9 The Polynomial Method

Our main goal here is to introduce a very simple and useful tool for solving certain types of combinatorial problems. The main idea is due to Alon and Tarsi, and uses only very basic properties of polynomials to achieve some surprisingly powerful results. We will first use this technique to get a new proof of the Cauchy-Davenport Theorem. Then, we will generalize this proof to achieve a result on a type of restricted sumset problem. If G is an abelian group and $A, B \subseteq G$, then we let $A \oplus B = \{a + b : a \in A,\ b \in B, \text{ and } a \neq b\}$. Our main result from this section is the following theorem on restricted sumsets as conjectured by Erdös and Heilbron.

Theorem 9.1 (Dias da Silva, Hamidoune) *Let p be prime and let $A \subsetneq \mathbb{Z}_p$ be nonempty. Then $|A \oplus A| \geq \min\{p, 2|A| - 3\}$.*

We begin with a quick review of polynomials. Throughout we will fix a finite field $\mathbb{F}$ of order q, and we will use $\mathbb{F}[x_1, x_2, \ldots, x_n]$ to denote the ring of polynomials over $\mathbb{F}$ with variables $x_1, x_2, \ldots, x_n$ (so members of $\mathbb{F}[x_1, \ldots, x_n]$ are formal linear combinations of monomials $x_1^{d_1} \ldots x_n^{d_n}$ with coefficients in $\mathbb{F}$). Every polynomial in this ring gives rise to a mapping from $\mathbb{F}^n$ to $\mathbb{F}$, and we call two polynomials $P, Q \in \mathbb{F}[x_1, \ldots, x_n]$ *equivalent* if they give the same mapping.

Proposition 9.2 *Let $\mathcal{B} = \{x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n} \in \mathbb{F}[x_1, \ldots, x_n] : d_i < q \text{ for } 1 \leq i \leq n\}$. Then $\mathcal{B}$ is a basis of the $\mathbb{F}$-linear space of functions from $\mathbb{F}^n$ to $\mathbb{F}$. In particular, two polynomials $P, Q \in \mathbb{F}[x_1, \ldots, x_n]$ are equivalent if and only if they reduce to the same polynomial by repeatedly using the rewrite rule $x_i^q = x_i$*

Proof: If $z_1, z_2, \ldots, z_n \in \mathbb{F}$, then the polynomial $\prod_{i=1}^n (1 - (x_i - z_i)^{q-1})$ has value 1 at $(z_1, \ldots, z_n)$ and 0 elsewhere. Further, by expanding, this polynomial may be written as a linear combination of elements from $\mathcal{B}$. Since every function may be expressed as a linear combination of such terms, it follows that every function from $\mathbb{F}^n$ to $\mathbb{F}$ may be written as a linear combination of members of $\mathcal{B}$. Since $|\mathcal{B}| = q^n$ and the dimension of the $\mathbb{F}$-linear space of functions from $\mathbb{F}^n$ to $\mathbb{F}$ also has dimension q^n, we find that $\mathcal{B}$ is a basis as required.

Since $\mathbb{F}$ has order q, the multiplicative group $\mathbb{F} \setminus \{0\}$ has order $q - 1$, and it follows that every $z \in \mathbb{F}$ satisfies $z^q = z$. By writing a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$ as a sum of monomials and then using the rewrite rule $x_i^q = x_i$, we reduce P to a linear combination of terms from $\mathcal{B}$ and the result follows. $\square$

If $d_1, d_2, \ldots, d_n < q$, then we define the degree of the monomial $x_1^{d_1} \ldots x_n^{d_n}$ to be $\sum_{i=1}^n d_i$. More generally, by the above proposition, every polynomial function P may be expressed uniquely as a linear combination of terms from $\mathcal{B}$, and we define the degree of P to be the largest degree of a term in the support of in this representation.

