Additive Combinatorics

Jacob Denson

October 10, 2020

Table Of Contents

Chapter 1

Additive Combinatorics

Additive combinatorics studies the structure of *additive sets*, i.e. subsets of an additive group, often the set of integers. Unlike the methods of number theory, which look at particular number theoretic sets with a strong amount of structure (e.g. the set of primes, the set of squares) we look at more general sets with less structure.

1.1 The Inverse Set Problem

A fundamental problem in additive combinatorics is the *inverse set problem*. If A and B are additive sets in a common G such that $A+B$ and $A-B$ are small, what can one say about A and B? Let A and B be subsets of an additive group G. Then

$$\max(|A|,|B|) \leqslant |A+B| \leqslant |A||B|$$

and

$$|A| \leqslant |A+A| \leqslant \frac{|A|(|A|+1)}{2}.$$

More generally,

$$|A| \leqslant |A^{\oplus n}| \leqslant \binom{|A|+n-1}{n}.$$

where $A^{\oplus n}$ denotes the n-fold sumset. This bound follows from a simple stars and bars argument.

For a generic sparse set A, the quantity $|A+B|$ is much more likely to be close to the upper bound given above than the lower bound. Thus we view a pair of sets whose sum is small as having more additive structure.

Example. *Let A and B to be sets of size N and M choosen uniformly at random from the interval $[0,1]$, then $|A+B| = |A||B|$ with probability one. If we let $A = \{X_1, \ldots, X_N\}$ and $B = \{Y_1, \ldots, Y_M\}$, then the variables are independant and uniformly distributed on $[0,1]$, and for any two values x_1, x_2,*

$$\mathbf{P}(x_1 + Y_{j_1} = x_2 + Y_{j_2}) = 0.$$

Thus for any distinct pairs (i_1, j_1) and (i_2, j_2), $\mathbf{P}(X_{i_1} + Y_{j_1} = X_{i_2} + Y_{j_2}) = 0$. Taking a union bound shows that with probability one, the elements $\{X_i + Y_j\}$ are distinct, and so $|A+B| = NM$.

Example. *Let A and B be subsets of $\mathbf{Z}/N\mathbf{Z}$ with each element in A and B uniformly chosen with probability K/N. Then for each $n \in \mathbf{Z}/N\mathbf{Z}$,*

$$\begin{aligned}\mathbf{P}(n \in A+B) &= \sum_{i=0}^{N-1} \mathbf{P}(i \in A)\,\mathbf{P}(n-i \in B) \\ &\quad - \sum_{i \neq j} \mathbf{P}(i \in A)\,\mathbf{P}(n-i \in B)\,\mathbf{P}(j \in A)\,\mathbf{P}(n-j \in B) \\ &\geqslant K^2/N - K^4/N^2.\end{aligned}$$

Thus $\mathbf{E}(|A+B|) \geqslant K^2 - K^4/N$, whereas $\mathbf{E}(|A|) = \mathbf{E}(|B|) = K$.

If $|A+B| = |A|$, then A and B have maximal additive structure in relation to one another, and in this case we have a strong characterization of the two sets.

Theorem 1.1. *Suppose A and B are finite additive sets. Then the following are equivalent:*

- $|A+B| = |A|$.
- $|A-B| = |A|$.
- $|A + B^{\oplus n} - B^{\oplus m}| = |A|$ *for some* $(n,m) \neq 0$.
- $|A + B^{\oplus n} - B^{\oplus m}| = |A|$ *for all* n, m.
- *There exists a finite subgroup H of G such that A is a union of cosets in G/H, and B is contained in a single coset of G/H.*

