ADDITIVE COMBINATORICS

Gautami Bhowmik

1 Olson's Theorem

For a non-commutative setting we use multiplicative notations. The Minkowski product set AB for two subsets A and B of a multiplicative group G is defined as

$$AB := \{ab : a \in A, b \in B\}.$$

In general, $AB \neq BA$. The inverse set of A is given by

$$A^{-1} := \{a^{-1} : a \in A\}$$

while the left and right translates with respect to an element $x \in G$ are defined as $xA := \{xa : a \in A\}$ and $Ax := \{ax : a \in A\}$.

We will prove Olson's theorem, a non-abelian analogue of Kneser's famous result. We recall that the stabiliser or period of X in an additive group G , denoted by Stab (X), is the subgroup Stab $(X) = \{g \in G : X + g = X\}$.

Theorem 1 (Kneser, 1955)**.** *Let G be an abelian group and $A, B \subset G$ two non-empty finite subsets of G. Then there exists a finite subgroup $H \leq G$ such that*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

Further we may take $H =$ Stab $(A + B)$.

The essential tool in the proof is the Kemperman transformation, a non-commutative analogue of Dyson's transformation.

The Kemperman transformation

Let G be a group and $A, B \subset G$ finite non-empty subsets of G. Let $x \in G$. We define

$$\begin{aligned} A' &= A \cup (Ax) \\ B' &= B \cap (x^{-1}B) \end{aligned}$$

and

$$\begin{aligned} A'' &= A \cap (Ax^{-1}) \\ B'' &= B \cup (xB). \end{aligned}$$

These pairs A', B' and A'', B'', depending on x, are the *Kemperman transformations* of A, B.

Lemma 2. *Let G be a group and $A, B \subset G$ two non-empty finite subsets of G. Now let*

$$D = (A^{-1}A) \cap (BB^{-1}).$$

If $AD \neq A$ or $DB \neq B$, then there exists a pair of finite non-empty subsets $A_1, B_1 \subset G$, obtained by Kemperman transformations of A, B such that

(1) $A_1B_1 \subset AB$

(2) either $|A_1| + |B_1| \geq |A| + |B|$ and $|A_1| > |A|$ or $|A_1| + |B_1| > |A| + |B|$.

Proof. By assumption there exists $d \in D$ such that $Ad \neq A$ or $dB \neq B$. Let $p = |(Ad) \setminus A|$, $q = |(dB) \setminus B|$. We have $\max(p, q) > 0$. Now we shall separate the cases $p \geq q$ and $p < q$.

• Case $p \geq q$. Let us consider the first Kemperman transformation with respect to d, i.e. $A_1 = A' = A \cup (Ad)$ and $B_1 = B' = B \cap (d^{-1}B)$. Then

$$|A_1| = |A \cup (Ad)| = |A| + |(Ad) \setminus A| = |A| + p,$$

and

$$\begin{aligned} |B_1| = |B \cap (d^{-1}B)| &= |B| - |B \setminus (d^{-1}B)| \\ &= |B| - |(dB) \setminus B| = |B| - q. \end{aligned}$$

It follows that $|A_1| + |B_1| = |A| + |B| + p - q \geq |A| + |B|$. In addition since $p = \max(p, q) > 0$ we have $Ad \neq A$ and thus $|A_1| > |A|$.

• Case $p < q$. This time we consider the second Kemperman transformation with respect to d, i.e. $A_1 = A'' = A \cap (Ad^{-1})$ and $B_1 = B'' = B \cup (dB)$. This gives

$$|A_1| = |A| - p, \ |B_1| = |B| + q.$$

It then follows that $|A_1| + |B_1| = |A| + |B| - p + q > |A| + |B|$ as desired. □

By applying the above transformation as long as possible starting with the pair A, B we obtain the following :

Proposition 3. *Let G be a group, $A, B \subset G$ two non-empty finite subsets of G. Then there exist non-empty finite $E, F \subset G$ such that*

(1) $EF \subset AB$

(2) $|E| + |F| \geq |A| + |B|$

(3) If $D = (E^{-1}E) \cap (FF^{-1}),$ then $ED = E$ and $DF = F$.