Theorem 9.3 (Alon, Tarsi) *Let $P \in \mathbb{F}[x_1, \ldots, x_n]$, and let $x_1^{d_1} \ldots x_n^{d_n}$ have degree equal to the degree of P, and assume that $x_1^{d_1} \ldots x_n^{d_n}$ appears in the expansion of P with nonzero coefficient. If $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}$ satisfy $|A_i| \geq d_i + 1$, then there exists $(z_1, z_2, \ldots, z_n) \in A_1 \times A_2 \ldots \times A_n$ so that $P(z_1, z_2, \ldots, z_n) \neq 0$.*

Proof: Let d be the degree of P which is also equal to $\sum_{i=1}^n d_i$. We may assume without loss that $|A_i| = d_i + 1$ for every $1 \leq i \leq n$ and we set $B_i = \mathbb{F} \setminus A_i$. Using the rewrite rule in the above proposition, we may assume that P is expressed as a linear combination of monomials in $\mathcal{B}$. Now, consider the following polynomial

$$Q(x_1, \ldots, x_n) = P(x_1, \ldots, x_n) \cdot \prod_{i=1}^n \prod_{z \in B_i} (x_i - z).$$

It is immediate from this construction that Q is not identically 0 if and only if there exists $(z_1, \ldots, z_n) \in A_1 \times \ldots \times A_n$ with $P(z_1, \ldots, z_n) \neq 0$. Thus, to complete the proof, it suffices to show that Q is not identically 0. To see that Q is nonzero, consider the term $x_1^{q-1} x_2^{q-1} \ldots x_n^{q-1}$ in the expansion of Q. Since P is written as a linear combination of monomials with degree $< q$ in each variable and total degree $\leq d$, every monomial $x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$ appearing in the expansion of Q has $\sum_{i=1}^n d_i \leq (q-1)^n$. It follows from this that after reducing, the only contribution to the coefficient of $x_1^{q-1} \ldots x_n^{q-1}$ comes from the term $x_1^{d_1} \ldots x_n^{d_n}$ in P and is nonzero. Thus, Q is not identically 0 and the proof is complete. $\square$

The above result also holds without the assumption that $\mathbb{F}$ is finite. The proof of this more general result is quite instructive and the interested reader is encouraged to see Alon's excellent survey article "Combinatorial Nullstellensatz" for a proof of this, and many applications. Our first application will be a new proof of the Cauchy-Davenport Theorem.

Theorem 9.4 (Cauchy-Davenport) *If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.*

Proof: Let A, B be a counterexample to the theorem with $|A|+|B|$ minimum and set $k = |A|$ and $\ell = |B|$. Note that by minimality, we must have $k + \ell \leq p + 1$. Now choose a set $C \supseteq A + B$ with $|C| = k + \ell - 2$ and consider the following polynomial in two variables

$$P(x,y) = \prod_{c \in C}(x + y - c).$$

The degree of P is $k + \ell - 2$ and the coefficient of the term $x^{k-1}y^{\ell-1}$ in the expansion of P is equal to $\binom{k+\ell-2}{k-1} \neq 0$. Applying the previous theorem to this polynomial for the sets A, B gives us a pair $a \in A$ and $b \in B$ with $P(a,b) \neq 0$. But then $a + b \notin C \supseteq A + B$, giving us a contradiction. □

This alternate proof of Cauchy-Davenport is quite useful since it leads to numerous generalizations which do not obviously follow from the original proof. Perhaps the most interesting of these is the following.

Theorem 9.5 (Alon, Nathanson, Ruzsa) *Let p be prime, let $A, B \subseteq \mathbb{Z}_p$ and assume that $|A| \neq |B|$. Then $|A \oplus B| \geq \min\{p, |A|+|B|-2\}$.*

Proof: Let A, B be a counterexample to the above theorem with $|A|+|B|$ minimum and let $k = |A|$ and $\ell = |B|$. We may assume that $2 \leq k \leq \ell$. By the minimality of our counterexample, we may further assume that $k + \ell - 2 \leq p$ (otherwise remove an element of A). Now, choose a set $C \supseteq A \oplus B$ with $|C| = k + \ell - 3$ and consider the following polynomial.

$$P(x,y) = (x - y)\prod_{c \in C}(x + y - c).$$

The coefficient of $x^{k-1}y^{\ell-1}$ is equal to

$$\binom{k+\ell-3}{k-2} - \binom{k+\ell-3}{k-1} = \frac{(k-\ell)(k+\ell-3)!}{(k-1)!(\ell-1)!}$$

which is nonzero modulo p. By applying Theorem 9.3 to this polynomial for the sets A and B we find that there exist $a \in A$ and $b \in B$ with $P(a,b) \neq 0$. But then $a \neq b$ and $a + b \notin C \supseteq A \oplus B$ and we have a contradiction. □

This gives us an easy proof of the Dias da Silva - Hamidoune Theorem as follows.

