Set systems with distinct sumsets

Javier Cilleruelo [a] Oriol Serra [b,1,3] Maximilian Wötzel [b,2,4]

[a] *Department of Mathematics, Universidad Autónoma de Madrid, 28049 Madrid, Spain*

[b] *Department of Mathematics, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain*

Abstract

A family $\mathcal{A}$ of k-subsets of $\{1, 2, \ldots, N\}$ is a Sidon system if the sumsets $A + A'$, $A, A' \in \mathcal{A}$ are pairwise distinct. We show that the largest cardinality $F_k(N)$ of a Sidon system of k-subsets of $[N]$ satisfies $F_k(N) \leq \binom{N-1}{k-1} + N - k$ and the asymptotic lower bound $F_k(N) = \Omega_k(N^{k-1})$. More precise bounds on $F_k(N)$ are obtained for $k \leq 3$. We also obtain the threshold probability for a random system to be Sidon for $k = 2$ and 3.

Keywords: Sidon sets, distinct sumsets, additive combinatorics

[1] Supported by the Spanish Ministerio de Economía y Competitividad projects MTM2014-54745-P and MDM-2014-0445.

[2] Supported by the Spanish Ministerio de Economía y Competitividad projects MTM2014-54745-P, MTM2017-82166-P and an FPI grant under the María de Maetzu research grant MDM-2014-0445.

[3] Email: oriol.serra@upc.edu

[4] Email: maximilian.wotzel@upc.edu

1 Introduction and Results

The study of Sidon sets of maximum cardinality is a classic topic in additive number theory; see e.g. the survey by O'Bryant [10]. A set A of integers is a Sidon set if the twofold sums of elements in A are pairwise distinct. The notion can be extended in a natural way to set systems.

Definition 1.1 Let $\mathcal{A} = \{A_i : i \in I,\, A_i \subseteq \mathbb{Z}\}$ be a family of subsets of the integers. We say that $\mathcal{A}$ is a *Sidon system* if

$$A_i + A_j = A_{i'} + A_{j'} \implies \{i, j\} = \{i', j'\}.$$

The analogous in this setting is to estimate the maximum cardinality of a Sidon system. We restrict ourselves to uniform set systems of k-subsets of the integer interval $[N] = \{1, 2, \ldots, N\}$.

Definition 1.2 Given integers $N > k \geq 1$, we denote by $F_k(N)$ the largest cardinality of a Sidon system $\mathcal{A} \subseteq \binom{[N]}{k}$.

The case $k = 1$ corresponds to classical Sidon sets and it is well-known that $F_1(N) \sim N^{1/2}$. We address here the problem for $k \geq 2$. First we give an upper bound for $F_k(N)$.

Theorem 1.3 *For $2 \leq k < N$ we have*

$$F_k(N) \leq \binom{N-1}{k-1} + N - k.$$

This upper bound is tight for $k = 2$, that is, $F_2(N) = 2N - 3$. We believe that it is asymptotically sharp for any $k \geq 2$, but we are only able to prove this for $k = 2$ and $k = 3$. For $k \geq 4$, we prove that N^{k-1} is the right order of magnitude.

Theorem 1.4

$$\begin{aligned} F_2(N) &= 2N - 3 \\ F_3(N) &\geq N^2/2 - O(N) \\ F_k(N) &= \Omega_k(N^{k-1}),\ k \geq 4. \end{aligned}$$

We also consider the problem of determining the size of a *typical* Sidon system. We consider the following model for random uniform families of subsets of $[N]$.

Definition 1.5 Let $N > k$ be positive integers and $0 < p \leq 1$. A random set system $\mathcal{A}$ in $\binom{[N]}{k}$ is obtained by choosing independently every set $A \in \binom{[N]}{k}$ with probability p. We write $\mathcal{A} \in \mathcal{S}(N, k, p)$ to denote that $\mathcal{A}$ is a random system in this model.

For $k = 1$ the above definition corresponds to the binomial model of random subsets. Godbole, Janson, Locantore and Rapoport [7] showed, among more general results, that $N^{-1/4}$ is the threshold probability for a random set in $[N]$ to be a Sidon set. In the case of random systems we obtain the threshold probability for $k = 2$ and 3.

Theorem 1.6 *Let $\mathcal{A} \in \mathcal{S}(N, k, p)$ be a random system. Then, for $2 \leq k \leq 3$,*

$$\lim_{N\to\infty} \Pr(\mathcal{A} \textit{ is Sidon}) = \begin{cases} 1, & \textit{if } p = o(N^{-(2k+1)/4}) \\ 0, & \textit{if } p = \omega(N^{-(2k+1)/4}) \end{cases}.$$

The full version of this paper is available at [4].