Proof. Let us show the first point implies the fifth. Suppose $|A+B| = |A|$. Without loss of generality, by translation assume B contains zero. It follows therefore that $A + B = A$. If we let $\mathrm{Aut}(A) = \{g \in G : A + g = A\}$ then G forms a group containing B. It is simple to see that $\#(\mathrm{Aut}(A)) \leqslant \#(A) < \infty$, so G is a finite group. It is then simple to show that A is a union of cosets in G/H, and since $B \subset H$, B is contained in a single subset. A similar argument shows that the second point implies the fifth, and it is easy to check that the fifth point implies the first and second, so the three properties are all equivalent. To show the fith point implies the fourth point, we may again assume that B contains the origin. Then B is contained in H, so $A + B^{\oplus n} - B^{\oplus m} = A$ for any n and m. The third point immediately implies the third point. Finally, the third point implies either the second or first point since if $n > 0$, then

$$|A| = |A + B^{\oplus n} - B^{\oplus m}| \geqslant |A + B|$$

and if $m > 0$,

$$|A| = |A + B^{\oplus n} - B^{\oplus m} \geqslant |A - B|.$$ □

On the other hand, it is possible to characterize the pairs of sets satisfying $|A + B| = |A||B|$, but it does not give quite as strong a result.

Theorem 1.2. *Suppose A and B are finite additive sets. Then the following are equivalent:*

- $|A + B| = |A||B|$.
- $|A - B| = |A||B|$.
- $|A \cap (x - B)| = 1$ *for all* $x \in A + B$.
- $|A \cap (B + y)| = 1$ *for all* $y \in A - B$.
- $(A - A) \cap (B - B) = \{0\}$.

Proof. TODO □

Remark. It is not always true that $A + B$ has the same cardinality as $A - B$. For instance, if $A = \{0, 1, 3\}$ in $\mathbf{Z}$ then $A + A = \{0, 1, 2, 3, 4, 6\}$ where $A - A = \{-1, 0, 1, 2, 3\}$.

If $|A| + |B| > |G|$, then $A + B = A - B = G$. TODO

1.2 Doubling Constant

Another way to measure the arithmetic structure of sets is via the *doubling constant*

$$\sigma[A] = \frac{|A+A|}{|A|}.$$

If K is small, we have lots of arithmetic structure, whereas if K is large, we have little structure. Similarily we define the *difference constant*

$$\delta[A] = \frac{|A-A|}{|A|}.$$

We have already calculated that that

$$1 \leqslant \sigma[A] \leqslant (|A|+1)/2$$

and it is also easy to see that

$$1 \leqslant \delta[A] \leqslant (|A|-1)/2 + \frac{1}{|A|}$$

which follows from the fact that $|A-A| \leqslant |A|^2 - |A| + 1$. A set which achieve this upper bound (for either the doubling or difference constant, since they are equivalent) is called a *Sidon set*.

Theorem 1.3. *Let A be an additive set. Then any subset of A can have doubling constant at most $\sqrt{\sigma(A)|A|/2}$, and any Sidon set in A has cardinality at most $\sqrt{2\sigma(A)|A|}$.*

Proof. TODO □

The doubling constant behaves poorly under taking unions, except if one of the sets is very small with respect to the other set.

Example. *Find sets A and B each of cardinality N, with $\sigma(A) \leqslant 2$, $\sigma(B) \leqslant 2$, but $\sigma(A \cup B) = N/2$. TODO*

On the other hand, if $\delta(A) = 1$ or equivalently, $\sigma(A) = 1$, then A is a single coset of G/H, where H is a finite subgroup of G. If $A + A = A$, then we actually have $A = H$. An important heuristic is that if $\sigma(A)$ is close to one, then A is 'close' to being a subgroup of G; we think of them as *approximate groups*. On the other hand, we have yet to obtain tools to analyze the structure of sets A with $\sigma(A)$ close to $(|A|+1)/2$, i.e. 'approximately Sidon sets'.

1.3 Ruzsa Distance

For two additive sets A and B we let

$$d(A,B) = \log\left(\frac{|A-B|}{|A|^{1/2}|B|^{1/2}}\right).$$

This is known as the *Ruzsa distance* between the two sets. Indeed, the distance is a non-negative, symmetric function and obeys the triangle inequality

$$d(A,C) \leqslant d(A,B) + d(B,C)$$

which is equivalent to the fact that

$$|A-C| \leqslant \frac{|A-B||B-C|}{|B|}$$

which follows from the identity that $a-c = (a-b)+(b-c)$ for any $b \in B$. The only problem is that we do not have $d(A,A) = 0$ for all sets A. In fact, we know that $d(A,A) = 0$ precisely when A is a coset with respect to some finite subgroup H of G.