Proof. By repeated use of the last lemma we find a sequence of subsets

$$(A, B) = (A_0, B_0), (A_1, B_1), \ldots, (A_j, B_j), \ldots$$

satisfying, for all $j \geq 1$,

(1) $A_j B_j \subset A_{j-1} B_{j-1}$.

(2) With lexicographic ordering,

$$(|A_j| + |B_j|,\ |A_j|) > (|A_{j-1}| + |B_{j-1}|,\ |A_{j-1}|).$$

But then the integers $|A_j|, |B_j|$ are bounded since $|A_j|, |B_j| \leq |A_j + B_j| \leq |A + B|$ for all $j \geq 0$. It is now clear that the sequence (A_j, B_j) is *finite*. Therefore there exists an integer $n \geq 0$ such that the assumptions of the lemma no longer applies to the pair $(E, F) = (A_n, B_n)$. Let then $D = (E^{-1}E) \cap (FF^{-1})$, which yields $ED = E$ et $DF = F$. Since $A_j B_j \subset AB$ and $|A_j| + |B_j| \geq |A| + |B|$ for every $j \geq 0$, it follows that $EF \subset AB$ and $|E| + |F| \geq |A| + |B|$. □

We are now in a position to prove Olson's theorem.

Theorem 4. *Let G be a group and let A, B be two non-empty finite subsets of G . Then there exist a nonempty subset $S \subset AB$ and a finite subgroup H of G such that*

$$|S| \geq |A| + |B| - |H|$$

and H stabilises S , i.e.

$$HS = S \text{ or } SH = S.$$

Proof. The last proposition assures us that there exist finite non-empty subsets E, F of G such that $EF \subset AB$ and $|E| + |F| \geq |A| + |B|$. In addition taking $D = (E^{-1}E) \cap (FF^{-1})$ we have $ED = E$ and $DF = F$.

Let now $S = EF$ which is clearly a nonempty subset of AB and whose cardinality we would like to bound in terms of $|A|, |B|$ and $|H|$ for some suitable subgroup H. We distinguish the cases $|E| \geq |F|$ and $|E| \leq |F|$.

Case $|E| \geq |F|$. Once again we have two cases depending on whether FF^{-1} is contained in $E^{-1}E$ or not.

• Suppose that $FF^{-1} \not\subset E^{-1}E$. Then there exist $x_1, x_2 \in F$ such that $x_1 x_2^{-1} \notin E^{-1}E$. We thus have $(Ex_1) \cap (Ex_2) = \emptyset$ and

$$S = EF \supset (Ex_1) \cup (Ex_2).$$

This being a disjoint union $|S| \geq |Ex_1| + |Ex_2| \geq |E| + |F|$. Taking $H = \{1\}$ to be the subgroup of G that stabilises S we get

$$|S| \geq |E| + |F| \geq |A| + |B| \geq |A| + |B| - |H|,$$

as required.

• Suppose now that $FF^{-1} \subset E^{-1}E$. Then $D = FF^{-1}$. Our aim is to show that D is a subgroup of G, that F is a left coset of D and that upto conjugation D is a suitable candidate for the desired subgroup.

Notice first that $0 \in FF^{-1} = D$, et

$$DD = DFF^{-1} = FF^{-1} = D.$$

Now it is easy to see that D is a subgroup of G. Le $z \in F$ be an arbitrary element. We then have

$$F = Fz^{-1}z \subset Dz \subset DF = F.$$

Thus $F = Dz$, a left coset of D. Let

$$H = z^{-1}Dz.$$

Then H is a subgroup of G which stabilise S from the right, since :

$$SH = EFz^{-1}Dz = EDz \subset EF = S.$$

We now evaluate $|S|$.

$$|S| = |EF| \geq |E| = |E| + |F| - |F| = |E| + |F| - |H| \geq |A| + |B| - |H|,$$

as wished for.

Case $|E| \leq |F|$. By the same method as above we obtain a subgroup H stabilising S from the left. □

We now present an application of Olson's theorem .

Definition 1. Let G be a group and r, s two positive integers. Then $\mu_G(r, s) :=$ min $\{|AB|, |A| = r, |B| = s\}$.

Though the function $\mu_G(r, s)$ has been evaluated for all abelian groups, it is yet unknown for non-abelian groups in general.

