SOME PROBLEMS RELATED TO SUM-PRODUCT THEOREMS

Mei-Chu Chang

The study of sum-product phenomena and product phenomena is an emerging research direction in combinatorial number theory that has already produced several striking results. Many related problems are not yet fully understood, or are far from being resolved. In what follows we propose several questions where progress can be expected and should lead to advances in this general area.

For two finite subsets A and B of a ring, the *sum set* and the *product set* of A, B are

$$A + B := \{a + b : a \in A, b \in B\},$$
$$\text{and} \qquad A \cdot B := \{ab : a \in A, b \in B\}.$$

§1. Product theorems in matrix spaces.

In a recent remarkable result, H. Helfgott [H] proved that if $A \subset SL_2(\mathbb{F}_p)$, $\mathbb{F}_p$ being the prime field with p elements, then either A is contained in a proper subgroup of $SL_2(\mathbb{F}_p)$ or $|A \cdot A \cdot A| > |A|^{1+\varepsilon}$, where $\varepsilon > 0$ is an absolute constant. This result has already caused a number of striking developments - in particular, in the theory of expanders [BG1] and the spectral theory of Hecke operators. (See [GJS] and [BG2].) Underlying this nonabelian 'product theorem' is the 'sum-product theorem' in $\mathbb{F}_p$, stating that if $A \subset \mathbb{F}_p$ and $1 < |A| < p^{1-\varepsilon}$, then $|A+A|+|A\cdot A| > |A|^{1+\delta}$, for some $\delta = \delta(\varepsilon) > 0$. (See [BGK] and [BKT].) Understanding how Helfgott's result generalizes to higher dimensions is a natural question. Thus

Problem 1. *Is there a generalization of Helfgott's theorem to subsets of $SL_3(\mathbb{F}_p)$?*

The proof of Helfgott's theorem is based on an explicit examination of $SL_2(\mathbb{F}_p)$ using product operations on a general subset. A similar procedure in $SL_3(\mathbb{F}_p)$ does not seem to be understood at this point. On the other hand, one could imagine that the validity of Kazhdan's property here may be of relevance. (See [L].) Instead of considering the characteristic p case, one might start with a characteristic 0 case such as $SL_d(\mathbb{C})$ or $SL_d(\mathbb{R})$. The issue is closely related to the theory of 'growth' and 'random walks' in finitely generated subgroups centered around the polynomial versus exponential dichotomy. Here we first recall Tits' Alternative for linear groups G over a field of characteristic 0: Either G contains a free group on two generators or G is virtually solvable (i.e. contains solvable subgroup of finite index). For a solvable group S, if S does not have any nilpotent subgroup of finite index, then S is of exponential growth. On the other hand, nilpotent groups are of polynomial growth. [Gro]

The difference in our problem however is that we are not iterating the product operation but only performing a few of them. In a recent paper, we showed the following

Theorem 1. [C1] *For all $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset SL_3(\mathbb{Z})$ is a finite set, then either $|A \cdot A \cdot A| > |A|^{1+\delta}$ or A intersects a coset of a nilpotent subgroup of $SL_3(\mathbb{Z})$ in a set of size at least $|A|^{1-\varepsilon}$.*

Several examples show that as a general statement the previous one is basically the best possible, up to the dependence of ε and δ.

In $SL_2(\mathbb{Z})$ or more generally, $SL_2(\mathbb{C})$, we have the following stronger statement that may be proved using Helfgott's method.

Theorem 2. [C1] *There is $\delta > 0$ such that if $A \subset SL_2(\mathbb{C})$ is a finite set not contained in a virtually abelian subgroup (that is, a group with an abelian subgroup of finite index) , then $|A \cdot A \cdot A| > c|A|^{1+\delta}$.*

In addition to certain subgroups introduced by Helfgott, the proof of Theorem 1 uses, in an essential way, the finiteness results of Evertse-Schlickewei-Schmidt [ESS] on solutions of linear equations

$$x_1 + x_2 + \cdots + x_r = 1$$

with variables x_i taken in a multiplicative subgroup of $\mathbb{C}$ of bounded rank (derived from quantitative versions of the subspace theorem). The Evertse-Schlickewei-Schmidt result turns out to be a powerful ingredient in our approach - one for which we have yet to find a characteristic-p substitute.

Problem 2. *Find a different proof of Theorem 1 not using the subspace theorem and that hopefully will permit progress on Problem 1.*

In fact, in this respect we may even put forward the following

Problem 3. *Prove the analogue of Theorem 1 for subsets of $SL_3(\mathbb{R})$.*

On the other hand, one can reasonably expect, with the same technique as in [C1] and additional work, to settle

Problem 4. *Generalize Theorem 1 to subsets of $SL_d(\mathbb{Z})$ for d arbitrary.*

Returning to Theorem 2 and observing that the free group F_2 is a subgroup of $SL_2(\mathbb{Z})$ (which in fact has the former as a subgroup of finite index), we obtain the following

Theorem 3. [C1] *There exists $\delta > 0$ such that if $A \subset F_2$ is a finite subset not contained in a cyclic subgroup, then $|A \cdot A \cdot A| > |A|^{1+\delta}$.*

Problem 5.
(i) Find a direct combinatorial proof of Theorem 3 (or a stronger result).
(ii) What may be said about the value of $\delta > 0$?