The *additive energy* $E(A,B)$ between two sets A and B is the number of solutions to the equation $a_1 + b_1 = a_2 + b_2$. Then

$$|A||B| \leqslant E(A,B) \leqslant |A||B|\min(|A|,|B|).$$

The lower bound follows because there are always at least this many trivial solutions, and the upper bound follows because given any three values in the equation, the fourth is always uniquely determined.

Lemma 1.4. *Let A and B be additive sets. Then*

$$|A||B| = \sum_{x\in A+B} |A\cap(x-B)| = \sum_{y\in A-B} |A\cap(B+y)|$$

and

$$\begin{aligned} E(A,B) &= \sum_{x\in A+B} |A\cap(x-B)|^2 \\ &= \sum_{y\in A-B} |A\cap(B+y)|^2 \\ &= \sum_{z\in(A-A)\cap(B-B)} |A\cap(z+A)||B\cap(z+B)|. \end{aligned}$$

1.4 Sum Free Sets

Given a subset A of an abelian group, we say A is **sum free** if $A + A$ is disjoint from A.

Theorem 1.5. *If A is an arbitrary finite subset of positive natural numbers, then A contains a sum-free subset of size greater than $|A|/3$.*

Proof. The idea of this proof rests on two observations. If $B \subset [1, N]$, and $p > 2N$, then $B + p\mathbf{Z}$ is sumfree in $\mathbf{Z}_p$ if and only if B is sumfree. Thus we can turn out problem into a problem modulo p. Next, we notice that if f is an automorphism, then a subset B of an abelian group is sumfree if and only if $f(B)$ is sumfree. The presense of many automorphisms of $\mathbf{Z}_p$ (one for each natural number between 1 and $p-1$) enables us to exploit randomness to construct a sumfree subset in A. If $X \subset \mathbf{Z}_p$ is sumfree, and does *not* contain zero, we consider the sets $X, 2X, \ldots, (p-1)X$, which are all sumfree. For every $a \in X$, and nonzero $b \in \mathbf{Z}_p$, there is a unique $c \in \{1, \ldots, p-1\}$ such that $ca = b$. Thus every nonzero $b \in \mathbf{Z}_p$ occurs in $|X|/(p-1)$ of the sets $X, \ldots, (p-1)X$. Thus means if we choose a nonzero $x \in \mathbf{Z}_p$ uniformly at random, then

$$\mathbf{E}|(A + \mathbf{Z}_p) \cap xX| = \sum_{a \in A + \mathbf{Z}_p} \mathbf{P}(a \in xX) = \frac{|A||X|}{p-1}$$

Since xX is sumfree, so too is $(A + \mathbf{Z}_p) \cap xX$, and so lower bounding the expectation gives rise to a large sumfree sert. In $\mathbf{Z}_p$, a good candidate for a sumfree set should be an interval, since an arithmetic progression has a small sumset, and all arithmetic progressions are mapped to an interval by an automorphism. Thus, taking $X = \{k, \ldots, 2k-1\}$, where $4k - 2 < p + k$, we get a squarefree set. Thus taking p congruent to two modulo 3, and setting $3k = p + 1$, we find a sumfree set of size

$$\frac{k}{p-1}|A| = \frac{p+1}{3(p-1)}|A| > |A|/3$$

which completes the proof. □

A fundamental problem in additive combinatorics is the *inverse sumset* problem. If $A + B$ or $A - B$ is small, what can one say about A and B?

More specifically, if $A + A$ is small, what can one say about A? We have $|A| \leqslant |A+A| \leqslant [|A|^2+|A|]/2$, and so we refer to the value $\sigma(A) = |A+A|/|A|$ as the **doubling constant** of the set A. We have $1 \leqslant |A| \leqslant (|A|+1)/2$.