Theorem 5. *Let G be a torsion-free group. Then $\mu_G(r, s) = r + s - 1$ for all integers $r, s \geq 1$.*

Proof. Let $A, B \subset G$ with $|A| = r, |B| = s$. By Olson's theorem, there exists a non-empty $S \subset A + B$ and a finite subgroup $H \leq G$ such that

$$|S| \geq |A| + |B| - |H|.$$

But $H = \{1\}$ since G is torsion-free and contains no finite non-trivial subgroup. It then follows that

$$|AB| \geq |S| \geq r + s - 1.$$

Thus $\mu_G(r, s) \geq r + s - 1$. On the other hand the lower bound is easily attainable : let $1 \neq x \in G$ be an element and let

$$A = \{x^i \mid 1 \leq i \leq r\}, \quad B = \{x^i \mid 1 \leq i \leq s\}.$$

Then $|A| = r$, $|B| = s$ and $AB = \{x^i \mid 2 \leq i \leq r+s\}$ has cardinality $r+s-1$. Thus $\mu_G(r, s) = r + s - 1$. □

2 The polynomial method

Let F be a field. If $f \in F[X]$ is a non-zero polynomial with r roots in F we know that $\deg(f) \geq r$. The polynomial method is a generalisation of this idea in several variables. The idea originated in a paper of Alon and Tarsi and was formalised as the Combinatorial Nullstellensatz by Alon in 1999. Here we use the notations of Eliahou and Kervaire (1998).

Let $R = F[X_1, \ldots, X_n]$ be the polynomial ring in n variables with coefficients in F. Every polynomial $f \in R$ can be decomposed uniquely as a sum $f = f_0 + f_1 + \cdots + f_m$ of its homogenous components.

Notation Let $f \in R \setminus \{0\}$. By $\mathrm{top}(f)$ we shall denote the homogenous component of highest degree of f . We set $\mathrm{top}(0) = 0$.

For example, $\mathrm{top}(X_1^2 + X_1X_2X_3 - X_1^3) = X_1X_2X_3 - X_1^3$.

Lemma 6. *Let $A_1, \ldots, A_n \subset F$ be finite subsets of cardinalities $|A_i| = r_i$ for each i. Let $f \in R$ be a polynomial that vanishes on the cartesian product $A_1 \times \cdots \times A_n$. Then top$(f) \in (X_1^{r_1}, \ldots, X_n^{r_n})$.*

Proof. By induction on n. The case $n = 1$ is true, since if $f(X_1)$ vanishes for r_1 points of F then $\deg(f) \geq r_1$ and hence $\mathrm{top}(f)$ is divisible by $X_1^{r_1}$.

Let $n \geq 2$ and let the result be true for $n-1$. If every monomial in $\mathrm{top}(f)$ is divisible by $X_n^{r_n}$ then $\mathrm{top}(f) \in (X_1^{r_1}, \ldots, X_n^{r_n})$ and we are done. Let us therefore suppose that $\mathrm{top}(f)$ does not belong to (X_n).

Let

$$g = \prod_{a \in A_n} (X_n - a) \ \in \ F[X_n] \subset F[X_1, \ldots, X_n].$$

Then $\deg_{X_n}(g) = r_n$ and $g(A_1 \times \cdots \times A_n) = \{0\}$. We now write

$$g = X_n^{r_n} - g'$$

with $g' \in F[X_n]$ and $\deg_{X_n}(g') < r_n$. We have $X_n^{r_n} \equiv g' \bmod (g)$ and we can replace every monomial multiple of $X_n^{r_n}$ in f by g' . Thus there exists a polynomial $\bar{f} \in F[X_1, \ldots, X_n]$ such that

1. $f \equiv \bar{f} \bmod (g)$
2. $\deg_{X_n}(\bar{f}) < r_n$
3. $\mathrm{top}(f) \in (X_n^{r_n}, \mathrm{top}(\bar{f}))$.

It now suffices to prove that $\mathrm{top}(\bar{f}) \in (X_1^{r_1}, \ldots, X_{n-1}^{r_{n-1}})$. We notice that $\bar{f}$ vanishes on $A_1 \times \cdots \times A_n$. We can write

$$\bar{f} = \varphi_0 + \varphi_1 X_n + \cdots + \varphi_d X_n^d$$

with $d < r_n$ et $\varphi_i \in F[X_1, \ldots, X_{n-1}]$ for every $0 \leq i \leq d$.

