On the additive bases problem in finite fields

Victoria de Quehen
Department of Mathematics and Statistics
McGill University
Montreal, Canada
dequehen@math.mcgill.ca

Hamed Hatami*
School of Computer Science
McGill University
Montreal, Canada
hatami@cs.mcgill.ca

Submitted: Jul 3, 2016; Accepted: Aug 5, 2016; Published: Aug 19, 2016
Mathematics Subject Classifications: 11B13

Abstract

We prove that if G is an Abelian group and $A_1, \dots, A_k \subseteq G$ satisfy $mA_i = G$ (the m-fold sumset), then $A_1 + \cdots + A_k = G$ provided that $k \geqslant c_m \log\log |G|$. This generalizes a result of Alon, Linial, and Meshulam [Additive bases of vector spaces over prime fields. *J. Combin. Theory Ser. A*, 57(2):203–210, 1991] regarding so-called additive bases.

1 Introduction

Let p be a fixed prime, and let $\mathbb{Z}_p^n$ denote the n-dimensional vector space over the field $\mathbb{Z}_p$. Given a multiset B with elements from $\mathbb{Z}_p^n$, let $\mathcal{S}(B) = \left\{ \sum_{b \in S} b \;\middle|\; S \subseteq B \right\}$. The set B is called an *additive basis* if $\mathcal{S}(B) = \mathbb{Z}_p^n$.

Jaeger, Linial, Payan, and Tarzi [JLPT92] made the following conjecture and showed that if true, it would provide a beautiful generalization of many important results regarding nowhere-zero flows. In particular the case $p = 3$ would imply the weak 3-flow conjecture, which has been proven only recently by Thomassen [Tho12].

Conjecture 1. [JLPT92] For every prime p, there exists a constant k_p such that the union (with repetitions) of any k_p bases for $\mathbb{Z}_p^n$ forms an additive basis.

Let us denote by $k_p(n)$ the smallest $k \in \mathbb{N}$ such that the union of any k bases for $\mathbb{Z}_p^n$ forms an additive basis. In [ALM91] two different proofs are given to show that $k_p(n) \leqslant c_p \log n$, where here and throughout the paper the logarithms are in base 2. The first proof is based on exponential sums and yields the bound $k_p(n) \leqslant 1 + (p^2/2) \log 2pn$, and the second proof is based on an algebraic method and yields $k_p(n) \leqslant (p-1)\log n + p - 2$.

*Supported by an NSERC Discovery Grant.

As observed in [ALM91], it is easy to construct examples showing that $k_p(n) \geqslant p$, and, to the best of our knowledge, it is quite possible that $k_p(n) = p$.

Let G be an Abelian group, and for $A, B \subseteq G$, define the sumset $A + B = \{a + b \mid a \in A, b \in B\}$. For $A \subseteq G$ and $m \in \mathbb{N}$, let $mA = A + \cdots + A$ denote the m-fold sumset of A. Note that for a basis B of $\mathbb{Z}_p^n$, we have $(p-1)\mathcal{S}(B) = \mathbb{Z}_p^n$. On the other hand if $B = B_1 \cup \ldots \cup B_k$ is a union with repetitions of k bases for $\mathbb{Z}_p^n$, then $\mathcal{S}(B) = \mathcal{S}(B_1) + \cdots + \mathcal{S}(B_k)$. Hence Theorem 2 below is a generalization of the above mentioned theorem of Alon *et al* [ALM91].

Theorem 2 (Main theorem)**.** *Let G be a finite Abelian group. Suppose $A_1, \ldots, A_{2K} \subseteq G$ satisfy $mA_i = G$ for all $1 \leqslant i \leqslant 2K$ where $K \geqslant m \ln \log(|G|)$. Then $A_1 + \cdots + A_{2K} = G$. Moreover, for $m = 2$, it suffices to have $K \geqslant \log\log(|G|)$.*

We present the proof of Theorem 2 in Section 2. While it is quite possible that Conjecture 1 is true, the following example shows that its generalization, Theorem 2, cannot be improved beyond $\Theta(\log\log|G|)$ even when $m = 2$.