Example. *Geometric progressions have the largest doubling constant possible. If*

$$A = \{1, a, a^2, \ldots, a^{N-1}\}$$

then the sum of any two elements of A is distinct, so $|A + A| = (N^2 + N)/2$, and so $\sigma(A) = (N + 1)/2$.

A set A with $\sigma(A)$ maximal among sets of size N is known as a **Sidon set**. This means that all pairwise sums of any two $a_0, a_1 \in A$ are distinct, modulo the trivial equalities $a_0+a_1 = a_1+a_0$. This is a 'generic' behaviour: If A is a subset of N points chosen uniformly at random frmo $[0, 1]$, then A is Sidon with probability one. It is more interesting to characterize when $\sigma(A)$ is small.

Example. *In the other extreme, the main example of sets with small doubling constant is an arithmetic progression. If $A = b_0 + [0, N - 1]a$, then $A + A = 2b_0 + [0, 2N - 2]a$, which consists of $2N - 1$ points, so $\sigma(A) = 2 - 1/N$.*

Example. *If $A \subset B$, and $|A| = \alpha|B|$, then $|A + A| \leqslant |B + B|$, so*

$$\sigma(A) \leqslant \frac{|B + B|}{K|B|} = \sigma(B)/\alpha$$

Thus if $\sigma(B)$ is small, and A contains a large percentage of B, then $\sigma(A)$ is also small. In the other direction, if $|B| = \beta|A|$, then

$$|B+B| \leqslant |A+A|+|A+(B-A)|+|(B-A)+(B-A)| \leqslant \sigma(A)|A|+(\beta-1)|A|^2+\beta^2|A|^2$$

so

$$\sigma(B) \leqslant \sigma(A)/\beta + (\beta + 1 - 1/\beta)|B|$$

Thus if $\sigma(A)$ is small, and B doesn't contain many more points than A, then $\sigma(B)$ is also small.

Example. *If we consider N and M, and a resultant 'rank 2' arithmetic progression $A = c + [0, N]a + [0, M]b$, then $\sigma(A) \leqslant 4$. These sets can look very different from the original arithmetic progressions we were considering.*

If A and B are additive sets, and we form the graph G

1.5 Graph Theoretic Techniques

Theorem 1.6 (Turán)**.** *Let G be a graph of n vertices. Then G contains an independant set of size at least*

$$\sum_{v \in G} \frac{1}{\deg(v)+1}$$

In particular, if the vertices have degree bounded by d, then there is an independant set of size $|G|(d+1)^{-1}$.

Proof. Let $\pi : V \to \{1, \ldots, n\}$ be a uniformly randomly chosen bijection. Let S be the set of all vertices v in V such that for any neighbour w of v, $\pi(v)$ is larger than $\pi(w)$. Then S is an independant set, and it suffices to show S is large in expectation. We find by the hockey stick identity that

$$\begin{aligned}
\mathbf{P}(v \in S) &= \frac{1}{n!} \sum_{m=1}^{n} \binom{m-1}{\deg(v)} \deg(v)!(n-1-\deg(v))! \\
&= \frac{\deg(v)!(n-1-\deg(v))!}{n!} \binom{n}{\deg(v)+1} \\
&= \frac{1}{\deg(v)+1}
\end{aligned}$$

and so

$$\mathbf{E}|S| = \sum_{v \in G} \mathbf{P}(v \in S) = \sum_{v \in G} \frac{1}{\deg(v)+1}$$

and this gives the required set. □

Given $B \subset A$, we say B is sumfree with respect to A if no element of A is the sum of two distinct elements of B. Given A, we let $\phi(A)$ denote the largest sumfree subset with respect to A. We let $\phi(n)$ be the smallest value of $\phi(A)$ among all sets $A \subset \mathbf{R}$ of size n.

