorem 1.1) on linear equations in multiplicative groups:
Theorem ESS. Let $\Gamma$ be a subgroup of the multiplicative group $(\mathbb{C}^\star)^n$ of rank $r$ and let $a_1, \ldots, a_n \in \mathbb{C}^\star$. Then the equation
\[ a_1x_1 + \cdots + a_nx_n = 1 \quad \text{with} \quad (x_1, \ldots, x_n) \in \Gamma \] (8)
has at most
\[ \exp(6n^3(r + 1)) \] (9)
non-degenerate solutions, meaning that no proper subsum of $a_1x_1 + \cdots + a_nx_n$ vanishes.

The precise bound (9) is very important for our purpose.

Let $G < \mathbb{C}^\star$ be a group generated by $d$ elements $\eta_1, \ldots, \eta_d$ with $d < c \log K$, and let $\Gamma = G^n$. Since $\Gamma$ is generated by the elements $(1, \ldots, \eta_i, \ldots, 1)$, we have $r := \text{rank } \Gamma \leq nd$. Therefore, given $a_1, \ldots, a_n \in \mathbb{C}^\star$, the equation $a_1x_1 + \cdots + a_nx_n = 1$ with $x_1, \ldots, x_n \in G$ has at most
\[ \exp(6n^3(\log K) nd + 3n(r + 1)) < \exp(cn(6n)3n \log K) = KC(n) \] (10)
non-degenerate solutions, where $C(n)$ is a constant depending on $n$.

For $S_1, \ldots, S_n \subset \mathbb{C}$, we denote the additive energy of $S_1, \ldots, S_n$ by
\[ E(S_1, \ldots, S_n) = \left| \left\{ (x_1, y_1, \ldots, x_n, y_n) \in S_1^2 \times \cdots \times S_n^2 : x_1 + \cdots + x_n = y_1 + \cdots + y_n \right\} \right|. \]

Recall the following lower bound on the size of the sum-set $S_1 + \cdots + S_n$:
\[ |S_1 + \cdots + S_n| \geq \frac{|S_1|^2 \cdots |S_n|^2}{E(S_1, \ldots, S_n)}. \]

Corollary 1. Let $G < \mathbb{C}^\star$ be a group generated by $d$ elements with $d < c \log K$ and let $A_1 \subset G$ be finite. Then
\[ E\left( \underbrace{A_1, \ldots, A_1}_n \right) \leq K^{C(n)}|A_1|^{n-1} + \frac{(2n)!}{n!}|A_1|^n, \]
where $C(n)$ is a constant depending on $n$.

Proof. Consider the equation
\[ x_1 + \cdots + x_n - x_{n+1} - \cdots - x_{2n} = 0, \quad x_i \in A_1. \]

We decompose (13) in minimal vanishing subsums. Each decomposition corresponds to a partition
\[ \{1, \ldots, 2n\} = \bigcup_{\alpha = 1}^{\beta} E_\alpha. \]

Since $|E_\alpha| \geq 2$, we have $\beta \leq n$. The case $\beta = n$ clearly contributes to the last term in (12). If $|E_\alpha| \geq 3$, we rewrite the equation
\[ \sum_{i \in E_\alpha} \pm x_i = 0 \] (15)
as
\[ \sum_{i \in E_\alpha \setminus \{r_1\}} \pm \frac{x_i}{x_{r_1}} = 1. \] (16)
(Specify some element $r_1 \in E_\alpha$.) Since no subsum of (15), (16) is assumed to vanish, the estimate (10) in Theorem ESS applies for the number of non-degenerate solutions of
\[ \sum_{i \in E_\alpha \setminus \{r_1\}} \pm \frac{z_i}{z_{r_1}} = 1 \quad \text{with} \quad z_i \in G. \] (17)
Therefore (15) has at most $K^C(|E_u|)|A_1|$ non-degenerate solutions. It follows that the number of solutions of (13) corresponding to the partition (14) is bounded by $|A_1|^{\beta} \prod_{\alpha=1}^\beta K^{C(|E_u|)}$, where $\beta \leq n - 1$. Summing over all possible partitions, we prove (12). \(\square\)

The next corollary is conditional to the Weak Polynomial Freiman–Ruzsa Conjecture.

