II. Polynomials and Their Applications

The aim of this brief chapter is to show that certain combinatorial problems can be attacked with the aid of polynomials. A central result with several applications is the version of Hilbert's Nullstellensatz Alon proved in 1995, a result we shall present in the first section, together with some related theorems. In the second section we shall use polynomials to prove several combinatorial results.

Throughout this chapter, we write $\mathbb{F}$ for a field, and X for the n-tuple $(X_1, \dots, X_n)$ of variables. We shall not assume that $\mathbb{F}$ is algebraically closed, but after the first four results we shall take it to be finite, with characteristic p. In particular, in our applications $\mathbb{F}$ will be a finite field, and occasionally even simply $\mathbb{Z}_p$. We would lose nothing if we assumed from the beginning that $\mathbb{F}$ is a finite field of characteristic p, although that would be an overkill.

1. Zeroes of Polynomials – Alon's Combinatorial Nullstellensatz and Other Results

In this section we shall study polynomials in n variables $X_1, \dots, X_n$ over our field $\mathbb{F}$, concentrating on the set of common zeroes of our polynomials. Our notation is standard and self-explanatory; $\mathbb{F}[X] = \mathbb{F}[X_1, \dots, X_n]$ is the ring of polynomials over $\mathbb{F}$ in n variables, $\deg f$ is the total degree of $f \in \mathbb{F}[X]$, and $\deg_{X_i} f$ is its degree in the variable X_i, etc. The degree of the zero polynomial is taken to be $-\infty$.

The main result of this section is Alon's Combinatorial Nullstellensatz (ACNS): we shall prove it in three bite-size parts we shall call lemmas, and a brief conclusion. These lemmas are just analogues of three basic facts about one-variable-polynomials. The first is division by a monic polynomial over a ring with a remainder term. For example, dividing $3X^4 + X^2 + 2 \in \mathbb{Z}_5[X]$ by $X^2 + X + 1 \in \mathbb{Z}_5[X]$, the remainder is $1 - 3X$:

$$3X^4 + X^2 + 2 = (3X^2 + 2X + 1)(X^2 + X + 1) - 3X + 1.$$

Lemma 1. *Let R be a ring, and $f \in R[X]$ a polynomial of degree d over R in n variables $X = (X_1, \dots, X_n)$. For $i = 1, \dots, n$, set $e_i = \deg_{X_i} f$ and let $g_i \in R[X_i] \subset R[X]$ be a monic polynomial of degree d_i in the*

single variable X_i. Then there are polynomials $h_1, h_2, \ldots, h_n$ and r in $R[X]$ such that

$$f = \sum_{i=1}^{n} h_i g_i + r. \tag{1}$$

and, for all i and j, we have

$$\deg h_i \leq d - d_i, \quad \deg_{X_i} h_i \leq e_i - d_i, \quad \deg_{X_j} h_i \leq e_j \tag{2}$$

and

$$\deg r \leq d, \qquad \deg_{X_i} r \leq d_i - 1, \qquad \deg_{X_j} r \leq e_j. \tag{3}$$

Proof. The conditions on the degrees look quite a mouthful, but in fact they arise trivially if we divide f by g_1, then the remainder by g_2, and so on. This is exactly what we shall do.

Consider f and g_1 as polynomials in X_1 over the ring $R[X_2, \ldots, X_n]$. Then, since g_1 is monic,

$$f = h_1 g_1 + r_1,$$

where h_1 satisfies all the conditions in (2), and r_1 those in (3) for $i = 1$:

$$\deg r_1 \leq d, \quad \deg_{X_1} r_1 \leq d_1 - 1, \quad \text{and} \quad \deg_{X_j} r_1 \leq e_j$$

for all j. Then repeat this with f replaced by r_1, g_1 by g_2, and X_1 by X_2 to obtain h_2 and r_2. Here h_2 satisfies all the conditions in (2) and r_2 those in (3) for $i = 2$ so that we have

$$\deg r_2 \leq \deg r_1 \leq d, \quad \deg_{X_2} r_2 \leq d_2 - 1, \quad \text{and} \quad \deg_{X_j} r_2 \leq e_j$$

for $i = 1, 2$ and all j, and (1) is starting to emerge:

$$f = h_1 g_1 + h_2 g_2 + r_2.$$

Continuing in this way, we obtain $h_3, \ldots, h_n$ and $r_3, \ldots, r_n$; these polynomials h_i and $r = r_n$ satisfy all the conditions in (1), (2) and (3). □

Our second lemma is the multinomial analogue of the fact that a polynomial over a field in a single variable has at most as many zeroes as its degree.

Lemma 2. *Let $r \in \mathbb{F}[X] = \mathbb{F}[X_1, \ldots, X_n]$, where $\mathbb{F}$ is a field, and let $S_1, \ldots, S_n$ be non-empty subsets of $\mathbb{F}$ such that $\deg_{X_i} r < |S_i|$ for every i. Suppose $r(x) = 0$ for all $x = (x_1, \ldots, x_n) \in S = S_1 \times \cdots \times S_n$. Then r is the zero polynomial in $\mathbb{F}[X]$.*

Proof. Let us apply induction on the number of variables. As we have remarked, for $n = 1$ the assertion is the trivial fact that a non-zero polynomial of degree $d \geq 0$ has at most d zeroes. Turning to the induction step, let $n \geq 2$ and suppose for a contradiction that r is a non-zero polynomial. Set $d_n = \deg_{X_n} r$ so that

$$r(X) = \sum_{i=0}^{d_n} g_i(X_1, \ldots, X_{n-1}) X_n^i,$$

where $g_i \in \mathbb{F}[X_1, \ldots, X_{n-1}]$. Fixing $x = (x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, write $c_i \in \mathbb{F}$ for the evaluation $g_i(x_1, \ldots x_{n-1})$. Our condition tells us that the one-variable polynomial f_x given by

$$f_x(X_n) = \sum_{i=0}^{d_n} c_i X_n^i \in \mathbb{F}[X_n]$$

is identically zero on S_n. Since f_x has at least $|S_n| > d_n \geq \deg f_x$ zeroes, by the trivial case $n = 1$ of our theorem f_x is the zero polynomial, so $c_i = 0$ for every i. Hence each $g_i \in \mathbb{F}[X_1, \ldots, X_{n-1}]$ is identically zero on $S_1 \times \cdots \times S_{n-1}$. Consequently, by the induction hypothesis, each g_i is the zero polynomial in $\mathbb{F}[X_1, \ldots, X_{n-1}]$, giving the contradiction that r is the zero polynomial in $\mathbb{F}[X]$. □

Our third and final lemma is an analogue of the fact that a polynomial (of a single variable X) that vanishes at some points $z_1, \ldots, z_k$ is a multiple of $(X - z_1) \ldots (X - z_k)$.

Lemma 3. *For $i = 1, \ldots, n$, let S_i be a non-empty finite subset of a field $\mathbb{F}$, and set $g_i(X_i) = \prod_{s \in S_i} (X_i - s) \in \mathbb{F}[X_i] \subset \mathbb{F}[X]$. Let $f \in \mathbb{F}[X]$ be a polynomial vanishing at the common zeroes of the polynomials g_i; thus $f(x) = 0$ for all $x = (x_1, \ldots, x_n) \in S = S_1 \times \cdots \times S_n$. Then there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[X]$ such that* deg $h_i \leq$ deg $f -$ deg g_i *and*

$$f = \sum_{i=1}^{n} h_i g_i.$$

Proof. As $g_i(X_i)$ is a monic polynomial of degree $|S_i|$, by Lemma 1 we have

$$f = \sum_{i=1}^{n} h_i g_i + r,$$

where deg $h_i \leq$ deg $f - |S_i|$ and $\deg_{X_i} r < |S_i|$. Since f and the polynomials g_i vanish on S, so does r. By Lemma 2, r is the zero polynomial, completing our proof. □

After this preparation, we are ready to prove the main result of this section, Alon's Combinatorial Nullstellensatz.

Theorem 4. *Let $f \in \mathbb{F}[X] = \mathbb{F}[X_1, \ldots, X_n]$ be a polynomial of degree $d = \sum_{i=1}^{n} d_i \geq 1$ in which the coefficient of the monomial $X_1^{d_1} \cdots X_n^{d_n}$ is non-zero and, for $i = 1, \ldots, n$, let $S_i \subset \mathbb{F}$ be such that $|S_i| = d_i + 1$. Then f is not identically zero on $S = S_1 \times \cdots \times S_n$.*

Proof. Suppose for a contradiction that f is identically zero on S. Define n polynomials $g_1, \ldots, g_n \in \mathbb{F}[X]$ as in Lemma 3 by setting

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s),$$

so that deg $g_i = d_i + 1$. Then, by Lemma 3, there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[X]$ such that

$$\deg h_i \leq d - (d_i + 1)$$

and

$$f = \sum_{i=1}^{n} h_i g_i.$$

We know that the coefficient of $X_1^{d_1} \cdots X_n^{d_n}$ in f is non-zero, hence so is the coefficient of this monomial $X_1^{d_1} \cdots X_n^{d_n}$ in one of the summands $h_i g_i = h_i \prod_{s \in S_i} (X_i - s)$. Since $\deg(h_i g_i) \leq d$, every monomial of degree d in $h_i g_i$ is a multiple of $X_i^{|S_i|} = X_i^{d_i+1}$, the highest degree term in g_i, so contains X_i raised to $d_i + 1$ or higher. Consequently, the monomial $X_1^{d_1} \cdots X_n^{d_n}$ (having degree d) cannot occur in $h_i g_i$ with a non-zero coefficient. This contradiction completes our proof. □

When we apply ACNS, we have to check two conditions: that f has degree $d = \sum_{i=1}^{n} d_i \geq 1$, and that the monomial $X_1^{d_1} \ldots X_n^{d_n}$ occurs in f with a nonzero coefficient. The existence of this monomial implies that the degree of f is at least d, so we have to check 'only' that $\deg(f) \leq d$ and the monomial $X_1^{d_1} \ldots X_n^{d_n}$ occurs in f with a nonzero coefficient.