Example 3. Let $n = 2^k$ and for $i = 1, \ldots, k$, let $C_i \subseteq \mathbb{Z}_p^{2^i}$ be the set of vectors in $\mathbb{Z}_p^{2^i} \setminus \{\vec{0}\}$ in which the first half or the second half (but not both) of the coordinates are all 0's. Note that $C_i + C_i = \mathbb{Z}_p^{2^i}$. Define $A_0 = (\mathbb{Z}_p \setminus \{0\})^{2^k}$ and for $i = 1, \ldots, k$, let

$$A_i = \underbrace{C_i \times \cdots \times C_i}_{2^{k-i}} \subseteq \mathbb{Z}_p^n.$$

It follows from $C_i + C_i = \mathbb{Z}_p^{2^i}$ that $A_i + A_i = \mathbb{Z}_p^n$. On the other hand a simple induction shows that for $j \leqslant k$,

$$A_0 + \cdots + A_j = (\mathbb{Z}_p^{2^j} \setminus \{\vec{0}\})^{2^{k-j}} \neq \mathbb{Z}_p^n.$$

Remark 4. Theorem 2 in particular implies that $k_p(n) \leqslant 2(p-1)\ln n + 2(p-1)\ln\log p$, and $k_3(n) \leqslant 2\log n + 2$. Note that for $p > 3$, the algebraic proof of [ALM91] provides a slightly better constant, however unlike the theorem of [ALM91], Theorem 2 can be applied to the case where p is not necessarily a prime.

2 Proof of Theorem 2

The proof is based on the Plünnecke-Ruzsa inequality.

Lemma 5 (Plünnecke-Ruzsa)**.** *If A, B are finite sets in an Abelian group satisfying $|A + B| \leqslant \alpha|B|$, then*

$$|kA| \leqslant \alpha^k |B|,$$

provided that $k > 1$.

Next we present the proof of Theorem 2. For $2 \leqslant i \leqslant K$, substituting $k = m$, $A = A_i$ and $B = A_1 + \cdots + A_{i-1}$ in Lemma 5, we obtain

$$|G| = |mA_i| \leqslant \left(\frac{|A_1 + \cdots + A_{i-1} + A_i|}{|A_1 + \cdots + A_{i-1}|} \right)^m |A_1 + \cdots + A_{i-1}|,$$

which simplifies to

$$|G|^{1/m} |A_1 + \cdots + A_{i-1}|^{\frac{m-1}{m}} \leqslant |A_1 + \cdots + A_{i-1} + A_i|.$$

Consequently,

$$|G|^{1-\lambda} |A_1|^{\lambda} \leqslant |A_1 + \cdots + A_K|,$$

where $\lambda = \left(\frac{m-1}{m}\right)^K$. Since $K \geqslant m \ln \log |G|$, we have $\lambda = \left(\frac{m-1}{m}\right)^K < e^{-K/m} \leqslant 1/\log |G|$, and thus $|G|^{\lambda} < 2$ and $|G|/2 < |A_1 + \cdots + A_K|$. Similarly we obtain

$$|G|/2 < |A_{K+1} + \cdots + A_{2K}|.$$

Since $A + B = G$ if $|A|, |B| > |G|/2$, we conclude

$$A_1 + \cdots + A_{2K} = G.$$

Finally note that for $m = 2$, we have $\lambda = 2^{-K}$, and thus to obtain $|G|/2 < |G|^{1-\lambda}|A_1|^{\lambda}$, it suffices to have $K \geqslant \log \log |G|$.

3 Quasi-random Groups

While Example 3 shows that the bound of $\Theta(\log \log |G|)$ is essential in Theorem 2, for certain non-Abelian groups, it is possible to achieve the constant bound similar to what is conjectured in Conjecture 1. A finite group G is called D-quasirandom if all non-trivial unitary representations of G have dimension at least D. The terminology "quasirandom group" was introduced explicitly by Gowers in the fundamental paper [Gow08] where he showed that dense Cayley graphs in quasirandom groups are quasirandom graphs in the sense of Chung, Graham, and Wilson [CGW89]. The group $\mathrm{SL}_2(\mathbb{Z}_p)$ is an example of a highly quasirandom group. The so-called Frobenius lemma says that $\mathrm{SL}_2(\mathbb{Z}_p)$ is $(p-1)/2$-quasirandom. This has to be compared to the cardinality of this group, $|\mathrm{SL}_2(\mathbb{Z}_p)| = p^3 - p$. The basic fact that we will use about quasirandom groups is the following theorem of Gowers (See also [Tao15, Exercise 3.1.1]).

