Additive Combinatorics

Jacob Denson

February 15, 2021

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.

Since we will almost always deal with subsets of the integers rather than subsets of the reals, for notational convenience we let the intervals $[a,b]$, $[a,b)$, (a,b), and $(a,b]$ denote the family of *integers* in these intervals rather than the family of all reals in these intervals, unless otherwise specified.

1.1 Sum Sets

If A and B are subsets of an additive group G, then

$$\max(\#(A),\#(B)) \leqslant \#(A+B) \leqslant \#(A)\#(B).$$

Accounting for symmetry in expressions when $A = B$, we have

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

More generally, a simple stars and bars argument shows that

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

where $A^{\oplus n}$ denotes the n-fold sumset. These bounds are all sharp, e.g. if $\#(A) = 1$. It is a general heuristic that for the 'average' pair of sets A and B, the quantity $\#(A+B)$ is much more likely to be close to $\#(A)\#(B)$, than to $\max(\#(A), \#(B))$.

Example. *Let A and B to be sets of size N and M choosen uniformly at random from $[0,1]$. Then*

$$\mathbf{P}(\#(A+B) = \#(A)\#(B)) = 1.$$

If we let $A = \{X_1, \dots, X_N\}$ and $B = \{Y_1, \dots, Y_M\}$, then the variables $\{X_i, Y_j\}$ are independant and uniformly distributed on $[0,1]$, and for any distinct indices (i_1, j_1) and (i_2, j_2),

$$\mathbf{P}(X_{i_1} + Y_{j_1} = X_{i_2} + Y_{j_2}) = 0.$$

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 for all i and j, and so $\mathbf{P}(\#(A+B) = NM) = 1$.

Example. *Let A and B be subsets of $\mathbf{Z}_N$ 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 $\mathbf{E}(\#(A+B) \geqslant K^2 - K^4/N = \mathbf{E}(\#(A)\#(B)) - K^4/N$. Markov's inequality implies that with high probability, $\#(A+B) \approx \#(A)\#(B)$ if $K \ll N^{1/2}$.

Thus if $\#(A+B)$ is relatively small, it is natural to expect there to be some structure to the sets A and B. A fundamental problem in additive combinatorics is to characterize this structure, the *inverse set problem*. If $\#(A+B) = \max(\#(A), \#(B))$, then A and B have maximal additive structure, and in this case we have a strong characterization of this structure.

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

1. $\#(A+B) = \#(A)$.

2. *$\#(A-B)=\#(A)$.*

3. *$\#(A+B^{\oplus n}-B^{\oplus m})=\#(A)$ for some $(n,m)\neq 0$.*

4. *$\#(A+B^{\oplus n}-B^{\oplus m})=\#(A)$ for all n,m.*

5. *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. Assume $0\in B$ without loss of generality. Then 1. implies $A+B=A$, so for each $a\in A$, $b\in B$, $a+b\in A$. But this means that B is a subset of the *symmetry group* of A, i.e. $\mathrm{Sym}(A)=\{x\in G : A+x=A\}$. If $v,w\in G$, $w\in A$, and $v-w\in\mathrm{Sym}(A)$, then $v=w+(v-w)\in A+(v-w)=A$. Thus A is a union of cosets. Thus we have shown 1. implies 5. A similar argument shows 2. and 3. imply 5., and the remaining implications are simple to verify. □

Corollary 1.2. *If $A=A+A$, then A is a subgroup of G.*

If we have an exact equality $\#(A+B)=\#(A)\#(B)$, we do not have quite as much structure but we note the condition is equivalent to the following properties:

- $\#(A+B)=\#(A)\#(B)$.
- $\#(A-B)=\#(A)\#(B)$.
- $\#\{(a_1,a_2,b_1,b_2)\in A^2\times B^2 : a_1+b_1=a_2+b_2\}=\#(A)\#(B)$.
- $\#\{(a_1,a_2,b_1,b_2)\in A^2\times B^2 : a_1-b_1=a_2-b_2\}=\#(A)\#(B)$.
- $(A-A)\cap(B-B)=\{0\}$.
- For each $c\in A+B$, $\#((A-c)\cap B)=1$.
- For each $c\in B-A$, $\#((A+c)\cap B)=1$.

Remark. It is not always true that $\#(A+B)=\#(A-B)$. For instance, if $A=\{0,1,3\}$ in $\mathbf{Z}$ then $A+A=\{0,1,2,3,4,6\}$ whereas $A-A=\{-1,0,1,2,3\}$. Thus in this case $\#(A+A)=6$ but $\#(A-A)=5$.

Theorem 1.3. *Let A and B be additive sets in a finite group G. If $\#(A)+\#(B)>\#(G)$¡ then $A+B=G$.*

Proof. Fix $x \in G$. If $x \notin A + B$, then for each $a \in A$, $x - a \notin B$. Thus $\#(B) \leqslant \#(G) - \#(A)$, which implies $\#(A) + \#(B) \leqslant \#(G)$, giving a contradiction. □

Theorem 1.4. *Fix $A, B \subset [0, N]$ with $0, N \in A$, and suppose that*

$$\#(A) + \#(B) \geqslant N + 3.$$

Then $\#(A + B) \geqslant N + \#(B)$.

Proof. Let $\phi_N : \mathbf{Z} \to \mathbf{Z}_N$ denote the canonical homomorphism. Then $\#(\phi_N(A)) = \#(A) - 1$, and $\#(\phi_N(B)) \geqslant \#(B) - 1$. Thus

$$\#(\phi_N(A)) + \#(\phi_N(B)) \geqslant \#(A) + \#(B) - 2 \geqslant N + 1.$$

The last theorem implies that $\phi_N(A+B) = \phi_N(A) + \phi_N(B) = \mathbf{Z}_N$. For each $n \in \mathbf{Z}_N$, let $\mu_n = \#((A+B) \cap \phi_N^{-1}(n))$. Then

$$\#(A + B) = \sum_{n \in \mathbf{Z}_N} \mu_n.$$

Our calculations above show that $\mu_n \geqslant 1$ for each $n \in \mathbf{Z}_N$. Furthermore, for each $b \in B$, b and $b + N$ are elements of $A + B$ with $\phi_N(b) = \phi_N(N + b) = b + N\mathbf{Z}$. Thus $\mu_{b+N\mathbf{Z}} \geqslant 2$ for each $b \in B$. But then we conclude that

$$\begin{aligned}
\#(A+B) &= \sum_{n \in \phi_N(B)} \mu_n + \sum_{n \notin \phi_N(B)} \mu_n \\
&\geqslant \sum_{n \in \phi_N(B)} 2 + \sum_{n \notin \phi_N(B)} 1 \\
&= 2\#(\phi_N(B)) + \#(\mathbf{Z}_N - \phi_N(B)) \\
&= N + \#(\phi_N(B)).
\end{aligned}$$