**Corollary 2.** Assume WPFRC. Given $n \in \mathbb{Z}_+$ and $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{C}^*$ is finite with $|A|$ large and $|AA| < |A|^{1+\delta}$, then the $n$-fold sumset $nA$ satisfies $|nA| > |A|^{n(1-\varepsilon)}$. \(\text{Proof.}\) Take $K = |A|^{\delta}$ in (6). WPFRC, Corollary 1 (letting $A_1 = A \cap G$ in (7)), and (11) imply

\[
|nA| \geq |nA_1| \geq \frac{|A_1|^{2n}}{K^{C(n)}|A_1|^{n-1} + \frac{(2n)!}{n!}|A_1|^n} > \min\left(\frac{n!}{(2n)!}|A_1|^n, K^{-C(n)}|A_1|^{n+1}\right)
\]

\[
> \min\left(\frac{n!}{(2n)!} K^{-c_1n}|A_1|^n, K^{-C(n)}|A_1|^{n+1}\right).
\]

Note that one has the following stronger conclusion:

**Corollary 3.** Assume WPFRC. Given $n \in \mathbb{Z}_+$ and $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{C}^*$ is a sufficiently large finite set satisfying (18) and $B \subset A$ is any subset such that $|B| > |A|^{\varepsilon}$, then $|nB| > |B|^{n(1-\varepsilon)}$.

**Proof.** As in the proof of Corollary 2, we start from $A_1 = A \cap G$ satisfying (7). Let $z_1, \ldots, z_s$ be a maximal subset of $A$ such that $z_iA_1 \cap z_jA_1 = \emptyset$ for any $i \neq j$. Hence

\[
s \leq \frac{|AA_1|}{|A_1|} \leq K^c \frac{|AA|}{|A|} < K^{c+1}
\]

and by construction, if $z \in A$, then $zA_1 \cap zA_1 \neq \emptyset$ for some $1 \leq i \leq s$. Therefore, $A \subset \bigcup_{i=1}^s z_iA_1A_1^{-1}$ and $B \subset \bigcup_{i=1}^s (B \cap z_iA_1A_1^{-1})$.

Hence there is $1 \leq i \leq s$ such that $|B_i := B \cap z_iA_1A_1^{-1}| \geq |B|/s$.

Note that since $A_1A_1^{-1} \subset G$, Corollary 1 remains valid for $z_i^{-1}B_1 \subset A_1A_1^{-1}$. In (19) $A, A_1$ are replaced by $B, B_1$. (Note also that $|z_i^{-1}B_1| = |B_1|$, etc.) \(\square\)

There are various weaker forms of Corollary 2 and Corollary 3 that hold unconditionally. The following is a version of Corollary 2:

**Proposition 4.** Given $m > 1$, there is $\delta > 0$ and $n \in \mathbb{Z}_+$ such that if $A \subset \mathbb{C}^*$ is a sufficiently large finite set satisfying $|AA| < |A|^{1+\delta}$, then $|nA| > |A|^m$.

Using the terminology in [9], a set $A$ satisfying (21) is called an approximate multiplicative group. It was shown in [1] (see also [9], Theorem 2.60) that given $H \neq \emptyset$ in $\mathbb{F}_p$ with $|HH| \leq K|H|$, and $m > 1, \varepsilon > 0$, there is an integer $n = n(m, \varepsilon) \in \mathbb{Z}_+$ such that $|nH| > c(m, \varepsilon)K^{-C(m, \varepsilon)} \min(|H|^m, p^{1-\varepsilon})$.

For $A \subset \mathbb{C}^*$, the same argument allows to show that $|nA| > c(m, \varepsilon)K^{-C(m, \varepsilon)}|A|^m$ and hence the proposition holds.

Regarding Corollary 3, there is the result from [2] for finite subsets $A \subset \mathbb{Z}$ and generalized in [3] for sets $A$ of algebraic numbers of bounded degree.
**Proposition 5.** Given \( d, n \in \mathbb{Z}_+ \) and \( \varepsilon > 0 \), there is \( \delta > 0 \) such that the following holds: Let \( A \subset \mathbb{C}^* \) be a sufficiently large finite set of algebraic numbers of degree at most \( d \). Assume \( |AA| < |A|^{1+\delta} \). Then, for any nonempty subset \( B \subset A, |nB| > |A|^{-\varepsilon} |B|^n \).

Note that in this proposition we do not require all elements of \( A \) to be contained in the same extension of \( \mathbb{Q} \) of bounded degree. This bounded degree hypothesis is removed because of WPFRC.

4. Finite subsets of linear groups

We recall the following theorem from [5,6]:

For all \( \varepsilon > 0 \), there is \( \delta > 0 \) such that if \( A \subset SL_3(\mathbb{Z}) \) is a finite set, then one of the following alternatives holds:

(i) \( A \) intersects a coset of a nilpotent subgroup in a set of size at least \( |A|^{1-\varepsilon} \).