Related to (ii), we should mention the recent work of A. Razborov [R], who proved that If A is a finite subset of a free group with at least two non-commuting elements then $|A \cdot A \cdot A| \geq \frac{|A|^2}{(\log |A|)^{O(1)}}$.

We conclude this section with the following vaguely formulated question expressing a 'nilpotent subgroup versus product theorem' type dichotomy beyond linear groups.

Problem 6. *To what extent does Theorem 1 generalizes to general groups?*

The obvious groups to explore in this context are the Grigorchuk counterexamples [Gri] to the polynomial versus exponential dichotomy. These groups are not linear and of growth between polynomial and exponential.

§2. Explicit functions on finite fields with 'large range'.

A. Wigderson raised the question of finding *explicit* (algebraic) functions $f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ with the property that whenever $A, B \subset \mathbb{F}_p$ and $|A|, |B| > \sqrt{p}$, we have that $|f(A, B)| > p^{\frac{1}{2}+\varepsilon}$ for some absolute constant $\varepsilon > 0$. A similar problem may be posed replacing the exponent $\frac{1}{2}$ by any $0 < \alpha < 1$. The first such example, $f(x, y) = x(x + y)$, was obtained by Bourgain. The proof relies on a version of the Szemerédi-Trotter theorem in the $\mathbb{F}_p$-plane (proved in [BKT]), itself derived from the sum-product theorem in $\mathbb{F}_p$. It is reasonable to expect that many other 2-variable polynomials have the 'expanding property' described above. The proper question would be

Problem 7. *What may be said about a polynomial $f(x, y) \in \mathbb{F}_p[x, y]$ that does not have the expanding property?*

Results along this line were obtained in characteristic 0, for instance in the work of Elekes and Ruzsa. Problem 7 is closely related to

Problem 8. *Prove a Szemerédi-Trotter type theorem in characteristic p for systems of algebraic curves.*

This problem is largely unresolved. It will require different methods from the characteristic 0 case.

The following expander problem was also posed by Wigderson: It is in a similar vein but now restricted to known structures in the finite field $\mathbb{F}_{2^n}$ in characteristic 2.

For a set S and a field K, we denote the vector space generated by S over K by $\langle S \rangle_K$.

Problem 9. *Let J be some constant. For $1 \leq j \leq J$, find an explicit system of linear maps $\phi_j : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with the property that whenever E is a linear subspace of $\mathbb{F}_{2^n}$ and $\dim_{\mathbb{F}_2} E > \frac{n}{2}$, then*

$$\dim \Big\langle \bigcup_{1 \leq j \leq J} \phi_j(E) \Big\rangle_{\mathbb{F}_2} > \Big(\frac{1}{2} + \varepsilon\Big) n,$$

where $\varepsilon > 0$ is a fixed constant.

There are other variants of this question of a similar flavor. Of relevance to Problem 9 is our result, which we formulate in nontechnical terms:

Theorem 4. [C2] *There is a function $c(K)$, with $c(K) \to \infty$ as $K \to \infty$, such that for any sufficiently large prime p, if θ is not a root of any polynomial in $\mathbb{F}_p[x]$ of degree at most K and coefficients bounded by K (as integers), then*

$$|A + \theta A| > c(K)|A|$$

for any subset $A \subset \mathbb{F}_p$ *for which* $p^{\frac{1}{10}} < |A| < p^{\frac{9}{10}}$.

The proof of Theorem 4 uses Freiman's theorem. We do not know much more about the behavior of $c(K)$, except for an upper bound of the form

$$\log c(K) \lesssim \sqrt{\log K}.$$

In particular one can show that the inequality in Problem 9 does not hold even for simple maps such as $\phi_j(y) = xy$ with $x \in \mathbb{F}_{2^n}$. (See [KL].) Also Theorem 4 should be compared with the recent result of Konyagin and Laba in characteristic 0.

Theorem 5. [KL] *If* $\theta \in \mathbb{R}$ *is transcendental, then*

$$|A + \theta A| > c(\log N)N$$

for any finite subset $A \subset \mathbb{R}$ *with* $|A| = N$.

Here the optimal result is not known and the 'true' expansion factor, $c(N)$, lies somewhere between $\log N$ and $2^{\sqrt{\log N}}$. In [KL] the authors use the more elementary Freiman's lemma instead of Freiman's theorem. We would like to work on the following problem, in the same spirit of the 'polynomial Freiman conjecture' proposed by B. Green and I. Ruzsa.

Denote by V an infinite dimensional vector space (say over a field of characteristic 0). Freiman's lemma states that if $A \subset V$ is a finite set and $|A + A| < K|A|$, then $\dim\langle A\rangle \leq K$. On the other hand, Freiman's theorem also gives a bound on the size of the smallest parallelogram in $\langle A\rangle$ containing A, by a function of K.