This completes the proof provided that B does not contain both 0 and N. In this case, if we let $B' = B - \{N\}$, then the last case implies that $\#(A+B') \geqslant N - 1 + \#(B)$, and then $(A+B)-(A+B')$ is nonempty, containing $2N$, and so $\#(A + B) \geqslant N + \#(B)$. □

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 1.5. *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. If $|B| \geqslant c|A|$, then $|B+B| \leqslant |A|\sigma(A) \leqslant |B|/c\sigma(A)$ so $\sigma(B) \leqslant \sigma(A)/c$. $\sqrt{2} \cdot \sigma(A)^{1/2}|A|^{1/2}/|A|^{1/2}$ □

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 1.6. *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 The e-transform

In general, the bound $\#(A+B) = \max(\#(A), \#(B))$ holds only if A is a coset and B is a union of cosets of a finite group H of the ambient group G. In particular, in a group containing no nontrivial finite subgroups, like $\mathbf{Z}$ or $\mathbf{Z}_p$, this can only occur A or B is a singleton. A natural question to ask is what the minimum size of $\#(A+B)$ is if A is *not* a singleton. A useful construction in such a setting is the *e-transform*.

Given two sets A and B, and given $e \in A - B$, we set

$$A_e = A \cup (B + e)$$

and

$$B_e = B \cap (A - e).$$

If $C = B \setminus (A - e)$, then A_e is the disjoint union of A and $C + e$. In particular, this means $\#(A_e) + \#(B_e) = \#(A) + \#(B)$; we are, in some sense, rearranging the elements of $A \cup B$ via a single translation. Moreover,

$$\begin{aligned} A_e + B_e &= (A \cup (B+e)) + (B \cap (A - e)) \\ &= (A + (B \cap (A-e))) \cup ((B+e) + (B \cap (A-e))) \\ &\subset (A + B) \cup ((B+e) + (A-e)) = A + B. \end{aligned}$$

Moreover, $\#(A_e) \geqslant \#(A)$ and $\#(B_e) \leqslant \#(B)$, with equality only being obtained if $A \subset B + e$.

Lemma 1.7. *For any set E,*

$$\begin{aligned} |A_e \cap E| + |B_e \cap E| = |A \cap E| + |B \cap E| \\ + |((B+e) \setminus A) \cap (E \setminus (E+e))| \\ - |((B+e) \setminus A) \cap ((E+e) \setminus E)|. \end{aligned}$$

In particular, if $e \in Sym(E)$, then $\#(A_e \cap E) + \#(B_e \cap E) = \#(A \cap E) + \#(B \cap E)$.

Proof. For any set $E \subset G$,

$$\begin{aligned} |A_e \cap E| + |B_e \cap E| &= |A_e \cap E| + |(B_e + e) \cap (E + e)| \\ &= |(A_e \cap E) \cup ((B_e + e) \cap (E+e))| \\ &\quad + |A_e \cap E \cap (B_e + e) \cap (E + e)| \\ &= |A \cap E| + |B \cap E| \\ &\quad + |((B+e) \setminus A) \cap (E \setminus (E+e))| \\ &\quad - |((B+e) \setminus A) \cap ((E+e) \setminus E)|. \end{aligned}$$

□

Let us use the e-transform to improve the lower bound for sum sets over the integers, using the fact that the integers are ordered.

Lemma 1.8. *If $A, B \subset \mathbf{Z}$, then*

$$\#(A+B) \geqslant \#(A) + \#(B) - 1.$$

Proof. Let $e = \max(A) - \min(B)$. Then

$$A_e = A \cup (B+e)$$

is the disjoint union of $A \setminus \{\max(A)\}$, $\{\max(A)\}$, and $(B+e) \setminus \{\max(A)\}$, and

$$B_e = B \cap (A-e) = \{\min(B)\}.$$

Thus

$$\begin{aligned} \#(A+B) &\geqslant \#(A_e + B_e) \\ &= \#(A_e) \\ &= (\#(A) - 1) + (\#(B) - 1) + 1 \\ &= \#(A) + \#(B) - 1. \end{aligned}$$

□

We have a characterization of when this inequality is sharp.

Lemma 1.9. *Let A and B be additive sets in $\mathbf{Z}$. Then $\#(A+B) = \#(A)+\#(B)-1$ if and only if A and B are arithmetic progressions with the same step size.*

Proof. By translating A and B appropriately we may assume $\max(A) = \min(B) = 0$. Then if $e = 0$, then since $\#(A+B)$ is minimal,

$$A + B = A_0 + B_0 = (A \cup B) + \{0\}.$$

Write $A = \{a_n < \cdots < a_1 < 0\}$ and $B = \{0 < b_1 < \cdots < b_m\}$. It is simple to argue combinatorially that $a_1 + b_1 = 0$, that for $2 < i < m$, $a_1 + b_i = b_{i-1}$, and that for $2 < j < n$, $a_j + b_1 = a_{j-1}$. But this implies that A and B are precisely arithmetic progressions with the same step length. □

Now we exploit the fact that $\mathbf{Z}_p$ has no proper subgroups.

Lemma 1.10 (Cauchy-Davenport Inequality)**.** *If p is prime, and A and B are additive sets in $\mathbf{Z}_p$, then*

$$\#(A+B) \geqslant \min(\#(A) + \#(B) - 1, p).$$

Proof. Assume $\#(B) \leqslant \#(A)$. We induct on $\#(B)$. If $\#(B) = 1$ the theorem is trivial. In general, if we can find $e \in A - B$ such that $\#(B_e) < \#(B)$, then induction implies

$$\#(A+B) \geqslant \#(A_e+B_e) \geqslant \min(\#(A_e)+\#(B_e)-1, p) = \min(\#(A)+\#(B)-1, p).$$

On the other hand, if $\#(B_e) = \#(B)$ for all $e \in A - B$, then $B + e \subset A$. This means that $(A + B) - B \subset A$. In particular, $\#(A + B) \leqslant \#(A)$, which actually implies that $\#(A + B) = \#(A)$, that A is a union of cosets of a subgroup of $\mathbf{Z}_p$, and that B is a subset of a coset of this subgroup. Since $\mathbf{Z}_p$ has no nontrivial subgroups, this implies either B is a singleton or $A = \mathbf{Z}_p$; in both of these cases the theorem is trivial. □

Again, aside from trivial examples the only way the Cauchy-Davenport inequality can be tight is if A and B are arithmetic progressions of the same step size.