(ii) \( |A^2| > |A|^{1+\delta} \).

The proof makes essential use of Theorem ESS, applied with \( \Gamma \) the unit group of the extension of a cubic polynomial over \( \mathbb{Q} \). This is the only significant place where a generalization to subset \( A \subset SL_3(\mathbb{C}) \) is problematic. Here we will discuss in some greater detail how the WPFRC allows us to recover the theorem in its full strength for subsets \( A \subset SL_3(\mathbb{C}) \).

**Theorem 6.** Assume WPFRC. Given a finite subset \( A \subset SL_3(\mathbb{C}) \) satisfying

\[
|AA| < K |A|, \tag{22}
\]

then there is a subset \( A' \subset A \) such that

\[
|A'| > K^{-c} |A| \tag{23}
\]

and \( A' \) is contained in a coset of a nilpotent group.

**Proof.** An initial key step in [5] (borrowed from Helfgott’s work [8]) is to construct a set \( D \subset A^{-1}A \) of commuting elements, where

\[
|D| > K^{-C} |A|^\theta \tag{24}
\]

with \( C, \theta \) absolute constants. This step is completely general and applies equally well to subsets \( A \subset SL_d(\mathbb{C}) \) with \( \theta = \theta(d) \). Change of bases permits simultaneous diagonalization of the elements of \( D \). They form the key ingredient in the amplification.

Going back to (22), one applies first Tao’s non-commutative version of the Balog–Szemerédi–Gowers Lemma (see [9]) and replaces \( A \) by a subset \( A_1 \subset A \) satisfying that

\[
|A_1| > K^{-c} |A| \tag{25}
\]

and \( A_1 \) is an approximate group, i.e. there is a subset \( X \subset SL_3(\mathbb{C}) \) such that

\[
|X| < K^c \quad \text{and} \quad A_1A_1 \subset XA_1 \cap A_1X, \tag{26}
\]

where \( c \) is an absolute constant.

Identifying \( A \) and \( A_1 \) and using (26), one can control the size of all product sets

\[
|A^{[k]}| < K^{c^3} |A| \tag{27}
\]

for given \( s \in \mathbb{Z}_+ \).

Let \( D \subset A^{-1}A \subset A^{[2]} \) be the diagonal set obtained above, satisfying (24). The next aim is to ensure that \( D \) has small multiplicative doubling.

Denote the set of diagonal matrices over \( \mathbb{C} \) by \( D \) and let \( D_s = D \cap A^{[s]} \) for \( s \geq 2 \). Hence \( D_s \supset D_2 \supset D \) satisfies (24). Consider a minimal subset \( B \subset A^{[2]} \) satisfying

\[
A^{[2]} \subset BD. \tag{28}
\]
It follows that
\[ gD \cap g'D = \emptyset, \quad \forall g \neq g' \in B \] (29)
and also
\[ A^{[2]} \subset BD_4. \]

Therefore, \( |A| \leq |A^{[2]}| \leq |B||D_4|. \) Also, \( D_4D_4 \subset D_8 \) and by (29) and (27)
\[ |D_8||B| = |D_8B| \leq |A^{[10]}| < K^{10c}|A|. \] (30)

Consequently
\[ |D_4D_4| \leq |D_8| \leq K^{10c} \frac{|A|}{|B|} \leq K^{10c}|D_4|. \] (31)

Replacing \( D \) by \( D_4 \), we obtain a subset of diagonal matrices in \( A^{[4]} \) satisfying (24) and
\[ |DD| < K^c|D|. \] (32)

This proves Theorem 6. \( \square \)

**Lemma 7.** Let \( A \subset A' \times R \) be finite and let \( \pi : A \to A' \) be the projection to the first coordinate. Assume \( |2A| = |A + A| < K|A| \). Then there exist \( C \subset A \) such that \( |C| > \frac{1}{\sqrt{\log K}} |A| \) and for every \( x \in C \), \( |\pi^{-1}(\pi(x))| \sim h \) for some \( h \).

**Remarks.**
1. We expect that generalization of the theorem to subsets \( A \subset SL_d(\mathbb{Z}) \), with \( d \) arbitrary, is only a technical matter.
2. It may be possible to reach the conclusion of Theorem 6 unconditionally by following the approach in [8].
3. Statements of this type have been suggested by B. Green.

**References**