As one of the many applications of his Combinatorial Nullstellensatz, Alon gave a short proof of the classical theorem of Chevalley. This result was conjectured by Artin in 1934 and proved by Chevalley and Warning a year later, the former in its simple form below and the latter in a sharper form, giving the best bound on the number of common zeroes.

Theorem 5. *Let $\mathbb{F}$ be a finite field of order q and characteristic p, and let $f_1, \ldots, f_m \in \mathbb{F}[X] = \mathbb{F}[X_1, \ldots, X_n]$ be non-zero polynomials with*

a common zero such that $\sum_{i=1}^{m} \deg f_i < n$. *Then these polynomials* $f_1, \ldots, f_m$ *have another common zero.*

Proof. Before we start, let us note that $\deg f_i \geq 1$ for every i, so $m < n$. Suppose for a contradiction that our polynomials have only one common zero. We may and shall assume that this common zero is $0 = (0)_1^n \in \mathbb{F}^n$. Define $f \in \mathbb{F}[X]$ by

$$f(X) = \prod_{i=1}^{m} \left(1 - f_i(X)^{q-1}\right) + \gamma \prod_{j=1}^{n} \prod_{\substack{s \in \mathbb{F} \\ s \neq 0}} (X_j - s),$$

where $\gamma \in \mathbb{F}$ is chosen so that $f(0) = 0$. Since at $X = 0$ the first summand on the right is 1, and the second is a non-zero multiple of γ, we have a (unique) choice for γ, which is not 0. Note that both summands are zero at every point $z \neq 0$ since if $f(z) \neq 0$ then, by Fermat's little theorem, $f(z)^{q-1} = 1$. Consequently f is *identically zero* on $\mathbb{F} \times \cdots \times \mathbb{F}$. To complete our proof, let us check that this contradicts Theorem 4.

To this end, note that the degree of the second summand is $n(q-1)$, while that of the first is no more than $(n-1)(q-1)$, so that the degree of f is $n(q-1)$. Furthermore, the coefficient of the monomial $X_1^{q-1} X_2^{q-1} \ldots X_n^{q-1}$ of degree $n(q-1)$ is $\gamma \neq 0$ in the second summand, and so in the polynomial f as well. In this monomial each X_i has degree $q - 1 < |\mathbb{F}| = q$, so by Theorem 4 f is not identically zero on $\mathbb{F} \times \cdots \times \mathbb{F}$, giving us our contradiction. □

In fact, in 1964 James Ax gave a very simple proof of Warning's first theorem for one polynomial, sharpening Chevalley's theorem above and giving us the Chevalley–Warning theorem for one polynomial.

Theorem 6. *Let* $\mathbb{F}$ *be a finite field of characteristic* p, *and let* $f \in \mathbb{F}[X_1, \ldots, X_n]$ *have degree* $d < n$. *Then the number of zeroes of* f *is a multiple of* p.

Proof. Let us write $N(f)$ for the number of zeroes of f as an element of the field $\mathbb{F}$, i.e. if f has $m \in \mathbb{N}$ zeroes then $N(f) = m \cdot 1 \in \mathbb{F}$, where 1 is the unit in $\mathbb{F}$. Then our task is to show that $N(f) = 0$. By Fermat's little theorem, for $z \in \mathbb{F}$ we have

$$z^{q-1} = \begin{cases} 0 & \text{if } z = 0, \\ 1 & \text{otherwise.} \end{cases}$$

Consequently, for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$,

$$1 - f(x)^{q-1} = \begin{cases} 1 & \text{if } f(x) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

and so

$$N(f) = \sum_{x \in \mathbb{F}^n} \left(1 - f(x)^{q-1}\right) = -\sum_{x \in \mathbb{F}^n} f(x)^{q-1}.$$

Now, $f(X)^{q-1}$ has degree $d(q-1) < n(q-1)$, so it is an $\mathbb{F}$-linear combination of monomials of degree less than $n(q-1)$. If $X^u = X_1^{u_1} X_2^{u_2} \ldots X_n^{u_n}$ is such a monomial then one of the exponents u_i is at most $q-2$: we may assume that $u_1 \leq q-2$. The sum $S(u)$ of all evaluations of this monomial over $\mathbb{F}^n$ is

$$S(u) = \sum_{x \in \mathbb{F}^n} x^u = \prod_{i=1}^{n} \sum_{x_i \in \mathbb{F}} x_i^{u_i} = \sum_{x \in \mathbb{F}} x^{u_1} \prod_{i=2}^{n} \sum_{x_i \in \mathbb{F}} x_i^{u_i} = 0,$$

since $\sum_{x \in \mathbb{F}} x^{u_1} = 0$. This implies that $N(f) = 0$ in $\mathbb{F}$, so $N(f)$ is indeed a multiple of p. □

Let us end this section with an extension of this last theorem to the common zeroes of several polynomials obtained by an application of ACNS. This is the Chevalley–Warning theorem.

Theorem 7. *Let p be a prime and let $f_1, \ldots, f_m \in \mathbb{Z}_p[X_1, \ldots, X_n]$ be polynomials such that $\sum_{i=1}^{m} \deg f_i < n$. Then the number of common zeroes of these polynomials $f_1, \ldots, f_m$ is a multiple of p. In particular, if they have a common zero then they have another common zero.*

Proof. Let $z_1, \ldots, z_k \in (\mathbb{Z}_p)^n$ be the common zeroes, with

$$z_i = (z_1^{(i)}, z_2^{(i)}, \ldots, z_n^{(i)}).$$

Assume for a contradiction that k is not a multiple of p. Define a polynomial $f \in \mathbb{Z}_p[X]$ by

$$f = \prod_{i=1}^{m} \left(1 - f_i^{p-1}\right) - \sum_{j=1}^{k} \prod_{i=1}^{n} \left(1 - (X_i - z_i^{(j)})^{p-1}\right). \tag{4}$$

The coefficient of $X_1^{p-1} X_2^{p-1} \ldots X_n^{p-1}$ in the second summand in (4) is $(-1)^{n+1} k \neq 0 \in \mathbb{Z}_p$, and the second summand has no other monomials of degree $n(p-1)$. Furthermore, since

$$(p-1) \sum_{i=1}^{m} \deg f_i \leq (p-1)(n-1) < n(p-1),$$

the first summand has no monomials of degree $n(p-1)$. Thus $\deg f = n(p-1)$ and the coefficient of the monomial $X_1^{p-1}X_2^{p-1}\dots X_n^{p-1}$ in f is not zero. By ACNS, Theorem 4, f is not identically 0 on $(\mathbb{Z}_p)^n$.

To arrive at a contradiction and so to complete our proof, we shall prove that every evaluation $f(x)$ of our polynomial f is 0. In showing this, we consider two cases, whether x is a common zero of our polynomials, or not.

First, what is $f(z_j)$ for a common zero z_j? In the expansion of $f(z_j)$ the first summand in (4) is 1, trivially. Also, the second is -1 since the jth product is 1, while the other $k-1$ products are 0, because for $0 \neq y \in \mathbb{Z}_p$ we have $y^{p-1} = 1$. Hence $f(z_j) = 0$.

Second, what is $f(x)$ if $x = (x_i)$ is not a common root of the f_i? Then $f_i(x) \neq 0$ for at least one i, so $1 - f_i(x)^{p-1} = 0$, implying that the first summand in (4) is 0. So is the second, since in each product

$$\prod_{i=1}^{n} \left(1 - (x_i - z_i^{(j)})^{p-1}\right)$$

at least one of the factors is 0, because $x_i \neq z_i^{(j)}$ for at least one i. Hence $f(x) = 0$, and so f is identically zero on $(\mathbb{Z}_p)^n$. This contradiction completes our proof. □

An even simpler proof of this result can be obtained by tweaking the proof of Ax of Theorem 6: see the Examples.

2. Applications of Polynomials

In this section we shall present some of the many applications of polynomials to combinatorial problems. Although there *are* many applications of polynomials in combinatorics, and people often talk of *'the polynomial method'*, polynomials can only be applied to rather special types of problem, so this 'method' is much less universal than the probabilistic method, say.

Let us start with the algebraic proof of the (very simple) Cauchy–Davenport theorem we have promised.

Theorem 8. *Let p be a prime and A and B two non-empty subsets of $\mathbb{Z}_p$ such that $|A| + |B| \leq p + 1$. Then $|A + B| \geq |A| + |B| - 1$.*

Proof. Suppose for a contradiction that $A+B \subset C \subset \mathbb{Z}_p$ with $|C| \leq |A|+|B|-2 \leq p-1$. Define $f \in \mathbb{Z}_p[X,Y]$ by

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

so that $f(x,y)=0$ for $(x,y) \in A \times B$. However, $\deg f = |A|+|B|-2$, and the coefficient of $X^{|A|-1}Y^{|B|-1}$ in f is

$$\binom{|A|+|B|-2}{|A|-1} \neq 0 \in \mathbb{Z}_p,$$

contradicting ACNS. □

Similarly, the prime order case of the Erdős-Ginzburg-Ziv theorem is an easy consequence of Theorem 5, Chevalley's theorem. Needless to say, our original proof was even simpler.