Lemma 1.11. *Let A and B be additive sets in $\mathbf{Z}_p$ for some prime p, such that $\#(A), \#(B) \geqslant 2$, $\#(A + B) \leqslant p - 2$, and $\#(A + B) = \#(A) + \#(B) - 1$. Then A and B are arithmetic progressions of the same step size.*

Proof. Suppose first that A is an arithmetic progression. Then $A = a + [0, n-1] \cdot v$ for some $v \in \mathbf{Z}_p$ and $n \geqslant 2$. Set $A' = a + [0, n-2] \cdot v$. Then $A + B = A' + (\{0, v\} + B)$, so

$$\begin{aligned}(n-1) + \#(B) &= \#(A) + \#(B) - 1\\ &= \#(A+B)\\ &= \#([0, n-2] + (\{0, v\} + B))\\ &\geqslant (n-1) + \#(\{0, v\} + B) - 1\\ &\geqslant (n-2) + \#(\{0, v\} + B).\end{aligned}$$

Thus $\#(\{0, v\} + B) \leqslant \#(B) + 1$. We cannot have $\{0, v\} + B = B$, since then $B = \mathbf{Z}_p$. Thus there is a unique $k \notin B$ such that $B + \{0, v\} = B \cup \{k\}$. But this means that $B = \{k - v, \dots, k - mv\}$ for some m, which shows B is an arithmetic progression with the same step size as A. By symmetry the claim we have just proven holds if we reverse A and B.

Now suppose instead that $A + B$ is an arithmetic progression. Let $C = -(\mathbf{Z}_p \setminus (A + B))$. Then C is also an arithmetic progression with $\#(C) = p + 1 - \#(A) - \#(B) \geqslant 2$. Note that $B + C \subset -(\mathbf{Z}_p \setminus A)$, so that $\#(B + C) \leqslant$

$p - \#(A) = \#(B) + \#(C) - 1$. The previous paragraph thus shows that B is an arithmetic progression, and thus A is an arithmetic progression.

In general, we induct on $\#(B)$. If $\#(B) = 2$, then B is an arithmetic progression and the theorem is trivial. In general, suppose we can find $e \in A - B$ such that $1 < \#(B_e) < \#(B)$. Then $A + B = A_e + B_e$, so by induction A_e and B_e are both arithmetic progressions with the same step length, so $A_e + B_e = A + B$ is an arithmetic progression, and thus A and B are also. Thus we may assume without loss of generality that $\#(B_e) = 1$ or $\#(B_e) = \#(B)$ for all $e \in A - B$.

If $E = \{e \in A - B : \#(B_e) = \#(B)\}$, then $B + E \subset A$, so by Cauchy-Davenport, $\#(E) \leqslant \#(A) - \#(B) + 1$. But $\#(A - B) \geqslant \#(A) + \#(B) - 1$, so by pidgeonholing there are at least $2\#(B) - 2$ values $e \in A - B$ such that $\#(B_e) = 1$. Since $\#(B) \geqslant 3$, $2(\#(B) - 1) \geqslant \#(B) + 1$, so further pidgeonholing allows us to find find distinct $e_1, e_2 \in A - B$ and $b \in B$ such that $B_{e_1} = B_{e_2} = \{b\}$. Thus

$$A + B = A_{e_1} + b = A_{e_2} + b.$$

Thus $A \cup (B + e_1) = A \cup (B + e_2)$. But $A \cap (B + e_1) = (b + e_1)$ and $A \cap (B + e_2) = (b + e_2)$, so $(B + e_1) \setminus (b + e_1) \subset B + e_2$. But this means that $B \setminus b \subset B + (e_2 - e_1)$, so comparing cardinalities, there exists $b' \in B$ such that $B \setminus b = (B \setminus b') + (e_2 - e_1)$. For each For each $x \in B$, let k_x denote the largest integer such that for $0 \leqslant k \leqslant k_x$, $x + k(e_2 - e_1) \in B$. The inequality above implies that $x + k_x(e_2 - e_1) = b'$. But this means there is m such that

$$B = \{b', b' - (e_2 - e_1), \dots, b' - (m-1)(e_2 - e_1)\},$$

so B is an arithmetic progression. □

We now generalize the last two theorems to arbitrary groups.

Theorem 1.12 (Kneser's Theorem)**.** *For any additive sets A and B, if $H = Sym(A + B)$, then*

$$\#(A + B) \geqslant \#(A + H) + \#(B + H) - \#(H).$$

Often, it is simpler to use the weaker bound

$$\#(A + B) \geqslant \#(A) + \#(B) - \#(H).$$

Proof. Assume $\#(A) \geqslant \#(B)$. We perform a *triple* induction, first on $\#(A+B)$, then $\#(A)+\#(B)$, then $\#(B)$. We induct upwards on $\#(A+B)$, downwards on $\#(A)+\#(B)$, and upwards on $\#(B)$. The downward induction is not contradictory because we have the bound $\#(A)+\#(B) \leqslant 2\#(A+B)$. The base cases where $\#(A+B)=1$, or $\#(A)+\#(B)=2\cdot\#(A+B)$, or where $\#(B)=1$ are obvious and so it suffices to prove the inductive step.

If H is nontrivial, we let $\pi : G \to G/H$ be the standard projection. Then

$$\#(A+B) = \#(H)\#(\pi(A+B)) = \#(H)\#(\pi(A)+\pi(B)).$$

Since $\#(H) > 1$, $\#(\pi(A)+\pi(B)) < \#(A+B)$, and $\mathrm{Sym}(\pi(A+B)) = \{e\}$, so we can apply induction to conclude that

$$\#(\pi(A)+\pi(B)) \geqslant \#(\pi(A)) + \#(\pi(B)) - 1.$$

But this implies that

$$\begin{aligned}\#(A+B) &= \#(H)\cdot\#(\pi(A)+\pi(B)) \\ &\geqslant \#(H)\cdot\#(\pi(A)) + \#(H)\cdot\#(\pi(B)) - 1 \\ &\geqslant \#(A+H) + \#(B+H) - 1.\end{aligned}$$

Thus we may assume in the rest of the argument, without loss of generality, that $\mathrm{Sym}(A+B) = \{e\}$.

Suppose $B_e = B$ for all $e \in A - B$. Then, as we saw in the Cauchy-Davenport theorem, we have $(A+B)-B \subset A$ and so B is contained in a coset of some finite subgroup K of G, and A is a union of cosets in G/K. But this means $K \subset \mathrm{Sym}(A+B) = \{e\}$, which implies that K is trivial, and so B is a singleton, in which case the theorem is trivial.

Thus we are reduced to the case where there exists some $e \in A - B$ such that $\#(B_e) < \#(B)$. Pick e which *maximizes* $\#(B_e)$ subject to the constraint that $\#(B_e) < \#(B)$. Without loss of generality, translating B if necessary, we may assume that $e = 0$. Thus $A_e = A \cup B$ and $B_e = A \cap B$.