2 Related Work

The extension of additive problems in the integers or in additive groups to the monoid of sumsets has also been considered in the literature. For instance, Cilleruelo, Hamidoune and Serra [3] proved analogues of the Cauchy–Davenport and Vosper theorems in this setting. An important question related to the current work is whether a certain set can be expressed as a sumset in multiple ways. Alon [1] used probabilistic arguments combined with spectral techniques to improve earlier bounds by Green [9] on the maximal cardinality of subsets of a cyclic group of prime order that cannot be expressed as a sumset. Fan and Tringali [5] used tools from factorization theory to give (among other results) necessary and sufficient conditions for when certain subsets of integers can be written as sumsets in more than one way. Selfridge and Straus [11] showed that the representation function $r_A(n) = |\{(a, a') \in A \times A : n = a + a'\}|$ of a subset A in a field of characteristic zero determines the set. They also considered the general case of s-fold sumsets sA and gave necessary conditions when the representation function of this sumset completely determines the set A. These results were later generalized by Gordon, Fraenkel and Straus [8] to torsion free abelian groups. For a more detailed look on these problems, see also the recent survey by Fomin [6]. In contrast to these results, in the asymmetric case, the representation function does not determine the pair of original sets, even in the case of twofold

sumsets $A + B$.

3 Proof Ideas

We start off by giving a needed definition. For integers $N > k$, let $\binom{[N]}{k}_0$ denote the family of k-subsets of $\{0, 1, \ldots, N\}$ that all contain 0.

The key idea for the proof of Theorem 1.3 is to consider for each A in $\binom{[N-1]}{k}_0$ the set of positive integers x such that $x + A$ is an element of the Sidon system, and to note that the set of positive differences of those sets will be pairwise disjoint due to the Sidon property.

For Theorem 1.4, we use different approaches for the cases $k = 2$, $k = 3$, and $k \geq 4$. In the first case, we just give an explicit family where verification of the Sidon property is easy. For $k = 3$, we make use of the *alteration method*, that is, we start by taking the family $\binom{[N-1]}{3}_0$, which will not be a Sidon system, and then employ a case analysis to show that one can remove $O(N)$ sets in order to make it Sidon. Finally, for $k \geq 4$, we use a sufficiently dense Sidon set to define disjoint intervals such that the sumsets of these intervals will also be disjoint. One then considers the family $\mathcal{A}$ of sets that contain exactly one element from each interval.

In order to prove Theorem 1.6, we follow the approach of Godbole et al. [7] and look at the set of quadruples violating the Sidon property. One can then partition these further depending on how many distinct sets they contain, such that the probability for any quadruple in the same block to be contained in the random family is uniform. The remaining aspect is then to estimate the cardinality of these blocks, which in our case is more complicated than in [7]. The 1-statement is then obtained by an easy application of Markov's inequality, while for the 0-statement the Janson inequality (see e.g. Theorem 8.1.1 in [2]) is used.

4 Concluding Remarks

The most begging question left open by the current work is whether Theorem 1.4 is asymptotically sharp for $k \geq 4$. Since for $k \geq 3$, translations cannot generate a significant number of new sets, this is essentially equivalent to saying that one can remove $o(N^{k-1})$ sets from $\binom{[N-1]}{k}_0$ such that the resulting family is a Sidon system. If we consider the family $\binom{[N-1]}{k}_0 + \binom{[N-1]}{k}_0$, then a randomly chosen element S will asymptotically almost surely have cardinality k^2, so it is reasonable to assume that sumsets of this cardinality are the most

important case to consider. However, while sumsets of this type have only one representation in the case $k = 3$, this will in general not be true anymore for larger values of k. To see this, consider for instance the case $k = 4$, and let a, b, c, d be integers such that

$$S = \{0, a\} + \{0, b\} + \{0, c\} + \{0, d\} \quad \text{and} \quad |S| = 16.$$

Then, in general, we have three different representations for S as a sumset of two 4-sets, namely by pairing $\{0, a\}$ with one of the remaining three 2-sets, and pairing the other two. Similar constructions can be done for any k that is composite. Numerical experiments for moderate values of N and k ($N = 100$ for $k = 4$, $N = 60$ for $k = 5$) suggest that these might be the only instances of sumsets of cardinality k^2 that violate the Sidon property. However, note that this does in general not refute the statement in the beginning of this section, since k-sets constructed in such a way will always obey some linear equations. In the case $k = 4$ for example, the largest element of a 4-set always has to be the sum of the other two nonzero elements, and hence there are only $N^2 = o(N^3)$ such sets, and one can remove them from $\binom{[N-1]}{4}_0$ without affecting the asymptotic density.