Theorem 9. *For a prime p, every sequence $a_1, a_2, \ldots, a_{2p-1} \in \mathbb{Z}_p$ has p terms whose sum is 0.*

Proof. Define $f_1, f_2 \in \mathbb{Z}_p[X] = \mathbb{Z}_p[X_1, \ldots, X_{2p-1}]$ as follows:

$$f_1(X) = \sum_{i=1}^{2p-1} a_i X_i^{p-1} \quad \text{and} \quad f_2(X) = \sum_{i=1}^{2p-1} X_i^{p-1}.$$

Since $\deg f_1 + \deg f_2 = 2(p-1) < 2p-1$ and $0 = (0)_1^{2p-1}$ is a common root of f_1 and f_2, by Theorem VI.5 there is another common root, $(x_1, \ldots, x_{2p-1})$, say. Setting $I = \{i : x_i \neq 0\} \neq \emptyset$,

$$x_i^{p-1} = \begin{cases} 1 & \text{if } i \in I, \\ 0 & \text{if } i \notin I, \end{cases}$$

so $|I| = p$ and $\sum_{i \in I} a_i = 0 \in \mathbb{Z}_p$. □

Returning to the topic of sumsets, this time we shall investigate *restricted sums* of sets. Given sets $A, B \subset \mathbb{Z}_p$, at least how large is their sum if we demand that the summands are different. Thus, at least how large is

$$A \oplus B = \{a+b : a \in A, b \in B, a \neq b\}?$$

Trivially, if $|A|=1$ then $|A \oplus B| = |B|$ if $A \not\subset B$ and $|A \oplus B| = |B|-1$ if $A \subset B$. Also, $[n] \oplus [n] = [3, 2n-1]$, so for $n \geq 2$ we have $|[n] \oplus [n]| \geq 2n-3$ provided $2n-3 \leq p$. In 1964, Erdős and Heilbronn conjectured that for $A = B$ the restricted sum is at least as large as for $A = [n]$:

$$|A \oplus A| \geq 2|A| - 3,$$

if $2|A| - 3 \leq p$. This conjectured inequality seems to be a short step from the Cauchy–Davenport theorem but, amazingly, in spite of a number of serious attacks by many people, the Erdős–Heilbronn conjecture remained unsolved for thirty years: eventually, in 1994, Dias da Silva and Hamidoune managed to prove it. Soon after this celebrated result, Alon, Nathanson and Ruzsa realized that in fact this conjecture is a very simple consequence of ACNS. Thus, given the right tool, the following theorem of Alon, Nathanson and Ruzsa, implying the Dias da Silva–Hamidoune theorem, is hardly more than a not too difficult exercise. Note that if $A = [n]$ and $B = [m]$ for $n \neq m$ then $A \oplus B = [3, n+m-2]$, so $|A \oplus B| = n + m - 2$. The result below claims that this is an extremal example.

Theorem 10. *Let p be a prime, and A and B non-empty subset of $\mathbb{Z}_p$ with $|A| \neq |B|$ and $|A| + |B| \leq p + 2$. Then*

$$|A \oplus B| \geq |A| + |B| - 2.$$

Proof. Set $a = |A|$ and $b = |B|$ so that a and b are different natural numbers. We may assume that $a < b$.

Suppose our assertion is false, so that $A \oplus B \subset C \subset \mathbb{Z}_p$, where $|C| = a + b - 3 < p$. Since $|A \oplus B| \geq |B| - 1 = b - 1$, we must have $a \geq 2$. Clearly, the polynomial

$$f(X,Y) = (Y - X) \prod_{c \in C} (X + Y - c) \in \mathbb{Z}_p[X,Y]$$

is identically zero on $A \times B$.

On the other hand, $\deg f = a+b-2$, and the coefficient of the monomial $X^{a-1}Y^{b-1}$ in f is

$$\binom{a+b-3}{a-1} - \binom{a+b-3}{a-2} = \frac{b-a}{a-1}\binom{a+b-3}{a-2} \neq 0 \in \mathbb{Z}_p,$$

since $a + b - 3 < p$. This contradicts ACNS, and so completes our proof. □

The following immediate consequence of this theorem is slightly stronger than the Erdős–Heilbronn conjecture, as stated above.

Corollary 11. *Let p be a prime and let A and B be non-empty subsets of $\mathbb{Z}_p$ with $|A| + |B| \leq p + 3$. Then $|A \oplus B| \geq |A| + |B| - 3$.*

Proof. If $|A| \neq |B|$ then this is obvious from Theorem 10, so it suffices to consider the case $|A| = |B| \geq 2$. Pick an element b of B and set

$B' = B \setminus \{b\}$, so that $|B'| < |A|$. By Theorem 10,

$$|A \oplus B| \geq |A \oplus B'| \geq |A| + |B'| - 2 = |A| + |B| - 3$$

as claimed. □

At a round table for $2n+1$ people, with the single host sitting in one of the chairs, n couples are to be seated in such a way that the ith couple are at distance d_i for each other. We call $(d_i)_1^n$ the *pattern* of this seating arrangement. What are the patterns $(d_i)_1^n$, $1 \leq d_i \leq n$ for every i, that can be realized?

Theorem 12. *Let $2n+1 = p$ be a prime $p \geq 3$ and let $1 \leq d_i \leq n$ for $i = 1, \ldots, n$. Then there is a seating arrangement with pattern $(d_i)_1^n$.*

Proof. Let us represent the round table by $\mathbb{Z}_p$, with the host in seat 0. We are looking for a seating arrangement in which the ith couple are sitting in seats numbered x_i and $x_i + d_i$, neither of which is 0. To spell it out, the x_i should be such that for all $1 \leq i \neq j \leq n$ we have

$$x_i \neq 0,\ \ x_i+d_i \neq 0,\ \ x_i \neq x_j,\ \ x_i \neq x_j+d_j,\ \ x_j \neq x_i+d_i,\ \ x_i+d_i \neq x_j+d_j.$$

Let us define a polynomial $f(X) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ whose evaluation at $x = (x_i)_1^n$ is 0 whenever one of the conditions above fails. Clearly,

$$f(X) = \left(\prod_{i=1}^{n} X_i\right)\left(\prod_{i=1}^{n}(X_i + d_i)\right)$$
$$\times \prod_{1 \leq i < j \leq n} (X_i - X_j)(X_i - X_j - d_j)(X_i + d_i - X_j)(X_i + d_i - X_j - d_j)$$

is such a polynomial. We see that

$$\deg f \leq 2n + 4\binom{n}{2} = 2n^2,$$

so by ACNS f is not identically zero on $(\mathbb{Z}_p)^n$ if the coefficient c of the monomial $X_1^{2n} X_2^{2n} \ldots X_n^{2n}$ in f is nonzero. Clearly, c is also the coefficient of this monomial in

$$\left(\prod_{i=1}^{n} X_i\right)^2 \prod_{1 \leq i < j \leq n} (X_i - X_j)^2 (X_j - X_i)^2$$
$$= \left(\prod_{i=1}^{n} X_i\right)^{2n} \prod_{i \neq j} \left(1 - \frac{X_i}{X_j}\right)^2.$$

Thus, c is the constant term of the Laurent polynomial

$$\prod_{i \neq j} \left(1 - \frac{X_i}{X_j}\right)^2.$$

By the result in Exercise II. 20, c is the multinomial coefficient

$$\binom{2n}{2, 2, \ldots, 2},$$

which is nonzero in $\mathbb{Z}_p = \mathbb{Z}_{2n+1}$. (In fact, c is 1 or -1 in $\mathbb{Z}_p$.) Hence f is not identically zero on $(\mathbb{Z}_p)^n$, and every place $x \in (\mathbb{Z}_p)^n$ with $f(x) \neq 0$ gives a suitable seating arrangement. □

Alon's Combinatorial Nullstellensatz also gives a proof of the following special case of a theorem of Marshall Hall.

Theorem 13. *Let p be a prime, and let $b_1, \ldots, b_p \in \mathbb{Z}_p$ be a sequence of (not necessarily distinct) elements with zero sum: $\sum_{i=1}^{p} b_i = 0$. Then there are two enumerations of the elements of $\mathbb{Z}_p$, say, $a_1, \ldots, a_p$ and $c_1, \ldots, c_p$, such that $a_i + b_i = c_i$ for every i, $i = 1, \ldots, p$.*

Proof. We shall prove this in the following equivalent formulation. Let $b_1, \ldots, b_{p-1} \in \mathbb{Z}_p$ be not necessarily distinct elements. Then there are two sequences of $p-1$ distinct elements of $\mathbb{Z}_p$, $a_1, \ldots, a_{p-1}$ and $c_1, \ldots, c_{p-1}$, such that $a_i + b_i = c_i$ for every i, $1 \leq i \leq p-1$. Equivalently, there is a sequence $a = (a_1, \ldots, a_{p-1})$ of $p-1$ distinct elements such that $a_1 + b_1, \ldots, a_{p-1} + b_{p-1}$ are also distinct. Note that our sequences have length only $p-1$, and the sequence $b_1, \ldots, b_{p-1}$ is not required to satisfy any condition. Indeed, each of the sequences $(a_i)_1^{p-1}, (b_i)_1^{p-1}, (c_i)_1^{p-1}$ has a unique extension, as in the case of (b_i) we must have $b_1 + \cdots + b_p = 0$, and each of the other two sequences must consist of p different terms. Then the last terms automatically satisfy the required relation $a_p + b_p = c_p$.