One may hope however to find a large subset A' of A for which $\dim\langle A'\rangle$ is much smaller. For instance one may ask

Problem 10. *Can one find a subexponential (perhaps polynomial) function* $f(K)$ *such that if* $|A + A| < K|A|$, *there is* $A' \subset A$ *satisfying* $|A'| > \frac{|A|}{f(K)}$ *and* $\dim\langle A'\rangle < \log f(K)$*?*

Any result of this type would lead to an improvement of Theorem 5.

§3. The Erdős-Szemerédi sum-product problem.

Recall the conjecture due to Erdős-Szemerédi about the size of sum and product sets of finite subsets A of $\mathbb{Z}$ or $\mathbb{R}$.

Conjecture. $|A + A| + |A \cdot A| \gg |A|^{2-\varepsilon}$ *for all* $\varepsilon > 0$

To date, the strongest general result is due to Solymosi [S]

$$|A + A| + |A \cdot A| \gg |A|^{\frac{14}{11}-\varepsilon}$$

Over the recent year, a number of estimates have been obtained by the author ([C3], [C4]), establishing the conjecture under the additional assumption that either $|A + A|$ or $|A \cdot A|$ is small. The methods we used are different from the geometric approach of [S] and borrow especially from the theory of algebraic number fields, such as prime factorization and consequences of the subspace theorem. The present state of affairs suggests that the solution to the Erdős-Szemerédi conjecture, if true, will be deep. We also believe that the methods involved in the problem so far have not been fully exploited. In [BC1], the following was shown

Theorem 6. *There is a function $\delta(\varepsilon) \to 0$, as $\varepsilon \to 0$ such that if $A \subset \mathbb{Z}$ is a finite set satisfying $|A \cdot A| < |A|^{1+\varepsilon}$, then $|A + A| > |A|^{2-\delta}$.*

The corresponding statement for subsets A of $\mathbb{R}$ is not even known. In [C5], a similar conclusion was reached under the stronger assumption $|A \cdot A| < K|A|$ (using the Evertse-Schlickewei-Schmidt theorem mentioned earlier) and in very recent work [BC2], the result in [BC1] was generalized to sets A of algebraic numbers of bounded degree. Perhaps one can eliminate the dependence on the degree. Thus we ask

Problem 11. *Prove Theorem 6 for finite sets of algebraic numbers without dependence on the degree.*

As is clear from this report, despite lots of progress in combinatorial number theory, there is still a wealth of natural problems remaining open in both commutative or non-commutative settings. It is likely that such results would also imply analogous results for subsets of $\mathbb{R}$, using a transference argument in the spirit of [C4] or [ESS].

References

[BC1]. J. Bourgain, M-C. Chang, *On the size of k-fold Sum and Product Sets of Integers*, J. Amer. Math. Soc., 17, No. 2, (2003), 473-497.

[BC2]. ———, *Sum-product theorems in algebraic number fields (in preparation).*

[BG]. J. Bourgain, A. Gamburd, *New results on expanders*, ComptesRendus Acad. Sci. Paris, Ser. I, 342, 2006, 717-721..

[BKT]. J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), no. 1, 27–57.

[C1]. M.-C. Chang, *Product theorems in SL_2 and SL_3*, J. Math. Jussieu (to appear).

[C2]. ———, *On sum-product representations in $\mathbb{Z}_q$*, J. of European Math. Soc. 8, (2006), 435-463.

[C3]. ———, *Erdös-Szemeredi problem on sum set and product set*, Annals of Math. 157 (2003), 939-957.

[C4]. ———, *Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems*, Geom. Funct. Anal. 113, (2002), 399-419.

[C5]. ———, *Sum and product of different sets*, Contributions to Discrete Math. Vol 1, 1 (2006), 57-67.

[ESS]. J.-H. Evertse, H. Schlickewei, W. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math 155, (2002), 807-836.

[GJS]. A. Gamburd, D. Jakobson, P. Sarnak, *Spectra of elements in the group ring of SU(2)*, Journal of the European Mathematical Society, 1, (1999), 51-85.

[Gri]. R.I. Grigorchuk, *On growth in group theory*, Proc. ICM, Kyoto, 1990, Vol. I, 325-338..

[Gro]. M. Gromov, *Groups of polymonial growth and expanding maps*, IHES, 53, (1981), 53-73.

[H]. H. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/\mathbb{Z}_p)$*, Annals of Math (to appear).

[KL]. S. Konyagin, I. Laba, *Distance sets of well-distributed planar sets for polygonal norms*, Israel J. Math (to appear).

[L]. A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progress in Mathematics 125 (Birkhauser, 1994).

[R]. A. Razborov, *A product theorem in free groups (preprint).*

[S]. J. Solymosi, *On the number of sums and products,*, Bulletin London Math. Soc. (4) 37 (2005) 491-494.

Department of Mathematics, University of California, Riverside, CA 92521
E-mail address: mcc@math.ucr.edu