Theorem 6 ([Gow08])**.** *Let G be a D-quasirandom finite group. Then every $A, B, C \subseteq G$ with $|A||B||C| > |G|^3/D$ satisfy $ABC = G$.*

We will also need the noncommutative version of Ruzsa's inequality.

Lemma 7 (Ruzsa inequality [Ruz96])**.** *Let $A, B, C \subseteq G$ be finite subsets of a group G. Then*

$$|AC^{-1}| \leqslant \frac{|AB^{-1}||BC^{-1}|}{|B|}.$$

Proof. The claims follows immediately from fact that by the identity $ac^{-1} = ab^{-1}bc^{-1}$, every element ac^{-1} in AC^{-1} has at least $|B|$ distinct representations of the from xy with $(x, y) \in (AB^{-1}) \times (BC^{-1})$. $\square$

Finally we can state the analogue of Theorem 2 for quasi-random groups.

Theorem 8. *Let G be a $|G|^{\delta}$-quasirandom finite group for some $\delta > 0$. If the sets $A_1, \ldots, A_K \subseteq G$ satisfy $A_iA_i^{-1} = G$ for all $1 \leqslant i \leqslant K$ where $K > \log(3/\delta)$. Then $A_1 \ldots A_{3K} = G$.*

Proof. Obviously $|A_1| \geqslant |G|^{1/2}$. For $2 \leqslant i \leqslant K$, substituting $A = C = A_i^{-1}$ and $B = A_1 \ldots A_{i-1}$ in Lemma 7, we obtain

$$\sqrt{|G||A_1 \ldots A_{i-1}|} \leqslant |A_1 \ldots A_i|,$$

which in turn shows

$$|G|^{1-2^{-K}} \leqslant |A_1 \ldots A_K|.$$

Since $K > \log(3/\delta)$, we have

$$|G||G|^{-\delta/3} < |A_1 \ \ldots A_K|.$$

We obtain a similar bound for $|A_{K+1} \ldots A_{2K}|$ and $|A_{2K+1} \ldots A_{3K}|$, and the result follows from Theorem 6. $\square$

Remark 9. Note that in particular for $G = \mathrm{SL}_2(\mathbb{Z}_p)$, if $p \geqslant 7$, and $A_1, \ldots, A_{12} \subseteq G$ satisfy $A_iA_i^{-1} = G$, then $A_1 \ldots A_{12} = G$.

Acknowledgements.

We would like to thank Kaave Hosseini, Nati Linial, and Shachar Lovett for valuable discussions about this problem.

References

[ALM91] N. Alon, N. Linial, and R. Meshulam. Additive bases of vector spaces over prime fields. *J. Combin. Theory Ser. A*, 57(2):203–210, 1991.

[CGW89] F. Chung, R. L. Graham, and R. M. Wilson. Quasi-random graphs. *Combinatorica*, 9(4):345–362, 1989.

[Gow08] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.

[JLPT92] F. Jaeger, N. Linial, C. Payan, and M. Tarsi. Group connectivity of graphs—a nonhomogeneous analogue of nowhere-zero flow properties. *J. Combin. Theory Ser. B*, 56(2):165–182, 1992.

[Ruz96] I. Z. Ruzsa. Sums of finite sets. In *Number theory (New York, 1991–1995)*, pages 281–293. Springer, New York, 1996.

[Tao15] T. Tao. *Expansion in finite simple groups of Lie type*, volume 164 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2015.

[Tho12] C. Thomassen. The weak 3-flow conjecture and the weak circular flow conjecture. *J. Combin. Theory Ser. B*, 102(2):521–529, 2012.