Clearly, a sequence $(a_i)_1^{p-1}$ will do if an only if $f(a) \neq 0$, where $f(X)$ is the following polynomial of $p-1$ variables $X = (X_1, \ldots, X_{p-1})$:

$$f(X) = \prod_{1 \leq i < j \leq p-1} (X_i - X_j)\,(X_i + b_i - X_j - b_j) \in \mathbb{Z}_p[X].$$

Then $\deg f \leq 2\binom{p-1}{2} = (p-1)(p-2)$, so by ACNS we are done if the coefficient c of the monomial $X_1^{p-2} \ldots X_{p-1}^{p-2}$ in the expansion of f is non-zero. Writing c' for the coefficient of the monomial $X_1^{p-2} \ldots X_{p-1}^{p-2}$

in the expansion of

$$g(X) = \prod_j \prod_{i \neq j} (X_i - X_j) = \left(\prod_{i=1}^{p-1} X_i^{p-2} \right) \prod_j \prod_{i \neq j} \left(1 - \frac{X_i}{X_j} \right),$$

we have $c = \pm c'$. But c' is just the constant term in

$$\prod_j \prod_{i \neq j} \left(1 - \frac{X_i}{X_j} \right),$$

which, by Exercise II. 20, is

$$\binom{p-1}{1, \ldots, 1} = (p-1)! = -1 \in \mathbb{Z}_p.$$

Hence $c \neq 0$, so our proof is complete. □

The penultimate result we shall present is an extension of the Erdős–Ginzburg–Ziv theorem to two dimensions. For a prime p, let $s(p, 2)$ be the minimal m such that every sequence of m vectors in the two-dimensional $\mathbb{Z}_p$-vector space $\mathbb{Z}_p \oplus \mathbb{Z}_p$ contains p terms summing to 0. Clearly, $s(p, 2) \geq 4p - 3$, since the sequence of length $4p - 4$ in which each of the vectors $(0, 0), (0, 1), (1, 0)$ and $(1, 1)$ occurs $p - 1$ times does not have p terms whose sum is 0.

In 1983, Kemnitz conjectured that this is an extremal example, so $s(p, 2) = 4p - 3$. In 2000, Rónyai came close to proving this conjecture: he proved that $s(p, 2) \leq 4p - 2$. Rónyai's proof below makes use of the result of Alon and Dubiner in Exercise II. 22 that if $a_1, \ldots, a_{3p}$ are vectors in $V = \mathbb{Z}_p \oplus \mathbb{Z}_p$ then some p of them also sum to 0. Soon after Rónyai's result, in October 2003, the conjecture was proved in full by two people independently: by Christian Reiher (an undergraduate at the time) and Carlos di Fiore (a high school student at the time). The two proofs are rather similar. The curious sequence of events continued when a fortnight later Savchev and Chen found a different proof, although not independently of the original two proofs.

Theorem 14. *Let p be a prime and let $v_1, v_2, \ldots, v_m$ be $m = 4p - 2$ vectors in the vector space $V = \mathbb{Z}_p \oplus \mathbb{Z}_p$ over $\mathbb{Z}_p$. Then some p of the vectors v_i sum to 0.*

Proof. The subsets of $[m]$ are in one-to-one correspondence with the points in $\{0, 1\}^m$. To express this one-to-one correspondence, we introduce the following notation: a set $J \subset [m]$ corresponds to the point

$z = x(J)$, where $z = (z_i)_1^m \in \{0,1\}^m$ is given by

$$z_i = \begin{cases} 1 & \text{if } i \in J, \\ 0 & \text{otherwise,} \end{cases}$$

and a point $z \in \{0,1\}^m$ corresponds to the set

$$I(z) = \{i \in [m] : \ z_i = 0\}.$$

Viewing $\{0,1\}^m$ as a subset of $\mathbb{Z}_p^m$, so that polynomials in $\mathbb{Z}_p[X, \dots, X_m]$ can be evaluated at the points in $\{0,1\}^m$, our task is to look for a point $x = (x_i)_1^m \in \{0,1\}^m$ with $\sum_1^m x_i v_i = 0$ and $|I(x)| = p$.

Assume that our theorem is false, so that our aim is to arrive at a contradiction. Trivially, $p \geq 3$, and by the result in Exercise II. 22, for all $J \subset [m]$ with $|J| = p$ or $|J| = 3p$ we have $\sum_{j \in J} v_j \neq 0 \in V$. Denote by a_i and b_i the coordinates of the vectors v_i so that $v_i = (a_i, b_i)$, $i = 1, \dots, m$. Write $f_0(X)$ for the polynomial

$$\left(\left(\sum_{i=1}^m a_i X_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^m b_i X_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^m X_i\right)^{p-1} - 1\right),$$

and set

$$g(X) = \sum_{I \in [m]^{(p)}} \prod_{i \in I} X_i,$$

so that $\deg f_0 \leq 3p-3$ and $\deg g = p$. If $f_0(x) \neq 0$ for some $x \in \{0,1\}^n$, then at this point x the three inner sums in f_0 are 0; in particular, $\sum_{i=1}^m x_i$ is 0 in $\mathbb{Z}_p$, so $|I(x)|$ is a multiple of p. As the possibilities $|I(x)| = 0$, p and $3p$ have been ruled out, if $f_0(x) \neq 0$ for some $x \in \{0,1\}^n$ then we must have $|I(x)| = 2p$. In that case $g(x) = \binom{2p}{p} = 2 \in \mathbb{Z}_p$. Consequently, the polynomial

$$f(X) = f_0(X)\big(g(X) - 2\big)$$

of degree at most $4p-3 = m-1$ is such that for $x \in \{0,1\}^m$ it satisfies

$$f(x) = \begin{cases} 2 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

An even more 'natural' polynomial with the same evaluation on $\{0,1\}^m$ as f is

$$h(X) = 2(X_1 - 1)(X_2 - 1) \dots (X_m - 1),$$

which is a polynomial of degree m. In this polynomial the monomial $X_1 \dots X_m$ has coefficient 2; since $p \geq 3$, this coefficient is non-zero. But then $h(X) - f(X)$ is also a polynomial of degree m with $2X_1 \dots X_m$ the

highest degree monomial . This contradicts ACNS, since $h(X) - f(X)$ is identically zero on $\{0,1\}^m$, the product of m sets of two elements each. □

Here is another way of arriving at a contradiction in the proof above. The set

$$\left\{\prod_{i\in I} X_i : I \subset [m]\right\}$$

of 2^m monomials is a basis for the $\mathbb{Z}_p$-vector space of functions $\{0,1\}^m \to \mathbb{Z}_p$, but the coefficient $c_{[m]}$ in the expansion of $h(X) - f(X)$ above is 2, which is nonzero in $\mathbb{Z}_p$.

Our last application of polynomials is of a rather different nature. Our aim is to prove an upper bound on the cardinality of a 'two-distance set' in $\mathbb{R}^n$, a set whose pairs of points determine only two distances. In this theorem, proved by Larman, Rogers and Seidel in 1977, we shall use just about the most basic properties of polynomials, namely that a subspace of the vector space $\mathbb{R}[X_1, \ldots, X_n]$ spanned by ℓ polynomials does not contain $\ell + 1$ linearly independent polynomials.

Theorem 15. *Let $S = \{s_1, \ldots, s_m\}$ be a set of m points in $\mathbb{R}^n$ such that any two points are at distance d_1 or d_2. Then $m \leq (n+1)(n+4)/2$.*

Proof. Write s_{ij} for the coordinates of our points: $s_j = (s_{1j}, s_{2j}, \ldots, s_{nj})$ so that for $1 \leq j < k \leq m$ the sum $\sum_{i=1}^m (s_{ij} - s_{ik})^2$ is either d_1^2 or d_2^2. Let us use the set S to define m polynomials $f_j(X) = f_j(X_1, \ldots, X_m)$ in the space $\mathbb{R}[X_1, \ldots, X_m]$ as follows:

$$f_j(X) = \left(\sum_{i=1}^n (X_i - s_{ij})^2 - d_1^2\right)\left(\sum_{i=1}^n (X_i - s_{ij})^2 - d_2^2\right).$$

Evaluating f_j on S, we see that it is $d_1^2 d_2^2$ at s_j and 0 at every other point; consequently as members of the real vector space of functions on S the polynomials $f_1, \ldots, f_m$ are independent. Therefore these polynomials are also independent in the vector space $\mathbb{R}[X]$. Also, each f_j is a linear combination of the polynomials

$$\left(\sum_{i=1}^n X_i^2\right)^2, \quad X_j\left(\sum_{i=1}^n X_i^2\right), \quad X_i X_j, \quad X_i, \quad 1$$

for $1 \leq i \leq j \leq n$. As the number of these polynomials is $1 + n + n(n+1)/2 + n + 1 = (n+1)(n+4)/2$, the number m of points in our two-distance set is indeed at most $(n+1)(n+4)/2$. □

This theorem is close to being best possible: writing $m(n)$ for the maximal cardinality of a 2-distance set, one can show that $m(n)$ is at least $n(n+1)/2$. Also, Blokhuis improved the upper bound in Theorem 15 to $(n+1)(n+2)/2$. For these results, see the Third Examples Sheet.

III. Projections of Bodies and Set Systems

In this chapter we shall prove and apply somewhat unusual isoperimetric inequalities in which our task is to minimize many quantities measuring the 'boundary'.