Now we know that $\#(A\cup B)+\#(A\cap B) = \#(A)+\#(B)$ and that $\#(A\cap B) < \#(B)$. Thus we may apply induction to conclude that if $X = (A\cup B)+(A\cap B)$, then

$$\#(X) \geqslant \#((A\cup B)+K) + \#((A\cap B)+K) - \#(K),$$

where $K = \mathrm{Sym}(X)$.

Let $C = (A\cap B)+K$. Then

$$(A\cup C)+(B\cup C) = A+B$$

Thus we can replace A and B with $A \cup C$ and $B \cup C$ without modifying $A+B$. If C is not contained in $A \cap B$, then $\#(A \cup C) + \#(B \cup C) > \#(A) + \#(B)$, and so we can apply induction to conclude that

$$\begin{aligned} \#(A+B) &\geqslant \#((A \cup C) + H) + \#((B \cup C) + H) - \#(H) \\ &\geqslant \#(A+H) + \#(B+H) - \#(H). \end{aligned}$$

Thus, without loss of generality, we may assume that $C = A \cap B$. But this means that $K \subset \mathrm{Sym}(A \cap B)$, and so $C = A \cap B$ is a union of cosets of G/K.

We know that X is a subset of $A+B$. If $X = A+B$, then $K = \mathrm{Sym}(A+B) = \{e\}$, and so by the inductive hypothesis,

$$\#(A+B) = \#(X) \geqslant \#(A \cup B) + \#(A \cap B) - 1 = \#(A) + \#(B) - 1.$$

Thus we may assume that X is a proper subset of $A+B$.

Let A' be the set of $a \in A$ such that $a+B$ is not a subset of X. Then A' is nonempty since X is a proper subset of $A+B$. If we pick $b \in B$ such that $a+b \notin X$, then $a+b+K$ is disjoint from X. This means that $((a+K) \cap A)+b$ is disjoint from X, but contained in $A+B$. Thus

$$\#(A+B) \geqslant \#(((a+K) \cap A) + b) + \#(X).$$

Since $b \in A \cup B$, and $X = (A \cap B) + (A \cup B)$, the fact that $a+(b+K)$ is disjoint from X implies that $a+K$ is disjoint from $A \cap B$. This means that

$$\begin{aligned} \#((A \cup B) + K) &\geqslant \#(A \cup B) + \#((a+K) \setminus (A \cup B)) \\ &= \#(A \cup B) + \#(K) - \#((a+K) \cap A) - \#((a+K) \cap B) \end{aligned}$$

Putting these two inequalities together with the inductive hypothesis on $\#(X)$, we find that

$$\begin{aligned} \#(A+B) &\geqslant \#(((a+K) \cap A) + b) + \#(X) \\ &\geqslant \#(((a+K) \cap A) + b) + \#((A \cup B) + K) + \#((A \cap B) + K) - \#(K) \\ &= \#(((a+K) \cap A)) + \#((A \cup B) + K) + \#(A \cap B) - \#(K) \\ &\geqslant \#(A \cup B) + \#(A \cap B) - \#((a+K) \cap B) \\ &= \#(A) + \#(B) - \#((a+K) \cap B). \end{aligned}$$

Our proof would be complete if there exists $a \in A'$ such that $\#((a+K) \cap B) \leqslant 1$. Thus we may assume that $\#((a+K) \cap B) > 1$ for all $a \in A'$. In the next paragraph we show this situation is impossible given our prior assumptions.

For each $a \in A'$, let $A_a = (a+K) \cap A$ and let $B_a = (a+K) \cap B$. Note that for each such a, $A_a - B_a \subset K$. Suppose we can find $a_1, a_2 \in A'$ such that $A_{a_1} - B_{a_1} + B_{a_2}$ is not a subset of A_{a_2}. Then we can find $e \in A_{a_1} - B_{a_1}$ such that $e + B_{a_2}$ is not a subset of A_{a_2}. This means that B is not contained in $A - e$, and so B_e is strictly smaller than B. Since $e \in K$, we find that $B \cap (A - e)$ contains

$$B \cap ((A \cap B) - e) = B \cap (A \cap B) = A \cap B.$$

But this contradicts the maximality of the e-transform we chose at the beginning of the argument, i.e. which gave $B_0 = A \cap B$. Thus we must always have $A_{a_1} - B_{a_1} + B_{a_2} \subset A_{a_2}$ for all $a, a' \in A'$. Symmetry thus implies that $\#(A_{a_1}) = \#(A_{a_2})$ for all $a_1, a_2 \in A'$, and this means that there exists a finite subgroup $L_{a_1 a_2}$ of G such that A_{a_1} and A_{a_2} are a finite union of cosets of $G/L_{a_1 a_2}$, and that B_{a_1} and B_{a_2}, being subsets of $B_{a_1} - B_{a_2}$ and $B_{a_2} - B_{a_1}$ respectively, are contained in a single coset of $G/L_{a_1 a_2}$. Taking $L = \bigcap L_{a_1 a_2}$ shows that B_a is contained in a single coset of G/L for each a and that each A_a is a union of cosets of G/L for each a. Since $\#(B_a) > 1$ for all $a \in A'$, this means that $\#(L) \geqslant 2$. Now

$$A + B = X \cup \bigcup_{a \in A'} (A_a + B)$$

Since $A_a = (a + K) \cap A$ is contained in a coset of K, this means a coset of G/L is contained in a coset of G/K, and thus $L \subset K$. Thus X, which is a union of cosets in G/K, is a union of coset in G/L. On the other hand, $A_a + B$ is also a union of cosets in G/L, since A_a is. But this means $A + B$ is a union of cosets in G/L, hence $L \subset \mathrm{Sym}(A+B)$, contradicting the fact that $\mathrm{Sym}(A+B)$ is trivial. □

Recall that basic estimates show that $\sigma(A) = \delta(A) = 1$ if and only if A is a coset of a finite group. In this corollary to Kneser's theorem, we show that if $\sigma(A)$ or $\delta(A)$ is small, then A is a large subset of a coset of a finite group.

Corollary 1.13. *The following are equivalent:*

1. $\sigma(A) < 3/2$.

2. $\delta(A) < 3/2$.

3. $\#(A+B) < (3/2)\#(A)$ *for some additive set* B *with* $\#(A) \leqslant \#(B)$.

4. $\#(nA - mA) < (3/2)\#(A)$ *for all* n *and* m.

5. A *is a subset of a coset of* G/H *for some subgroup* H *with* $\#(H) < (3/2)\#(A)$.

Proof. It is obvious that (1),(2), and (4) individually imply (3). If we assume (5), then $A + A$ is contained in a single coset of H, and so

$$\sigma(A) = \frac{\#(A+A)}{\#(A)} \leqslant \frac{\#(H)}{\#(A)} < (3/2).$$

Thus (1) holds. Thus it remains to show that (3) implies (5).