Theorem 1.7 (Choi)**.** *If A is any set of n real numbers, there is a set $B \subset A$ of cardinality $\log n - O(1)$ sumfree with respect to A. Thus $\phi(n) \geqslant \log n - O(1)$.*

Proof. Assume first that A is a subset of positive reals. Order $A = \{a_1 > a_2 > \cdots > a_n > 0\}$. Consider the graph G with vertices A, and edges (a_n, a_m)

if $a_n + a_m \in A$. By Turán's theorem, since $\deg(a_i) \leqslant n - i$, we find an independant set S with

$$|S| \geqslant \sum_{i=1}^{n} \frac{1}{n-i+1} = \sum_{i=1}^{n} \frac{1}{i} = \log n - O(1)$$

In general, any set A of n real numbers either contains $n/2 - O(1)$ positive real numbers or $n/2 - O(1)$ negative real numbers, and the theorem then follows in this case. □

The $n/(d+1)$ bound for graphs of bounded degree d cannot be improved for general graphs G. However, it is surprising that one can improve the bound by a $\log d$ factor, provided that the resultant graph has no three cycles.

Theorem 1.8. *If G has no three cycles with maximal degree d, then G contains an independant set of size $\Omega(n \log d/d)$.*

Proof. Choose a set I uniformly from the set of all independant sets in G. For each $v \in V$, define the random variable

$$X_v = d|I \cap \{v\}| + |N(v) \cap I| = \begin{cases} d & v \in I \\ |N(v) \cap I| & v \notin I \end{cases}$$

Any vertex can be in the neighbourhood of at most d other vertices, so

$$\sum_v X_v = d|I| + \sum_{v \notin I} |N(v) \cap I| \leqslant 2d|I|$$

Taking expectations gives that

$$\mathbf{E}|I| \geqslant \frac{1}{2d} \sum_v \mathbf{E}(X_v)$$

Thus it suffices to show that $\mathbf{E}(X_v)$ is large for each v. TODO: FINISH LATER. □

The Balog-Szemerédi theorem says that if $E(A,B) \geqslant K_0 n^2$ and $|A +_G B| \leqslant K_1 n$, then one can find $A_0 \subset A$ and $B_0 \subset B$ such that $|A_0|, |B_0|$, and $|A_0 + B_0|$ are $\Theta_{K_0,K_1}(n)$. Gower's recently strengthened the theorem to showing the

constants in the bound are polynomial in $1/K_0$ and K_1. We shall find that this result can be converted into a graph problem.

If $E(A,B) \gtrsim |A|^{3/2}|B|^{3/2}$, then there is $A_0 \subset A$ and $B_0 \subset B$ with $|A_0| \sim |A|$, $|B_0| \sim |B|$, and $|A_0 + B_0| \lesssim |A_0|^{1/2}|B_0|^{1/2}$. In particular, if A and B have n elements, and $E(A,B) \gtrsim n^3$, then there is $A_0 \subset A$ and $B_0 \subset B$ with $|A_0|, |B_0| \sim n$, and $|A_0 + B_0| \lesssim n$. Can we generalize this theorem to more general operations than addition, i.e. linear transformations of the coordinates?

Lemma 1.9. *If G is a bipartite graph with $|E| \geqslant |A||B|/K$ for some $K \geqslant 1$, then for any $0 < \varepsilon < 1$, there is $A_0 \subset A$ such that $|A_0| \geqslant |A|/K\sqrt{2}$, and such that $1 - \varepsilon$ of the pairs of vertices in A_0 are connected by $\varepsilon|B|/2K^2$ paths of length 2 in G.*

Proof. By decreasing K, we may assume that $|E| = |A||B|/K$. Now

$$\frac{\mathbf{E}_b|N(b)|}{|A|} = \frac{\mathbf{E}_a|N(a)|}{|B|} = \frac{|E|}{|A||B|} = \frac{1}{K}$$

and

$$\frac{\mathbf{E}_b|N(b)|^2}{|A|^2} = \mathbf{E}_{a,a'}\frac{|N(a) \cap N(a')|}{|B|}$$

□

Let $A_1, \ldots, A_k$ be additive sets with cardinality n, and consider a k uniform k-partite hypergraph H on $A_1, \ldots, A_k$. If H has $\Omega(n^k)$ edges and $|\bigoplus^H A_i| = O(n)$, then we can find $A_i' \subset A_i$ with $|A_i'| = \Omega(n)$ and $|A_1' + \cdots + A_k'| = \Omega(n)$. If we let H be