1. The Box Theorem of Bollobás and Thomason

By a *body* in $\mathbb{R}^n$ we shall mean a *bounded open subset* of $\mathbb{R}^n$. As it happens, nothing is gained by considering general probability measures (rather than $\mathbb{R}^n$ with the standard Lebesgue measure) and measurable sets (rather than open sets), so we shall stray with this very pleasant set-up. In fact, we would lose nothing if we restricted our attention to even 'nicer' bodies, like unions of finitely many cubes in standard position. Nevertheless, in the results below and in later applications there is no need to make sure that our bodies are open sets, as any 'nice' set will do for a body. Our aim is to relate the volume of a body to the volumes of its canonical projections.

To set the scene, let $(e_1, \dots, e_n)$ be the canonical basis for $\mathbb{R}^n$, and for $A \subset [n]$ let K_A be the orthogonal projection of a body K into $\mathrm{lin}\{e_i : i \in A\}$, the subspace spanned by the basis vectors e_i, $i \in A$. We denote by $|K|$ the appropriate dimensional volume of a body, so that if K is a body in $\mathbb{R}^n$ and $A \subset [n]$, $|A| = d$, then $|K|$ is the n-dimensional volume of K and $|K_A|$ is d-dimensional volume of K_A. We shall use the convention that $|K_\emptyset| = 1$ whenever $K \neq \emptyset$, although much of the time we shall avoid the trivial projection $K_\emptyset$. Clearly, $|K| \leq \prod_{i=1}^n |K_{\{i\}}|$, and it is only a little less obvious that

$$|K| \leq \prod_{i=1}^{s} |K_{A_i}|,$$

whenever the sets $A_1, A_2, \dots, A_s$ partition $[n]$, since in that case $K \subset \prod_{i=1}^s K_{A_i}$. Our aim is to go beyond these trivial observations.

If we view the set of numbers $\{|K_A| : A \subset [n]\}$ as a measure of the 'boundary' of $K \subset \mathbb{R}^n$, we are led to a natural isoperimetric problem. Recall that if our aim is to minimize the 'perimeter length' (measure of the boundary) of a 2-dimensional body $K \subset \mathbb{R}^2$, then a circular disc will do for L. Somewhat similarly, given a body K, is there a canonical

body L such that $|L| = |K|$ and $|L_A| \leq |K_A|$ for *every* $A \subset [n]$? A moment's thought tells us that we cannot look for a canonical body that depends only on the volume $|K|$: our solution L has to depend on the 'shape' of K as well.

Note that, unlike in a usual isoperimetric problem, our aim is to minimize not only one scalar, but $2^n - 2$ quantities: $|K_A|$ for all $A \subset [n]$, $A \neq \emptyset, [n]$. Nevertheless, the Box Theorem of Bollobás and Thomason shows that, somewhat surprisingly, this multi-scalar isoperimetric problem also has a rather pleasant solution. By a *box* we mean a canonically oriented rectangular parallelepiped, i.e. one whose sides are parallel to the coordinate axes. If we wish to be pedantic, then we define a box in $\mathbb{R}^n$ as a product of n finite open intervals.

After this preparation, we may state the following Box Theorem of Bollobás and Thomason, BTBT. Clearly, this result should have been published in the middle of the 19th century, rather than in 1995.

Theorem 1. *Let $K \subset \mathbb{R}^n$ be a body. Then there is a box $L \subset \mathbb{R}^n$ such that $|K| = |L|$ and $|K_A| \geq |L_A|$ for every $A \subset [n]$.*

We shall deduce Theorem 1 from a certain cover inequality we shall prove first. In fact, a variant of this inequality was proved by Shearer in 1978, years before the Box Theorem appeared, but was published only in 1986 in a paper by Chung, Graham, Frankl and Shearer.

For $k \geq 1$, a *k-cover* of $[n]$ is a multiset $\mathcal{A}$ of nonempty subsets of $[n]$ such that every $i \in [n]$ is contained in ('covered by') *at least* k members of $\mathcal{A}$. We call $\mathcal{A}$ an *exact k-cover* or a *uniform k-cover* if every $i \in [n]$ is contained in precisely k members of $\mathcal{A}$. Finally, $\mathcal{A}$ is a *uniform cover* of $[n]$ if it is a uniform k-cover for some $k \geq 1$. Thus, using an obvious shorthand, $\{1, 12, 13, 23, 23\}$ is a uniform 3-cover of $[3]$, and $\{123, 234, 345, 456\}$ is a 2-cover of $[6]$ which is not uniform.

As further preparations for our first result in this chapter, let us make some remarks about sections of bodies and their connections to projections. Formally, for $K \subset \mathbb{R}^n = \mathbb{R}^{[n]}$ and $A \subset [n]$, the *projection* of K into $\mathrm{lin}\{e_i : i \in A\}$ is

$$K_A = \{(x_i)_{i \in A} \in \mathbb{R}^A : \exists\, (y_i)_1^n \in K \text{ such that } y_i = x_i \text{ whenever } i \in A\}.$$

For a real number x, the *section* of K (really, the section of K at height x in direction n) is

$$K(x) = K_n(x) = \{(x_i)_1^{n-1} \in \mathbb{R}^{[n-1]} : (x_1, \ldots, x_{n-1}, x) \in K\}.$$

For $K \subset \mathbb{R}^A$, with $n \in A$, the section $K(x) = K_n(x) \subset \mathbb{R}^{A\setminus\{n\}}$ is defined analogously. Note that for a body $K \subset \mathbb{R}^n$ we have $K_A \subset \mathbb{R}^A$ and $K(x) \subset \mathbb{R}^{[n-1]}$. Also,

$$\bigcup_{x\in\mathbb{R}} K(x)_B = K_B \quad \text{if} \quad B \subset [n-1],$$

and, more importantly for us, one can check that

$$K_{B\cup\{n\}}(x) = K(x)_B \subset K_B \quad \text{if} \quad B \subset [n-1]. \tag{1}$$

Finally, Fubini's theorem tells us that

$$|K| = \int |K(x)|\mathrm{d}x. \tag{2}$$

Having defined the ingredients for its proof, here is *Uniform Cover Inequality*, UCI.

Theorem 2. *Let K be a body in $\mathbb{R}^n$, and let $\mathcal{A}$ be a uniform k-cover of $[n]$. Then*

$$|K|^k \leq \prod_{A\in\mathcal{A}} |K_A|. \tag{3}$$

Proof. Let us apply induction on n. For $n = 1$ there is nothing to prove, so let us turn to the induction step. Suppose that $n \geq 2$, and the inequality holds for bodies of dimension less than n. Let us split $\mathcal{A}$ into two multisets:

$$\mathcal{B} = \{B \in \mathcal{A} : \ n \notin B\}$$

and

$$\mathcal{C} = \{C \in \mathcal{A} : \ n \in C\}.$$

Note that $|\mathcal{C}| = k$; furthermore, $\mathcal{D} = \mathcal{B} \cup \{C \setminus \{n\} : \ C \in \mathcal{C}\}$ is a uniform k-cover of $[n-1]$. Hence, by Fubini's theorem, i.e. identity

(2), the induction hypothesis, and relation (1),

$$\begin{aligned}
|K| &= \int |K(x)|\mathrm{d}x \le \int \prod_{D\in\mathcal{D}} |K(x)_D|^{1/k}\mathrm{d}x \\
&= \int \prod_{B\in\mathcal{B}} |K(x)_B|^{1/k} \prod_{C\in\mathcal{C}} |K(x)_{C\setminus\{n\}}|^{1/k}\mathrm{d}x \\
&\le \prod_{B\in\mathcal{B}} |K_B|^{1/k} \int \prod |K_C(x)|^{1/k}\mathrm{d}x \\
&\le \prod_{B\in\mathcal{B}} |K_B|^{1/k} \prod \left(\int |K_C(x)|\mathrm{d}x\right)^{1/k} \\
&= \prod_{B\in\mathcal{B}} |K_B|^{1/k} \prod_{C\in\mathcal{C}} |K_C|^{1/k} = \prod_{A\in\mathcal{A}} |K_A|^{1/k}.
\end{aligned}$$

In the third (and final) inequality we applied the general form of Hölder's inequality for exponents $k, k, \ldots, k$ (k times): $\|\prod_1^k f_i\|_1 \le \prod_1^k \|f_i\|_k$. □

This Uniform Cover Inequality is an extension of the classical inequality of *Loomis and Whitney*, proved in 1949.

Corollary 3. *For a body $K \subset \mathbb{R}^n$ and an integer d, $1 \le d \le n-1$ we have*

$$|K|^{\binom{n-1}{d-1}} \le \prod_{A\in[n]^{(d)}} |K_A|.$$

Proof. The collection of all d-subsets of $[n]$ is a uniform $\binom{n-1}{d-1}$-cover of $[n]$. □

In 1981, Allan rediscovered the Loomis–Whitney inequality, and also gave a more streamlined proof of it.

Note that the Uniform Cover Inequality is an immediate consequence of the Box Theorem. Indeed, given a body $K \subset \mathbb{R}^n$ and a uniform k-cover $\mathcal{A}$ of $[n]$, let L be a box as in Theorem 1. Then

$$|K|^k = |L|^k = \prod_{A\in\mathcal{A}} |L_A| \le \prod_{A\in\mathcal{A}} |K_A|.$$

On the other hand, to deduce the Box Theorem from the Uniform Cover Inequality we shall have to work a little, and also need another ingredient, a simple assertion about uniform covers.

Call a uniform cover $\mathcal{A}$ *reducible* if it is the disjoint union of two uniform covers, and *irreducible* otherwise. For example, the uniform 3-cover of [3] we mentioned earlier, $\{1, 12, 13, 23, 23\}$, is reducible, while $\{1234, 156, 156, 23, 245, 245, 346\}$ is an irreducible 3-cover of [6].