Suppose (3) is true. Applying Kneser's theorem, setting $H = \mathrm{Sym}(A+B)$, we conclude that

$$(3/2)\#(A) > \#(A) + \#(B) - \#(H) \geqslant 2\#(A) - \#(H).$$

Rearranging, we find that $\#(H) > \#(A)/2$. But since $\#(H)$ divides $\#(A+B) < 3\#(H)$, this implies that either $\#(A+B) = 2\#(H)$ or $\#(A+B) = \#(H)$. Suppose first that $A + B$ is a union of two cosets in H. Then $\#(H) = (1/2)\#(A+B) < (3/4)\#(A) \leqslant (3/4)\#(B)$, which implies that neither A nor B is contained in a single coset of H. Thus Kneser's theorem implies that

$$2\#(H) = \#(A+B) \geqslant \#(A+H) + \#(B+H) - \#(H) \geqslant 3\#(H),$$

which gives a clear contradiction. On the other hand, if $\#(A+B) = \#(H)$, then $A+B$ is a single coset of G/H, so A is contained in a single coset of G/H, which proves that (5) holds. □

In the next result, we show that if $\#(A+B)$ is suitably small, then Kneser's theorem is actually an equality.

Corollary 1.14. *If* $\#(A+B) \leqslant \#(A) + \#(B) - 1$, *and* $H = Sym(A+B)$, *then*

$$\#(A+B) = \#(A+H) + \#(B+H) - \#(H).$$

Proof. By Kneser's theorem, it suffices to prove

$$\#(A+B) \leqslant \#(A+H) + \#(B+H) - \#(H).$$

Now $\#(H)$ divides $\#(A+B)$, $\#(A+H)$, and $\#(B+H)$. We have the trivial inequality

$$\#(A+B) \leqslant \#(A)+\#(B)-1 \leqslant \#(A+H)+\#(B+H)-1.$$

But since everything here is divisible by $\#(H)$, this inequality immediately improves to give the result that

$$\#(A+B) \leqslant \#(A+H)+\#(B+H)-\#(H). \qquad \square$$

Theorem 1.15. *Let A and B be additive sets. Then*

$$\#(A+B) \geqslant \#(A)+\#(B)-\min_{c\in A+B} \#\{(a,b)\in A\times B : a+b=c\}.$$

Proof. It suffices to prove that for each $c\in A+B$,

$$\#\{(a,b)\in A\times B : a+b=c\} \geqslant \#(A)+\#(B)-\#(A+B).$$

If $\#(A+B)\geqslant \#(A)+\#(B)$, this inequality is trivial. Thus we may assume $\#(A+B)\leqslant \#(A)+\#(B)-1$, in which case it follows that

$$\#(A+B)=\#(A+H)+\#(B+H)-\#(H),$$

where $H=\mathrm{Sym}(A+B)$. We therefore have to prove that

$$\#\{(a,b)\in A\times B : a+b=c\} \geqslant \#(H)-\#((A+H)\smallsetminus A)-\#((B+H)\smallsetminus B).$$

Fix $(a_0,b_0)\in A\times B$ with $a_0+b_0=c$. Then for each $h\in H$,

$$(a_0+h)+(b_0-h)=c.$$

If $(a_0+h,b_0-h)\notin A\times B$, either $a_0+h\in (A+H)\smallsetminus A$ or $b_0-h\in(B+H)\smallsetminus B$. Thus

$$\begin{aligned}\#\{(a,b)\in A\times B &: a+b=c\}\\ &\geqslant \#\{h\in H : (a_0+h,b_0-h)\in A\times B\}\\ &\geqslant \#(H)-\#\{h\in H : a_0+h\in \#((A+H)\smallsetminus A)\}\\ &\qquad\qquad -\#\{h\in H : b_0-h\in \#((B+H)\smallsetminus B)\}\\ &\geqslant \#(H)-\#((A+H)\smallsetminus A)-\#((B+H)\smallsetminus B). \qquad \square\end{aligned}$$

Here is an interesting analytic consequence of Kneser's theorem.

Theorem 1.16. *For any two open sets $A, B \subset \mathbf{T}^d$,*

$$|A+B| \geqslant \min(1, |A|+|B|),$$

where $|\cdot|$ is the unit Haar measure on $\mathbf{T}^d$.

Proof. We note that for each prime p, $\mathbf{T}^d$ has a subgroup G_p isomorphic to $\mathbf{Z}_p^d$. For any open set $U \subset \mathbf{T}^d$, let $U_p = U \cap G_p$. Then

$$|U| = \lim_{p\to\infty} \#(U_p)/p^d.$$

Applying Kneser's theorem, we conclude that

$$\begin{aligned}
|A+B| &= \lim_{p\to\infty} \#((A+B)_p)/p^d \\
&\geqslant \lim_{p\to\infty} \#(A_p+B_p)/p^d \\
&\geqslant \lim_{p\to\infty} \#(A_p)/p^d + \#(B_p)/p^d - \#(\mathrm{Sym}(A_p+B_p))/p^d \\
&\geqslant |A|+|B| - \liminf_{p\to\infty} \#(\mathrm{Sym}(A_p+B_p))/p^d.
\end{aligned}$$

Write $\#(\mathrm{Sym}(A_p+B_p)) = p^{k_p}$ for some $k_p \in [0,d]$. We have $|A+B| \geqslant |A|+|B|$ unless $\#(\mathrm{Sym}(A_p+B_p)) = p^d$ for all sufficiently large p. But this implies that $A_p+B_p = G_p$, which means $A+B$ contains G_p for all sufficiently large p. Since $A+B$ is open, and $\bigcup_{p \geqslant p_0} G_p$ is dense for all choices of p_0, $A+B$ is a dense, open set, and so $|A+B| = 1$. □

Remark. For $A, B \subset \mathbf{R}^d$, the Brunn Minkowski inequality implies that $|A+B| \geqslant (|A|^{1/d}+|B|^{1/d})^d$. This bound is not true in $\mathbf{T}^d$. The bound

$$|A+B| \geqslant \min(1, (|A|^{1/d}+|B|^{1/d})^d)$$

is also not true for $d \geqslant 2$, since we can set $A = \mathbf{T}^{d-1} \times [0,\varepsilon]$ for some $\varepsilon < 1/4$, in which case $A+A = \mathbf{T}^{d-1} \times [0, 2\varepsilon]$, and so $|A+A| = 2\varepsilon$, whereas $(|A|^{1/d}+|B|^{1/d})^d = 2^d\varepsilon$.

If A and B are additive subsets of $[1,N]$, with $\#(A)+\#(B) \geqslant \alpha N$, then Kneser's theorem implies that $\#(A+B) \geqslant \alpha N$. However, it may not be true that $\#((A+B) \cap [1,N]) \geqslant \alpha N$. Mann's theorem shows that this is true if we assume that the numbers in A and B are not heavily weighted to the end of the interval, and also contain the origin.