Let $\alpha = (a_1, \ldots, a_{n-1}) \in A_1 \times \cdots \times A_{n-1}$ and let us write

$$\bar{f}_\alpha(X_n) = \varphi_0(\alpha) + \varphi_1(\alpha) X_n + \cdots + \varphi_d(\alpha) X_n^d \ \in \ F[X_n].$$

Then $\bar{f}_\alpha$ vanishes on A_n. Since $\deg \bar{f}_\alpha < r_n$ we have $\bar{f}_\alpha = 0 \in F[X_n]$. It follows that $\varphi_i(\alpha) = 0$ for every $\alpha \in A_1 \times \cdots \times A_{n-1}$ and every $0 \leq i \leq d$. By the induction hypothesis we get

$$\mathrm{top}(\varphi_i) \in (X_1^{r_1}, \ldots, X_{n-1}^{r_{n-1}})$$

for every i. Clearly

$$\mathrm{top}(\bar{f}) \in \big(\mathrm{top}(\varphi_0), \ldots, \mathrm{top}(\varphi_d)\big) \subset (X_1^{r_1}, \ldots, X_{n-1}^{r_{n-1}})$$

which gives $\mathrm{top}(f) \in (X_1^{r_1}, \ldots, X_n^{r_n})$. □

An ideal in R generated by monomials is called a *monomial ideal*.

Lemma 7. *Let $I = (u_1, \ldots, u_r)$ be a monomial ideal generated by the monomials $u_1, \ldots, u_r \in R = F[X_1, \ldots, X_n]$. Let $g \in R$. Then $g \in I$ if and only if every monomial in g with non-zero coefficients is divisible by one of the u_i.*

Proof. Let $\mathcal{M} = \{X_1^{a_1} \cdots X_n^{a_n} \mid a_i \in \mathbb{N} \ \forall i\}$ the set of monomials in R. Then $\mathcal{M}$ is a $F-$base of R. If $g = 0$ the condition is empty. Let $g \in I \setminus \{0\}$. Then there exists $g_1, \ldots, g_r \in R$ such that

$$g = u_1 g_1 + \cdots u_r g_r.$$

On the other hand there exist unique scalars $\{\lambda_u\}_{u \in \mathcal{M}}$ and $\{\mu_{v,i}\}_{v \in \mathcal{M}, i \geq 1}$ such that

$$g = \sum_{u \in \mathcal{M}} \lambda_u u \ \text{ et } \ g_i = \sum_{v \in \mathcal{M}} \mu_{v,i} v$$

for every $i = 1 \ldots, r$. Hence we get

$$\sum_{u \in \mathcal{M}} \lambda_u u = g = \sum_{v \in \mathcal{M}, i \geq 1} \mu_{v,i} u_i v.$$

Since $\mathcal{M}$ is a F-base of R it follows that every monomial $u \in \mathcal{M}$ such that $\lambda_u \neq 0$ is of the form $u_i v$ for $i \geq 1$ and some suitable $v \in M$. □

We conclude :

If $f \in R$ is a non-zero polynomial that vanishes on a finite cartesian product $A_1 \times \cdots \times A_n \subset F^n$, then for every monomial u of maximal degree in f, there exist $i = 1, \ldots, n$ such that

$$X_i^{|A_i|} \text{ divides } u.$$

Let us consider some applications :

Theorem 8. *(Cauchy 1813, Davenport 1935) Let p be a prime number and let A, B be subsets of $\mathbb{Z}/p\mathbb{Z}$. Then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

Proof. Let A, B be subsets of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with cardinalities $|A| = r$, $|B| = s$. We know that if $r + s > p$ then $A + B = \mathbb{F}_p$ and so $|A + B| = p = \min(r + s - 1, p)$.

So let $r + s \leq p$ and set $n = |A + B|$. We would like to show that $n \geq r + s - 1$.