We claim that there are only finitely many irreducible uniform covers of $[n]$. Indeed, suppose that we do have an infinite sequence of distinct irreducible covers, $\Sigma_0 = (\mathcal{A}_0^{(j)})_{j=1}^{\infty}$, say. Let $S_1, \ldots, S_{2^n}$ be an enumeration of the subsets of $[n]$. For $i = 1, \ldots, 2^n$, select infinite sequences $\Sigma_i = (\mathcal{A}_i^{(j)})_{j=1}^{\infty}$ of uniform covers such that Σ_i is a subsequence of Σ_{i-1}, and the number of copies of S_i in $\mathcal{A}_i^{(j)}$ is a non-decreasing function of j. Since every infinite sequence (n_j) of non-negative integers has an infinite non-decreasing subsequence, we can indeed select $\Sigma_1, \ldots, \Sigma_{2^n}$. But then, the number of copies of S_i in $\mathcal{A}_{2^n}^{(j)}$ is a non-decreasing function of j for every i, $i = 1, \ldots, 2^n$; in particular, if $\mathcal{A} = \mathcal{A}_{2^n}^{(1)}$ and $\mathcal{A}' = \mathcal{A}_{2^n}^{(2)}$ then $\mathcal{A} \subset \mathcal{A}'$, since every set $S_i \subset [n]$ occurs at least as many times in $\mathcal{A}'$ as in $\mathcal{A}$. Consequently, $\mathcal{A}'$ is reducible, contradicting our assumption.

Note that this little argument tells us that there are only finitely many irreducible uniform covers of $[n]$, but gives no upper bound for this number $D(n)$. Such an upper bound was given by Huckeman, Jurkat and Shapley (see Graver(1976)): $D(n) \leq (n+1)^{(n+1)/2}$ for every n, and similar results have been proved by Alon and Berman (1986) and Füredi (1992). In 1997, Alon and Vu went much further: they essentially determined $D(n)$: proved that $D(n) \sim n^{(1/2+o(1))n}$.

Proof of Theorem 1. We may and shall assume that $\emptyset \neq K \subset \mathbb{R}^n$, and $n \geq 2$. Theorem 1 tells us that

$$|K|^k \leq \prod_{A \in \mathcal{A}} |K_A| \tag{4}$$

whenever $k \geq 1$ and $\mathcal{A}$ is an irreducible uniform k-cover of $[n]$. Furthermore, as remarked earlier, for every set $A \subset [n]$ we have the trivial inequality

$$|K_A| \leq \prod_{i \in A} |K_{\{i\}}|. \tag{5}$$

Note that we have *finitely many* inequalities in (4) and (5), but (4) holds for *every* uniform k-cover $\mathcal{A}$, since every uniform cover is the disjoint union of irreducible uniform covers.

We shall arrive at our box by reducing the $|K_A|$, $\emptyset \neq A \subset [n]$ as much as we can without violating these inequalities, keeping $|K|$ constant.

To this end, let $\{x_A : A \in \mathcal{P}(n)\}$ be a collection of *minimal* nonnegative numbers such that

$$0 \leq x_A \leq |K_A| \tag{6}$$

for every $A \subset [n]$ with equality for $A = [n]$ and $A = \emptyset$, so that $x_{[n]} = |K|$ and $x_\emptyset = 1$,

$$|K|^k \leq \prod_{A \in \mathcal{A}} x_A \tag{7}$$

for every irreducible k-cover $\mathcal{A}$, and

$$x_A \leq \prod_{i \in A} x_i \tag{8}$$

for every $A \subset [n]$, $2 \leq |A| \leq n$.

Why is there such an array of x_A? At the danger of overexplaining the obvious, note that the collection Π of arrays $\{x_A : A \in \mathcal{P}(n)\}$ satisfying (6), (7) and (8) is a compact subset of $\mathbb{R}^{\mathcal{P}(n)}$, so the continuous function $\sum_{A \in \mathcal{P}(n)} x_A$ attains its minimum: with a slight abuse of terminology we write $\{x_A : A \in \mathcal{P}(n)\}$ for a place where this minimum is attained.

Trivially, each x_A is strictly positive. Since the x_A have to satisfy only finitely many constraints, every x_A, $A \neq [n]$, must appear on the right-hand side of at least one inequality of type (7) or (8) in which *equality holds*. The crucial step in our proof is the following claim.

Claim. For every i, $i \in [n]$, there is a uniform k_i-cover $\mathcal{C}_i$ containing $\{i\}$ with

$$|K|^{k_i} = \prod_{A \in \mathcal{C}_i} x_A. \tag{9}$$

Indeed, each x_i appears on the right-hand side of at least one inequality of type (7) or (8) in which equality holds. If this equality has type (7), we are done. Otherwise, $x_A = \prod_{i \in A} x_i$ for some set $A \subset [n]$ with $2 \leq |A| \leq n$. But then, as x_A itself is minimal, it appears on the right-hand side of an inequality of type (7) with equality: there is a uniform k_i-cover $\mathcal{A}_i$ with $A \in \mathcal{A}_i$ such that

$$|K|^{k_i} = \prod_{A \in \mathcal{A}_i} x_A.$$

Then $\mathcal{C}_i = (\mathcal{A}_i \setminus \{A\}) \cup \{\{j\} : j \in A\}$ will do for (9), proving our claim.

The uniform cover $\mathcal{C}_i$ we have found need not be irreducible, but if we needed it to be irreducible (we don't!), we could assume that it was since every set contained in a uniform cover is in a minimal uniform subcover which is, by definition, irreducible.

To complete the proof of our theorem, set $\mathcal{C} = \bigcup_{i=1}^{n} \mathcal{C}_i$ and $k = \sum_{i=1}^{n} k_i$: by our construction, $\mathcal{C}$ is a uniform k-cover containing every singleton set $\{i\}$, with

$$|K|^k = \prod_{A \in \mathcal{C}} x_A.$$

Clearly, $\mathcal{C}' = \mathcal{C} \setminus \{\{1\}, \{2\}, \ldots, \{n\}\}$ is a uniform $(k-1)$-cover, so

$$|K|^{k-1} \leq \prod_{A \in \mathcal{C}'} x_A.$$

Consequently.

$$|K| = |K|^k / |K|^{k-1} \geq \left(\prod_{A \in \mathcal{C}} x_A \right) \Big/ \left(\prod_{A \in \mathcal{C}'} x_A \right) = \prod_{i=1}^{n} x_i.$$

Recalling (7), we see that

$$|K| = \prod_{i=1}^{n} x_i.$$

Finally, given $A \subset [n]$, the 1-uniform cover of $[n]$ formed from A and the singleton sets $\{i\}$, $i \in [n] \setminus A$, tells us that

$$|K| \leq x_A \prod_{i \notin A} x_i \leq \prod_{i \in A} x_i \prod_{i \notin A} x_i = \prod_{i=1}^{n} x_i = |K|.$$

Hence $x_A = \prod_{i \in A} x_i$, and so the box L with side length x_i in the direction of e_i satisfies $|L| = |K|$ and $|L_A| = x_A \leq |K_A|$ for every $A \subset [n]$. □

In our results like UCI, a uniform k-cover of $[n]$ by multisets may be replaced by an *exact fractional cover*, a function $\psi : \mathcal{P}(n) \to [0,1]$ such that

$$\sum \{\psi(A) : \ i \in A \subset [n]\} = 1$$

for every i. The value $\psi(A)$ is the multiplicity or 'weight' of A. If we relax the condition on ψ and demand only that the sum of the multiplicities of the sets containing a point $i \in [n]$ is *at least* 1, rather than exactly 1, then we get a *fractional cover* of $[n]$. The 'normalized form' of a uniform k-cover $\mathcal{A}$ is the exact fractional cover ψ in which $\psi(A)$ is the number of times A occurs in the multiset $\mathcal{A}$ divided by k. Clearly, UCI is equivalent to the assertion that if $K \subset \mathbb{R}^n$ is a body and ψ is an exact fractional cover of $[n]$ then

$$|K| \leq \prod_{A \subset [n]} |K_A|^{\psi(A)}. \tag{10}$$

Much of the time, UCI suffices for our applications, but occasionally we do need BTBT, which can be viewed as the totality of the UCIs for all uniform covers or fractional covers. Here is an example of the latter. Consider real-valued functions of 2^n variables, with the variables indexed by the 2^n subsets of $[n]$; for example, $f((x_A)_{A\subset[n]}) = -1 + \sum_{A\neq\emptyset} x_A^{\min A}$. Given such a function $f : \mathbb{R}^{\mathcal{P}(n)} \to \mathbb{R}$ and a body $K \subset \mathbb{R}^n$, we call K *f-dominated* if $f((|K_A|)_{A\subset[n]}) \leq 0$. So, in our example, K is f-dominated if $\sum_A |K_A|^{\min A} \leq 1$. Theorem 1 tells us how to find the largest volume of a body which is f-dominated for a family of monotone functions f.

Theorem 4. *Let $f_\gamma : \mathbb{R}^{\mathcal{P}(n)} \to \mathbb{R}$, $\gamma \in \Gamma$, be monotone increasing functions in each of the 2^n variables. Then*

$$\begin{aligned} &\sup\{\, |K| : \ K \text{ is } f_\gamma\text{-dominated for every } \gamma \in \Gamma\} \\ = \ &\sup\{\, |L| : \ L \text{ is a box and } L \text{ is } f_\gamma\text{-dominated for every } \gamma \in \Gamma\}. \end{aligned}$$ □

Let us make some further remarks about Theorems 1 and 2. First, it is not unreasonable to hope that Theorem 1 can be strengthened to preserve inclusions. To be precise, BTBT tells us that for every body $K \subset \mathbb{R}^n$ there is a box $L = L(K) \subset \mathbb{R}^n$ such that $|L| = |K|$ and $|L_A| \leq |K_A|$ for every $A \subset [n]$. Can this map $K \mapsto L(K)$ be chosen to preserve inclusions so that $L(K') \subset L(K)$ whenever $K' \subset K$? For this, see the Third Examples Sheet.