Theorem 1.17 (Mann's Theorem)**.** *Let $N \geqslant 1$, let $0 < \alpha < 1$, and let A and B be additive subsets of $\mathbf{Z}$, with $0 \in A \cap B$, and for all $1 \leqslant n \leqslant N$,*

$$\#(A \cap [1,n]) + \#(B \cap [1,n]) \geqslant \alpha n.$$

Then $\#((A+B) \cap [1,n]) \geqslant \alpha n$ for all $1 \leqslant n \leqslant N$.

Proof. We prove by induction, first on N and secondly on $\#(B)$. The case where $N = 1$ is trivial. Similarily, if $\#(B) = 1$, then $B = \{0\}$, and then the theorem is trivial. By the inductive hypothesis, for $1 \leqslant n < N$,

$$\#((A+B) \cap [1,n]) \geqslant \alpha n,$$

and it suffices to show that $\#((A+B) \cap [1,N]) \geqslant \alpha N$. Without loss of generality we may assume that $A, B \subset [0,N]$ since adding other elements to A and B only helps us. We will find $e \in A$, which is a subset of $A - B$ since $0 \in B$, such that $\#(B_e) < \#(B)$ and such that for all $1 \leqslant n \leqslant N$,

$$\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) \geqslant \alpha n.$$

The fact that $e \in A$ implies immediately that $0 \in A_e \cap B_e$. We may thus apply the inductive hypothesis together with the fact that $A_e + B_e \subset A + B$, which proves the theorem.

If B is not a subset of A, then we could pick $e = 0$, since then $\#(B_e) < \#(B)$ and by the basic results of the e-transform, for any $1 \leqslant n \leqslant N$,

$$\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) = \#(A \cap [1,n]) + \#(B \cap [1,n]) \geqslant \alpha n.$$

Thus we may assume $B \subset A$. Let e be the minimum element of A such that $e + B$ is not a subset of A. The largest element of A certainly belongs to this set (since B contains a positive integer) so e is well defined. By construction, $(A \cap [0, e-1]) + B$ is contained in A, and $\#(B_e) < \#(B)$. We calculate using basic properties of the e-transform that for $1 \leqslant n \leqslant N$,

$$\begin{aligned}\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) &= \#(A \cap [1,n]) + \#(B \cap [1,n]) \\ &\quad + \#(((B+e) \smallsetminus A) \cap [1,e]) \\ &\quad - \#(((B+e) \smallsetminus A) \cap (n, n+e]) \\ &= \#(A \cap [1,n]) + \#(B \cap [1,n]) \\ &\quad - \#((B \smallsetminus (A-e)) \cap (n-e, n]) \\ &\geqslant \#(A \cap [1,n]) + \#(B \cap [1, n-e]).\end{aligned}$$

If $B \cap (n-e, n] = \varnothing$, then it is simple to conclude by the assumptions of the theorem that $\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) \geqslant \alpha n$. Thus we may assume that $B \cap (n-e, n]$ is nonempty. If b is the minimal element of $B \cap (n-e, n]$. Then $n - b \leqslant e - 1 < N$. Since $A \cap [1,n] = (A_e \cap [1, b-1]) \cup \{b\} \cup (A_e \cap [b+1, n])$,

$$\begin{aligned}\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) &\geqslant \#(A \cap [1,n]) + \#(B \cap [1, n-e]) \\ &= \#(A \cap [1, b-1]) + \#(A \cap [b+1, n]) + 1 \\ &\quad + \#(B \cap [1, b-1]).\end{aligned}$$

By assumption, $\#(A \cap [1, b-1]) + \#(B \cap [1, b-1]) \geqslant \alpha(b-1)$. Since A contains $A \cap [0, e-1] + B$, we conclude that

$$\begin{aligned}\#(A \cap [b+1, n]) &\geqslant \#(((A \cap [0, e-1]) + B) \cap [b+1, n]) \\ &\geqslant \#(((A \cap [0, e-1]) + b) \cap [b+1, n]) \\ &= \#(A \cap [0, e-1] \cap [1, n-b]) \\ &= \#(A \cap [1, n-b]) \\ &= \#((A+B) \cap [1, n-b]) \\ &\geqslant \alpha(n-b).\end{aligned}$$

Putting these inequalities together gives

$$\#(A_e \cap [1,n]) + \#(B_e \cap [1,n]) \geqslant \alpha(b-1) + 1 + \alpha(n-b) \geqslant \alpha n. \qquad \square$$

Finally, we develop an inverse theorem characterizing the behaviour of additive sets A in $\mathbf{Z}$ with $\sigma(A) < 3 - 3/\#(A)$.

Lemma 1.18. *Let A be an additive set in $\mathbf{Z}$, with $0 \in A$. Let $N \geqslant 1$ be an integer, let $\phi_N : \mathbf{Z} \to \mathbf{Z}_N$ be the standard projection map, and for each $x \in \phi_N(A)$, let $\mu(x) = \#\{a \in A : \phi_N(a) = x\}$. Let $m = \min_{x \in \phi_N(A) - \{0\}} \mu_x$. Then*

$$\#(2A) \geqslant \#(A) + (2m-1) \cdot \#(\phi_N(2A)) - (2m - \mu_0) \cdot \#(\phi_N(A)).$$

Proof. We calculate that

$$\begin{aligned}
\#(2A) &= \sum_{x \in \phi_N(2A)} \#(2A \cap \phi_N^{-1}(x)) \\
&\geqslant \sum_{x \in \phi_N(2A)} \sup_{\substack{y,z \in \phi_N(A) \\ y+z=x}} \{\#((A \cap \phi_N^{-1}(y)) + (A \cap \phi_N^{-1}(z)))\} \\
&\geqslant \sum_{x \in \phi_N(2A)} \sup_{\substack{y,z \in \phi_N(A) \\ y+z=x}} \Big(\#(A \cap \phi_N^{-1}(y) + \#(A \cap \phi_N^{-1}(z)) - 1\Big) \\
&= \left(\sum_{x \in \phi_N(2A)} \sup_{\substack{y,z \in \phi_N(A) \\ y+z=x}} \mu(y) + \mu(z) \right) - \#(\phi_N(2A)) \\
&\geqslant \sum_{x \in \phi_N(A)} (\mu_0 + \mu_x) + \sum_{x \in \phi_N(2A) \setminus \phi_N(A)} (2m) - \#(\phi_N(2A)) \\
&= \mu_0 \cdot \#(\phi_N(A)) + \#(A) + 2m \cdot \#(\phi_N(2A) \setminus \phi_N(A)) - \#(\phi_N(2A)) \\
&= \#(A) + (2m-1) \cdot \#(\phi_N(2A)) - (2m - \mu_0) \cdot \#(\phi_N(A)). \qquad \square
\end{aligned}$$