- If $n = p$ all is well.
- If $n < p$, consider the following polynomial $f \in \mathbb{F}_p[X, Y]$:

$$f(X, Y) = \prod_{c \in A+B} (X + Y - c).$$

By construction we have $f(A \times B) = \{0\}$. So we use the Lemma above and obtain $\mathrm{top}(f) \in (X^r, Y^s)$. But

$$\mathrm{top}(f) = \prod_{c \in A+B} (X+Y) = (X+Y)^n.$$

This gives the following condition on n :

$$(X+Y)^n \in (X^r, Y^s)$$

in the polynomial ring $\mathbb{F}_p[X,Y]$. Since the monomial rings X^iY^j form a base of $\mathbb{F}_p[X,Y]$ as a vector space over $\mathbb{F}_p$ the above condition is equivalent to every monomial of $(X+Y)^n$ belonging to the ideal (X^r, Y^s). We have

$$(X+Y)^n = \sum_{i=0}^{n} \binom{n}{i} X^i Y^{n-i},$$

where the binomial coefficients are elements of $\mathbb{F}_p$ and hence reduced modulo p. Now since $n < p$ we have $\binom{n}{i} \not\equiv 0 \bmod p$. It follows that for $0 \leq i \leq n$, the monomial X^iY^{n-i} is in the ideal (X^r, Y^s). In particular for $i = r-1$ we have

$$X^{r-1}Y^{n-r+1} \in (X^r, Y^s),$$

which yields $n - r + 1 \geq s$. Thus $n \geq r + s - 1$. □

As another example we consider the case of restricted sumsets. Erdős and Heilbronn conjectured in 1964 that $|A\dot{+}A| \geq \min\{p, 2|A| - 3\}$, where instead of the whole sumset we consider the restricted one

$$|A\dot{+}B| := \{a + b, a \in A, b \in B, a \neq b\}.$$

This conjecture was proved by Dias da Silva and Hamidoune in 1994 using Grassmanian spaces. The proof, due to Alon, Nathanson and Ruzsa became incredibly simple using the Combinatorial Nullstellensatz.

Theorem 9. *Let p be a prime number and let A, B be subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A\dot{+}B| \geq \min\{p, |A| + |B| - 3\}.$$

Further if $|A| \neq |B|$, then

$$|A\dot{+}B| \geq \min\{p, |A| + |B| - 2\}.$$

Proof. The idea is the same as that for the Cauchy-Davenport theorem, the details are not worked out. Here the polynomial considered is

$$f(X,Y) = (X-Y)\prod_{c\in A+B}(X+Y-c).$$

The coefficients of the monomial are

$$\binom{|A|+|B|-3}{|A|-2} - \binom{|A|+|B|-3}{|A|-1} \bmod p = \frac{(|A|+|B|-3)!}{(|A|-1)!(|B|-1)!}(|B|-|A|) \bmod p$$

which are non-zero modulo p. □

The polynomial method has given many new results in the recent past. Here we mention two concerning sequences with zero sums. We are interested in the minimal size of sequences of $(\mathbb{Z}/p\mathbb{Z})^r$ where p is a prime number, that always contain a zero-sum subsequence of length p. For $r = 1$ this size is known to be $2p-1$ since 1962 but for $r = 2$ the conjectural size was asserted only recently by a very clever use of the polynomial method.

Theorem 10. *(Reiher, 2007) Every sequence of at least* $4p-3$ *elements of* Z_p^2 *contains a zero sum sub-sequence of length* p*.*

We do not give a proof here, the interested reader can contact the author (of these notes).

As an inverse question we describe maximal zero-sum-free sequences of $(\mathbb{Z}/p\mathbb{Z})^r$. For $r = 2$ where it is known that every sequence of at least $2p-1$ elements necessarily contains a zero-sum sequence (of unspecified length), it was very recently proved again by Reiher (2010) that a zero-sum-free sequence of $2p-2$ elements necessarily contains, upto isomorphism, $p-1$ times an element of the type $(1,0)$ and another $p-1$ times an element of the type $(0,1)$. This has the following pertinent consequence!

Proposition 11. *Every sequence of at least* 2011 *elements of* $\mathbb{Z}_3 \oplus \mathbb{Z}_{1005} \oplus \mathbb{Z}_{1005}$ *always contains a zero-sum subsequence.*

How many such elements would be required in the case of an arbitrary group $\mathbb{Z}_a \oplus \mathbb{Z}_{ab} \oplus \mathbb{Z}_{abc}$ is yet unknown and expected to be $a + ab + abc - 2$.