Turning to the Uniform Cover Inequality, does it remain true for (not necessarily uniform) k-covers? A moment's thought tells us that it does not. Indeed, suppose that $\mathcal{A}$ is a non-uniform k-cover of $[n]$ so that some $i \in [n]$ is in at least $k+1$ sets $A \in \mathcal{A}$. For $0 < \varepsilon < 1$, let $K = [0, \varepsilon]^n$ be a cube of volume ε^n. Then $|K|^k = \varepsilon^{kn}$, while $\prod_{A\in\mathcal{A}} |K_A| \leq \varepsilon^{kn+1}$. However, if our body is 'not too thin', like a pancake, then we do not have to assume that our cover is uniform. We state this in a very special case.

Corollary 5. *Let $K \subset \mathbb{R}^n$ be the union of some canonically oriented unit cubes. Then for every k-cover $\mathcal{A}$ of $[n]$ we have*

$$|K|^k \leq \prod_{A\in\mathcal{A}} |K_A|.$$

Proof. Since for $\emptyset \neq B \subset A \subset [n]$ we have $|K_B| \leq |K_A|$, our inequality follows by reducing $\mathcal{A}$ to a uniform k-cover, and applying UCI. □

It is much less facetious to ask when equality holds in (3). Call two points $i, j \in [n]$ *equivalent* with respect to a cover $\mathcal{A}$ if they belong

to exactly the same sets in $\mathcal{A}$, and let $\mathcal{E}(\mathcal{A})$ be the set of equivalence classes. It is clear that if for $E \in \mathcal{E} = \mathcal{E}(\mathcal{A})$ we have a body K^E in $\mathbb{R}^E$ then for the body $K = \prod_{E\in\mathcal{E}} K^E \subset \mathbb{R}^n$ and the cover $\mathcal{A}$ we have equality in (3). In fact, one can show that equality holds only in this case.

Crudely, UCI tells us that if we can bound the volumes of the projections K_A for the members A of a uniform cover $\mathcal{A}$ then we can bound the volume of the body K. Of course, the same holds if $\mathcal{A}$ itself is not a uniform cover, but it *generates* a uniform cover in the sense that there is a uniform cover $\mathcal{B}$ such that $A \in \mathcal{A}$ whenever $A \in \mathcal{B}$. (Thus the uniformly covering multiset $\mathcal{B}$ is formed by taking some members of $\mathcal{A}$ with certain multiplicities. Needless to say, this cannot happen unless $\mathcal{A}$ is a cover of $[n]$.) As the following result shows, in no other case can we prove a bound on $|K|$.

Theorem 6. *Let $\mathcal{A}$ be a cover of $[n]$ which does not generate a uniform cover. Then for every $c > 0$ there is a body K in $\mathbb{R}^n$ with $|K_A| \le 1$ for all $A \in \mathcal{A}$ and $|K| > c$.*

The proof is left as an exercise.

Let us note some consequences of BTBT and UCI for finite sets and sequences: some of these corollaries are easily seen to be equivalent to the original inequality.

Corollary 7. *Let S be a finite subset of $\mathbb{Z}^n$ and for $A \subset [n]$ let S_A be the projection of S onto the subspace spanned by $\{e_i : i \in A\}$. Then there are $b_1, \dots, b_n \ge 0$ such that*

$$|S| = \prod_1^n b_i \quad \text{and} \quad |S_A| \ge \prod_{i\in A} b_i \tag{11}$$

for every $A \subset [n]$. Also, for every k-cover $\mathcal{A}$ of $[n]$ we have

$$|S|^k \le \prod_{A\in\mathcal{A}} |S_A|. \tag{12}$$

Proof. Identify a lattice point $\mathbf{z} \in \mathbb{Z}^n$ with the unit cube $Q_\mathbf{z} \subseteq \mathbb{R}^n$ with centre $\mathbf{z}$, and map S into $\cup_{\mathbf{z}\in S} Q_\mathbf{z}$. Apply Corollary 5. □

Note that in (12) we did not demand that the k-cover $\mathcal{A} = \{A_i\}$ is uniform. Indeed, if $A' \subset A$ then $|S_{A'}| \le |S_A|$; therefore, by removing elements from the sets A_i so as to obtain a *uniform* k-cover $\mathcal{A}' = \{A_i'\}$ with $A_i' \subset A_i$, we have $|S|^k \le \prod_i |S_{A_i'}| \le \prod_i |S_{A_i}|$.

We may also think of S as a finite set of sequences of length n, with S_A as the set of subsequences indexed by A. This gives us the following reformulation of Corollary 7.

Corollary 8. *Let S be a finite set of sequences of length n. Then are numbers $b_1, \dots, b_n \geq 0$ such that*

$$|S| = \prod_1^n b_i \quad \text{and} \quad |S_A| \geq \prod_{i \in A} b_i \tag{13}$$

for every $A \subset [n]$. In particular, for every k-cover $\mathcal{A}$ of $[n]$ we have

$$|S|^k \leq \prod_{A \in \mathcal{A}} |S_A|. \tag{14}$$

If we are dealing with 0–1 sequences, then we are led to set systems since, as usual, a set $X \subset [n]$ is naturally identified with its indicator sequence $x = (x_i) \in \{0,1\}^n$. In this set-up, given a set system $\mathcal{F} \subset \mathcal{P}(n)$ and a set $A \subset [n]$, the projection of $\mathcal{F}$ onto A is also known as the *trace* of $\mathcal{F}$ on A: $\mathcal{F}_A = \{F \cap A : F \in \mathcal{F}\}$. Inequality (16) is the variant of UCI that Shearer had proved in 1978, years before UCI was published. We shall also note a simple form of these bounds suitable for applications.

Corollary 9. *Let $\mathcal{F}$ be a set of subsets of $[n]$. Then are numbers $b_1, \dots, b_n \geq 0$ such that*

$$|\mathcal{F}| = \prod_1^n b_i \quad \text{and} \quad |\mathcal{F}_A| \geq \prod_{i \in A} b_i \tag{15}$$

for every $A \subset [n]$. In particular, for every uniform k-cover $\mathcal{A}$ of $[n]$ we have

$$|\mathcal{F}|^k \leq \prod_{A \in \mathcal{A}} |\mathcal{F}_A|. \tag{16}$$

Specializing even further, let $\mathcal{A}$ be a uniform cover of $[n]$, and $0 < \alpha \leq 1 \leq c, d$. If $|\mathcal{F}_A| \leq \alpha c^{|A|}$ and $|A| \leq n/d$ for every $A \in \mathcal{A}$ then $|\mathcal{F}| \leq \alpha^d c^n$.

Proof. Although all the assertions are immediate, let us spell out an argument to justify the last one. If $\mathcal{A}$ is a uniform k-cover then

$$|\mathcal{F}|^k \leq \prod_{A \in \mathcal{A}} |\mathcal{F}_A| \leq \alpha^{|\mathcal{A}|} c^{\sum_{A \in \mathcal{A}} |A|} \leq \alpha^{kd} c^{kn}$$

since $\sum_{A \in \mathcal{A}} |A| = kn$ and so $|\mathcal{A}| \geq kd$. □

In the next section we shall present some applications of the results above; for further applications, see the Third Example Sheet. The final section is about some other aspects of projections.

2. Hereditary Properties of Hypergraphs

A *property* $\mathcal{P}$ of r-uniform hypergraphs is an infinite class of r-uniform hypergraphs closed under isomorphism. We call $\mathcal{P}$ *hereditary* if every induced subgraph of every member of $\mathcal{P}$ is also in $\mathcal{P}$. Let $\mathcal{P}^n$ be the set of hypergraphs in $\mathcal{P}$ with vertex set $[n]$. We are interested in the rate of growth of $|\mathcal{P}^n|$ with n. It is convenient to define the constant c_n by $|\mathcal{P}^n| = 2^{c_n\binom{n}{r}}$. This constant c_n is the logarithmic density of $\mathcal{P}^n$ in the set of all r-graphs on $[n]$; in particular, if *every* r-uniform hypergraph on $[n]$ has property $\mathcal{P}$ then $|\mathcal{P}^n| = 2^{\binom{n}{r}}$ so $c_n = 1$. Note that eventually $0 < c_n < 1$ unless $\mathcal{P}$ is a *trivial* class, consisting of the hypergraphs with no edges only, or the complete hypergraphs only, or of all the hypergraphs. In 1994, Scheinerman and Zito asked whether the sequence (c_n) was convergent for every hereditary property. Unbeknown to Scheinerman and Zito, this had been proved by Alekseev in 1993. In answer to a question of Scheinerman and Zito, in 1995, Bollobás and Thomason made use of Corollary 9 to conclude that the sequence (c_n) is not only convergent, but also monotone decreasing.