Theorem 1.19. *Let A be an additive set in $\mathbf{Z}$ such that $\sigma(A) < 3 - 3/\#(A)$. Then there is an arithmetic progression of length $\#(2A) - \#(A) + 1$ containing A.*

Proof. Without loss of generality, assume $\min(A) = \{0\}$. Assume also that the elements of A have no common divisor, and that $\#(A) \geqslant 3$. Let $N = \max(A)$. It will suffices to show that $N \leqslant \#(2A) - \#(A)$. Suppose instead that $\#(N) > \#(2A) - \#(A)$. We now apply the last lemma, with $\mu_0 = 2$ and $m = 1$. Thus

$$\#(2A) \geqslant \#(A) + \#(\phi_N(2A)).$$

The hypothesis that $\#(2A) < 3\#(A) - 3$ implies that

$$\#(\phi_N(2A)) < 2\#(A) - 3 = 2\#(\phi_N(A)) - 1.$$

If N were prime we could apply the Cauchy-Davenport theorem. Instead, we use Kneser's theorem, so that

$$2\#(\phi_N(A)) - 1 > \#(\phi_N(2A)) \geqslant 2\#(\phi_N(A) + H) - \#(H),$$

where $H = \text{Sym}(\phi_N(2A))$. If $M = \#(\phi_N(A) + H) - \#(\phi_N(A))$, then

$$0 \leqslant M < \frac{\#(H) - 1}{2}.$$

Since M is an integer, this improves to give a bound

$$0 \leqslant M \leqslant \frac{\#(H) - 2}{2}.$$

Thus $2 \leqslant \#(H) < N$, since $\phi_N(2A) \neq \mathbf{Z}_N$. We can write $H = L\mathbf{Z} + N\mathbf{Z}$ for some $2 \leqslant L \leqslant N/2$ that divides N. Since the elements of A have no common divisor, $\#(\phi_L(A)) \geqslant 2$. We apply the last lemma with ϕ_N replaced by ϕ_L. □

1.5 Freiman Homomorphisms

If A and B are additive sets in two groups G and H, a *Freiman homomorphism* of rank k is a map $f : A \to B$ such that for any $a_1, \dots, a_k, a'_1, \dots, a'_k \in A$, if $a_1 + \dots + a_k = a'_1 + \dots + a'_k$, then $\phi(a_1) + \dots + \phi(a_k) = \phi(a'_1) + \dots + \phi(a'_k)$. If ϕ is a Freiman homomorphism of rank k, it is also a Freiman homomorphism of rank k' for any $k' \leqslant k$. Many problems in additive combinatorics are invariant under Freiman isomorphisms of a suitably large rank.

Remark. One could have defined a 'rank k' additive set A intrinsically by considering an equivalence relation on A^k, i.e. where we imagine that $(a_1, \dots, a_k) \sim (a'_1, \dots, a'_k)$ if $a_1 + \dots + a_k = a'_1 + \dots + a'_k$. One can develop the theory of additive sets intrinsically, but there does not seem to be much advantage in working intrinsically vs extrinsically.

Obviously, all homomorphisms of groups are Freiman homomorphisms of arbitrarily large rank. Similarily, 'affine maps', i.e. homomorphisms composed by translations, are also Freiman homomorphisms. Let us consider some less trivial examples which cannot be induced by homomorphisms of ambient groups.

Example. *The quotient map $\phi : \mathbf{Z} \to \mathbf{Z}_n$, which is a Freiman homomorphism of any order. On the other hand, it is not a Freiman isomorphism, though it restricts to a rank k isomorphism from $[1, m]$ onto its image if $n > k(m-1)$.*

Example. *Fix $a, r \in G$, and let $P = \{a, a+r, \dots, a+(n-1)r\}$ be the corresponding length n arithmetic progression in G. We have a natural Freiman homomorphism $\phi : [0,n) \to P$ which has arbitrarily large rank, because if $m_1 + \dots + m_k = m_1' + \dots + m_k'$, then*

$$\begin{aligned}\phi(m_1) + \dots + \phi(m_k) &= ka + (m_1 + \dots + m_k)r \\ &= ka + (m_1' + \dots + m_k')r \\ &= \phi(m_1') + \dots + \phi(m_k').\end{aligned}$$

On the other hand, this is a Freiman isomorphism of rank k if and only if $ord(r) > k(n-1)$.

Example. *The sets $\{0,1,10,11\}$ and $\{0,1,100,101\}$ are Freiman isomorphic of order k for any $k < 10$, but not for any $k \geqslant 10$.*

Lemma 1.20. *Let $f : A \to B$ be a Freiman homomorphism of rank k. Then if $|\varepsilon_1| + \dots + |\varepsilon_n| \leqslant k$, and $A_1, \dots, A_n \subset A$, then*

$$\#(\varepsilon_1 \phi(A_1) + \dots + \varepsilon_n \phi(A_n)) \leqslant \#(\varepsilon_1 A_1 + \dots + \varepsilon_n A_n).$$

This inequality becomes an equality if f is an isomorphism.

Proof. Without loss of generality assume that $\varepsilon_i \in \{\pm 1\}$ for each i, and that $n = k$. Consider the two maps

$$\psi_1 : A_1 \times \dots \times A_k \to B$$

and

$$\psi_2 : A_1 \times \dots \times A_k \to A$$

where

$$\psi_1(a_1, \dots, a_k) = \varepsilon_1 \phi(a_1) + \dots + \varepsilon_k \phi(a_k),$$

and

$$\psi_2(a_1, \dots, a_k) = \varepsilon_1 a_1 + \dots + \varepsilon_k a_k.$$

Then $\psi_1(A_1 \times \dots \times A_k) = \varepsilon_1 \phi(A_1) + \dots + \varepsilon_n \phi(A_n)$ and $\psi_2(A_1 \times \dots \times A_k) = \varepsilon_1 A_1 + \dots + \varepsilon_n A_n$. If $\psi_2(a_1, \dots, a_k) = \psi_2(a_1', \dots, a_k')$, then

$$\sum_{\varepsilon_i = 1} a_i + \sum_{\varepsilon_i = -1} a_i' = \sum_{\varepsilon_i = 1} a_i' + \sum_{\varepsilon_i = -1} a_i$$

and so

$$\sum_{\varepsilon_i=1} \phi(a_i) + \sum_{\varepsilon_i=-1} \phi(a'_i) = \sum_{\varepsilon_i=1} \phi(a'_i) + \sum_{\varepsilon_i=-1} \phi(a_i)$$

which implies $\psi_1(a_1,\dots,a_k) = \psi_2(a'_1,\dots,a'_k)$. Thus the theorem follows. □