Proof of Theorem 9.1: If $|A| = 1$ there is nothing to prove. Otherwise choose $a \in A$ and set $A' = A \setminus \{a\}$. Now by the previous theorem we have $|A \oplus A| \geq |A \oplus A'| \geq \min\{p, 2|A| - 3\}$ as required. $\square$

As in the preceeding results in this section, the tool is very simple to prove, but is still quite useful. Our main application of this tool is a lemma due to Alon called the Permanent Lemma, which has found application in graph theory as well as additive number theory.

Lemma 9.6 (Alon's Permanent Lemma) *Let M be an $n \times n$ matrix over $\mathbb{F}$ and assume that $perm(M) \neq 0$. If $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}$ and $|A_i| = 2$ for every $1 \leq i \leq n$ and $z_1, z_2, \ldots, z_n \in \mathbb{F}$, then there exists a vector $a = (a_1, a_2, \ldots, a_n) \in A_1 \times \ldots \times A_n$ so that the i^{th} coordinate of Ma is not equal to z_i for every $1 \leq i \leq n$.*

Proof: Let $M = \{m_{i,j}\}$ and consider the following polynomial

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{n} (m_{i,1}x_1 + m_{i,2}x_2 + \ldots m_{i,n}x_n - z_i).$$

The coefficient of $x_1 x_2 \ldots x_n$ in the expansion of P is equal to the permanent of M which is nonzero. Thus, by Theorem 9.3 there exists a vector $a = (a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$ with $P(a_1, \ldots, a_n) \neq 0$, but then by construction, the i^{th} coordinate of Ma is not equal to z_i for every $1 \leq i \leq n$. $\square$

Next we will use the Permanent Lemma to get another proof of the Erdös Ginzburg Ziv theorem for $\mathbb{Z}_p$. This proof is similar to that of Proposition 5.3, but uses the Permanent Lemma instead of Cauchy-Davenport.

Theorem 9.7 (Erdös, Ginzburg, Ziv) *If β is a sequence in $\mathbb{Z}_p$ of length $2p - 1$, then there is a subsequence of β of length p with sum 0.*

Proof: Let β be given by $b_1, b_2, \ldots, b_{2p-1}$. Identify the elements of $\mathbb{Z}_p$ with the representatives $0, 1, \ldots, p-1$ as usual. By possibly reordering our sequence, we may assume that $b_1 \leq b_2 \ldots \leq b_{2p-1}$. If there exists $1 \leq i \leq p-1$ so that $b_i = b_{p-1+i}$ then some element occurs p times and this subsequence has zero sum. Otherwise, let M be the $(p-1) \times (p-1)$ matrix over $\mathbb{Z}_p$ with all entries 1 and let $z = (z_1, z_2, \ldots, z_{p-1})$ be a list of all elements in $\mathbb{Z}_p \setminus -b_{2p-1}$. By the previous lemma we may choose a vector $a = (a_1, \ldots, a_{p-1}) \in \{b_1, b_p\} \times \{b_2, b_{p+1}\} \ldots \times \{b_{p-1}, b_{2p-2}\}$ so that Ma and z have no coordinates equal. But then by construction, $a_1, a_2, \ldots, a_{p-1}$ is a subsequence of $b_1, \ldots, b_{2p-2}$ with sum equal to $-b_{2p-1}$ so appending the term b_{2p-1} gives us the desired subsequence. □

Conjecture 9.8 (Jaeger) *If M is an invertible matrix over a finite field with order > 3, then there exist a pair of vectors x, y with $Mx = y$ so that x and y have no coordinates equal to zero.*

Since permanents and determinants are the same over fields of characteristic two, the Permanent Lemma implies the truth of Jaeger's conjecture over all such fields. More generally, Alon and Tarsi have shown that Jaeger's conjecture holds over all fields with order not equal to a prime.