Another immediate open question is that of generalizing Theorem 1.6 to arbitrary $k \geq 2$. The main obstruction is that we currently rely on a case analysis to bound one particular type of partition block, which becomes intractable for larger k. Note that this is mainly related to the 1-statement. In fact, a generalization of the 0-statement is true not only for the case of twofold sumsets, but more generally for h-fold sumsets.

It is also possible to further generalize the definition of a Sidon system, in the same way that Sidon sets can be generalized to so called $B_h[g]$ sets. For a family $\mathcal{A}$ of integer subsets, a set of integers C, and an integer $h \geq 2$, let $r_{h\mathcal{A}}(C)$ denote the number of different multisets $\{A_1, A_2, \ldots, A_h\}$, $A_i \in \mathcal{A}$ such that $A_1 + A_2 + \cdots + A_h = C$. A $B_h[g]$ *system* is a family $\mathcal{A}$ of integer subsets such that $r_{h\mathcal{A}}(C) \leq g$ for all sets $C \subseteq \mathbb{Z}$. So a Sidon system is a $B_2[1]$ system. One can now define $F_{k,g,h}(N)$ as the largest cardinality of a $B_h[g]$ system $\mathcal{A} \subseteq \binom{[N]}{k}$. We consider $h = 2$, and write $F_{k,g,2}(N) = F_{k,g}(N)$. As proved in Theorems 1.3 and 1.4, for $k \geq 2$ we have $F_{k,1}(N) = \Theta_k(N^{k-1})$. Interestingly, we can show that for any $g \geq 2$, it actually holds that $F_{k,g}(N) = \Theta_k(\sqrt{g}N^{k-1/2})$. Indeed, since any fixed sumset $A + B$ with $A, B \in \binom{[N]}{k}$ is essentially a translation of a sumset of two sets in $\binom{[N]}{k}_0$, there are at most $O_k(N^{2k-1})$ of them. Now, any one of these has at most g representations in $\mathcal{A} + \mathcal{A}$, which implies the upper bound. On the other hand, take a $B_h[\lfloor g/2 \rfloor]$ set $A \subseteq \{1, 2, \ldots, N/2\}$

of size $|A| = \Omega(\sqrt{gN})$, which is well known to exist, and a Sidon system $\mathcal{I} \subseteq \binom{[N/2]}{k}_0$, of size $|\mathcal{I}| = \Omega_k(N^{k-1})$, which exists by Theorem 1.4. Using the definition of $B_h[g]$ sets and Sidon systems, it is then not hard to see that the set $\mathcal{A} = A + \mathcal{I}$ will be a $B_2[g]$ system, and the lower bound follows. One particularly interesting aspect of this is that while Theorem 1.3 and 1.4 are not consistent with the case $k = 1$, these results in fact are.

Finally, all these problems can also be studied in arbitrary additive groups instead of in the integers.

References

[1] Alon, N., *Large sets in finite fields are sumsets*, J. Number Theory **126** (2007), pp. 110–118.

[2] Alon, N. and J. H. Spencer, "The probabilistic method. With an appendix on the life and work of Paul Erdős. 3rd ed." Hoboken, NJ: John Wiley & Sons, 2008, 3rd ed. edition, xv + 352 pp.

[3] Cilleruelo, J., Y. O. Hamidoune and O. Serra, *Addition theorems in acyclic semigroups*, in: *Additive number theory. Festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson*, New York, NY: Springer, 2010 pp. 99–104.

[4] Cilleruelo, J., O. Serra and M. Wötzel, *Set systems with distinct sumsets* (2018), preprint, arXiv:1802.10511.

[5] Fan, Y. and S. Tringali, *Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics* (2017), preprint, arXiv:1701.09152.

[6] Fomin, D., *Is the Multiset of n Integers Uniquely Determined by the Multiset of Its s-sums?* (2017), preprint, arXiv:1709.06046.

[7] Godbole, A. P., S. Janson, N. W. Locantore Jr. and R. Rapoport, *Random Sidon sequences*, J. Number Theory **75** (1999), pp. 7–22.

[8] Gordon, B., A. S. Fraenkel and E. Straus, *On the determination of sets by the sets of sums of a certain order*, Pac. J. Math. **12** (1962), pp. 187–196.

[9] Green, B., *Counting sets with small sumset, and the clique number of random Cayley graphs*, Combinatorica **25** (2005), pp. 307–326.

[10] O'Bryant, K., *A complete annotated bibliography of work related to Sidon sequences*, Electron. J. Comb. **DS11** (2004), p. 39.

[11] Selfridge, J. and E. Straus, *On the determination of numbers by their sums of a fixed order*, Pac. J. Math. **8** (1958), pp. 847–856.