If one wants to understand the sum sets of a *fixed* family of sets $A_1,\dots,A_n$, one needs less structure than a Freiman homomorphism from $A_1 \cup \dots \cup A_n$ to B. Indeed, individual translations of each set preserve all sum sets of the form $\#(k_1A_1 + \dots + k_nA_n)$ and so we would hope these are included in the family of transformations we consider. One trick to doing this is to consider the disjoint union

$$A = A_1 \times \{e_1\} \cup \dots \cup A_n \times \{e_n\}$$

in $G \times \mathbf{Z}^n$. If $\phi : A \to B$ is a rank k Freiman homomorphism, if $|k_1| + \dots + |k_n| = k$, and if we define $\phi_i(a) = \phi(a, e_i)$ for $i \in [1,n]$, then

$$\#(k_1\phi_1(A_1) + \dots + k_n\phi_n(A_n)) \leqslant \#(k_1A_1 + \dots + k_nA_n).$$

We note that the map $\phi : A \to G$ given by setting $\phi(a, e_i) = (a + s_i, e_i)$ is a Freiman isomorphism of arbitrary order.

Theorem 1.21. *Suppose $\phi : A \to B$ is a Freiman homomorphism of order $k \geqslant 2$. If P is a rank k arithmetic progression in A TODO*

An interesting corollary to these definitions is that for any additive set A in a torsion free group, and any $k > 0$, there is an order k Freiman isomorphism from A to a subset of $\mathbf{Z}$, or even to a subset of $\mathbf{Z}_n$ for some large n. We also have a 'compression lemma' in this setting.

Theorem 1.22. *Let A be an additive set in a group G which is torsion, or cyclic of prime order. Fix integers $n, m \geqslant 1$ such that*

$$2n\#(nA - nA) < m < \#(Z).$$

Then there is $A' \subset A$ with $\#(A') \geqslant (1/n)\#(A)$ and an order n Freiman isomorphism from A' to a subset of $\mathbf{Z}_m$.

Proof. Without loss of generality, in light of the preceding paragraph, we may assume A is a subset of $\mathbf{Z}_p$ for some prime p. Consider the three maps $\pi_p : \mathbf{Z} \to \mathbf{Z}_p$, $\pi_m : \mathbf{Z} \to \mathbf{Z}_m$, and $i : \mathbf{Z}_p \to \{0,\dots,p-1\}$, defined in the obvious manner, and set $\pi = \pi_m \circ i$. The function π is not a homomorphism of groups, but it is a Freiman homomorphism of order n when restricted to any set of the form $\pi_p(X)$, where X are a set of fewer than p/n contiguous elements of $\mathbf{Z}$; if $a_1, \dots, a_n$ and $a'_1, \dots, a'_n$ are elements of X, then

$$-p < (a_1 + \cdots + a_n) - (a'_1 + \cdots + a'_n) < p.$$

Thus if $\pi_p(a_1) + \cdots + \pi_p(a_n) = \pi_p(a'_1) + \cdots + \pi_p(a'_n)$, then $a_1 + \cdots + a_n = a'_1 + \cdots + a'_n$, and so $\pi_m(a_1) + \cdots + \pi_m(a_n) = \pi_m(a'_1) + \cdots + \pi_m(a'_n)$.

Consider the disjoint family of sets

$$\{Z_k = \pi_p((k(p/n), (k+1)p/n]) : 0 \leqslant k \leqslant n-1\}.$$

whose union is $\mathbf{Z}_p$. Applying the pidgeonhole principle, for each λ, there exists k_λ such that $\#(Z_{k_\lambda} \cap (\lambda \cdot A)) \geqslant \#(A)/n$. If we set $A_\lambda = Z_{k_\lambda} \cap (\lambda \cdot A)$, then $\pi : A_\lambda \to \mathbf{Z}_n$ is an injective Freiman homomorphism of rank n. All that remains is to show that for some choice of $\lambda \in \mathbf{Z}_p^\times$, π is a Freiman isomorphism of rank n when restricted to the domain A_λ.

It suffices to show that there is some $\lambda \in \mathbf{Z}_p^\times$ such that for any family of elements $a_1, \dots, a_n$ and $a'_1, \dots, a'_n$ in $i(A_\lambda)$ with

$$\pi_m(a_1) + \cdots + \pi_m(a_n) = \pi_m(a'_1) + \cdots + \pi_m(a'_n),$$

then $a_1 + \cdots + a_n = a'_1 + \cdots + a'_n$. We call such an occurence a *collision*. This can only happen if $ni(A_\lambda) - ni(A_\lambda)$ contains a nonzero multiple of m. Since $-n(p-1) \leqslant ni(A_\lambda) - ni(A_\lambda) \leqslant n(p-1)$, if $ni(A_\lambda) - ni(A_\lambda)$ contains km, then $|k| \leqslant n(p-1)/m$. Now for each such integer k,

$$\begin{aligned}
\mathbf{P}(km \in ni(\lambda \cdot A) - ni(\lambda \cdot A)) &= \mathbf{P}(km + p\mathbf{Z} \in \lambda \cdot (nA - nA)) \\
&= \sum_{x \in nA - nA} \mathbf{P}(\lambda x = km + p\mathbf{Z}) \\
&= \sum_{x \in nA - nA} \mathbf{P}(\lambda^{-1} = x/(km + p\mathbf{Z})) \\
&= \sum_{x \in (nA - nA) \setminus \{0\}} \frac{1}{p-1} \\
&\leqslant \frac{\#(nA - nA)}{p-1}.
\end{aligned}$$

A union bound thus implies that a collision happens with probability at most $(2n/m)\#(nA - nA)$. Since $m > 2n\#(nA - nA)$ this probability is less than one, so there is some $\lambda \in \mathbf{Z}_p^\times$ for which no collision occurs. □

Chapter 2

Miscellania

2.1 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 2.1. *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 $X, 2X, \dots, (p-1)X$, which are all sumfree. For every $a \in X$, and nonzero $b \in \mathbf{Z}_p$, there is a unique $c \in [1, p)$ such that $ca = b$. Thus every nonzero $b \in \mathbf{Z}_p$ occurs in $|X|/(p-1)$ of the sets $X, \dots, (p-1)X$. 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 $X = [k, 2k)$, 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*

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

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

2.2 Graph Theoretic Techniques

Theorem 2.2 (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 $\pi : V \to [1,n]$ 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 2.3 (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 2.4. *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. $\square$

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 2.5. *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

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

$\square$

Let $A_1, \dots, A_k$ be additive sets with cardinality n, and consider a k uniform k-partite hypergraph H on $A_1, \dots, A_k$. 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 $|A_1' + \dots + A_k'| = \Omega(n)$. If we let H be