Theorem 10. *Let $\mathcal{P}$ be a hereditary property of r-uniform hypergraphs and let $|\mathcal{P}^n| = 2^{c_n\binom{n}{r}}$. Then $c_{n-1} \geq c_n$ for $n \geq r+1$. In particular $\lim_{n\to\infty} c_n$ exists.*

Proof. Let $n \geq r+1$, and recall that $[n]^{(r)}$ denotes the set of r-subsets of $[n]$. An r-uniform hypergraph on $[n]$ is naturally identified with its edge set, a subset of $[n]^{(r)}$. Then $\mathcal{P}^n$ becomes a set system on $[n]^{(r)}$. Let $A(i)$ be the set of r-subsets of $[n] \setminus \{i\}$. Then $\mathcal{P}^n_{A(i)}$, the projection of the set system $\mathcal{P}^n$ onto $A(i)$, is the set of hypergraphs induced by the hypergraphs in $\mathcal{P}^n$ on the vertex set $[n]\setminus\{i\}$. Since $\mathcal{P}$ is hereditary, and $\mathcal{P}^n_{A(i)}$ consists of r-graphs with property $\mathcal{P}$ on an $(n-1)$-element set, $|\mathcal{P}^n_{A(i)}| \leq |\mathcal{P}^{n-1}|$ for every such $A(i)$.

Now the sets $A(i)$, $1 \leq i \leq n$, form a uniform cover of $[n]^{(r)}$ (in fact, $(n-r)$-uniform cover). Also $|A(i)| = \binom{n-1}{r}$ and $|\mathcal{P}^n_{A(i)}| \leq |\mathcal{P}^{n-1}| = 2^{c_{n-1}|A(i)|}$. By Corollary 9, $|\mathcal{P}^n| \leq 2^{c_{n-1}|[n]^{(r)}|} = 2^{c_{n-1}\binom{n}{r}}$, as required. □

A direct application of BTBT to prove Theorem 10 is just as easy. Indeed, identifying an r-uniform hypergraph H on $[n]$ with its edge

set, H corresponds to a point x_H of the hypercube $\{0,1\}^{[n]^{(r)}} \subset \mathbb{R}^{[n]^{(r)}}$. Replacing H by the unit cube with centre x_H, and $\mathcal{P}^n$ by the union K^n of the appropriate unit cubes, the body K^n in $\mathbb{R}^{[n]^{(r)}}$ has volume $|\mathcal{P}^n| = 2^{c_n\binom{n}{r}}$. Since a subgraph of a graph in $\mathcal{P}^n$ induced by $n-1$ vertices is in $\mathcal{P}^{n-1}$, the projection of K^n into the subspace spanned by the standard vectors corresponding to the set of r-subsets in $A(i)$ has volume at most $2^{c_{n-1}\binom{n-1}{r}}$. An application of BTBT to the uniform cover of $[n]^{(r)}$ by the sets $A(i)$ tells us that $c_n \leq c_{n-1}$, as claimed.

3. The Trace of a Set System

Given a set system $\mathcal{F} \subset \mathcal{P}(n)$, its *trace* on a set $S \subset [n]$ (also called the *restriction* of $\mathcal{F}$ to S) is

$$\mathcal{F} \cap S = \mathcal{F}|S = \{F \cap S : \ F \in \mathcal{F}\}.$$

The notation $\mathcal{F}|S$ used for the restriction of $\mathcal{F}$ to S is somewhat clumsy when it comes to taking cardinalities and we have to write $|\mathcal{F}|S|$: this if why we prefer the notation $\mathcal{F} \cap S$.

As an example, note that if $\mathcal{E}$ consists of the edges of a graph with vertex set $[n]$, with each edge viewed as a 2-element subset of $[n]$, then for a set $S \subset [n]$ the trace $\mathcal{E} \cap S$ consists of all edges in S, together with the vertices in S with a neighbour not in S, and the empty set if there is an edge not incident with any vertex of S.

We say that $\mathcal{F}$ *shatters* S if $\mathcal{F} \cap S = \mathcal{P}(S)$, i.e. if for every subset A of S (including S and the empty set) there is a set $F \in \mathcal{F}$ with $A = F \cap S$. The *trace number* of a set system $\mathcal{F}$ is

$$\mathrm{tr}(\mathcal{F}) = \max\{|S| : \ S \text{ is shattered by } \mathcal{F}\}.$$

The main aim of this very short section is to present the basic result about traces of set systems, the *Sauer-Shelah-Perles lemma*, giving us an optimal lower bound on $\mathrm{tr}(\mathcal{F})$ in terms of the cardinality of $\mathcal{F} \subset \mathcal{P}(n)$. This will be an instant consequence of the next lemma stating that so-called 'down-compression' do not increase the size of the trace. All this is very similar to our proofs of various isoperimetric inequalities, only it is even simpler.

The *down-compression* at $i \in [n]$ is defined as follows. For $F \in \mathcal{P}(n)$,

$$D_i(F) = \begin{cases} F \setminus \{i\} & \text{if } \ i \in F, \\ F & \text{otherwise.} \end{cases}$$

Also, for $\mathcal{F} \subset \mathcal{P}(n)$,

$$D_i(\mathcal{F}) = \{D_i(F) : \ F \in \mathcal{F}\} \cup \{F \in \mathcal{F} : \ D_i(F) \in \mathcal{F}\}.$$

Equivalently, the sets in $\mathcal{P}(n)$ are partitioned into pairs $(E, E \cup \{i\})$, with $E \subset [n] \setminus \{i\}$, and then $D_i(\mathcal{F})$ is defined to contain exactly as many members of a pair as $\mathcal{F}$: the only stipulation is that if $\mathcal{F}$ contains exactly one of E and $E \cup \{i\}$ then $D_i(\mathcal{F})$ contains precisely E, rather than $E \cup \{i\}$. By construction, a down-compression does not change the cardinality of a family: $|\mathcal{F}| = |D_i(\mathcal{F})|$.

Lemma 11. *Let $\mathcal{F} \subset \mathcal{P}(n)$, $\emptyset \neq S \subset [n]$ and $1 \leq i \leq n$. Then $|D_i(\mathcal{F}) \cap S| \leq |\mathcal{F} \cap S|$.*

Proof. Set $\mathcal{G} = \mathcal{F} \cap S$ and $\mathcal{G}' = D_i(\mathcal{F}) \cap S$. If $i \notin S$ then $\mathcal{G} = \mathcal{G}'$, so we may assume that $i \in S$.

Our task is to show that if $A \subset S \setminus \{i\}$ then

$$|\mathcal{G}' \cap \{A, A \cup \{i\}\}| \leq |\mathcal{G} \cap \{A, A \cup \{i\}\}|. \tag{17}$$

Suppose $A \cup \{i\} \in \mathcal{G}'$ and let $F \in D_i(\mathcal{F})$ be such that $F \cap S = A \cup \{i\}$. Then F and $F \setminus \{i\}$ both belong to $D_i(\mathcal{F})$ so they have to belong to $\mathcal{F}$ as well. It follows that $|\mathcal{G} \cap \{A, A \cup \{i\}\}| = 2$, which implies (17).

Hence, in proving (17), we may assume that $A \in \mathcal{G}'$ and $A \cup \{i\} \notin \mathcal{G}'$. Then $F \cap S = A$ for some $F \in D_i(\mathcal{F})$, so $\mathcal{F}$ contains at least one of F and $F \cup \{i\}$. Therefore $|\mathcal{G} \cap \{A, A \cup \{i\}\}| \geq 1$, completing our proof. □

As usual, repeated down-compressions result in a family with pleasant properties. Call a family $\mathcal{D} \subset \mathcal{D} \subset \mathcal{P}(n)$ *monotone decreasing*, *down-compressed* or simply a *down-family* if $D_i(\mathcal{F}) = \mathcal{F}$ for every i, $i = 1, \ldots, n$. Equivalently, $\mathcal{D}$ is a down-family if $D \in \mathcal{D}$ whenever $D \subset E \in \mathcal{D}$.

Corollary 12. *For $\mathcal{F} \subset \mathcal{P}(n)$ there is a down-family $\mathcal{D}$ such that $|\mathcal{D}| = |\mathcal{F}|$ and*

$$|\mathcal{D} \cap S| \leq |\mathcal{F} \cap S|$$

for every $S \subset [n]$.

Proof. By now, a proof of this kind is dime a dozen for us. (Not that it ever was more than a triviality.) Indeed, let $\mathcal{D} \subset \mathcal{P}(n)$ be such that $|\mathcal{D}| = |\mathcal{F}|$, $|\mathcal{D} \cap S| \leq |\mathcal{F} \cap S|$ for every $S \subset [n]$, and $\sum_{D \in \mathcal{D}} |D|$ is minimal. If $D_i(\mathcal{D}) \neq \mathcal{D}$ for some i then by Lemma 11 the family $D_i(\mathcal{D})$ has the required properties, and

$$\sum_{D \in D_i(\mathcal{D})} |D| < \sum_{D \in \mathcal{D}} |D|,$$

contradicting the minimality of $\mathcal{D}$. Hence $\mathcal{D}$ is a down-family with the required properties. □

After this preparation, here is the main (and terribly easy) result of this section, the Sauer–Shelah–Perles lemma, which we state as a theorem.

Theorem 13. *Let $\mathcal{F} \subset \mathcal{P}(n)$, $1 \leq k \leq n$, and*

$$|\mathcal{F}| > \sum_{i=0}^{k-1} \binom{n}{i}. \tag{18}$$

Then $\mathcal{F}$ shatters a k-subset of $[n]$, i.e. the trace number of $\mathcal{F}$ is at least k.

Proof. By Corollary 12 we may assume that $\mathcal{F}$ is a down-family. Inequality (18) tells us that $\mathcal{F}$ has to contain a set S with at least k elements. As $\mathcal{F}$ is a down-family, it contains every subset of S, i.e. $\mathcal{P}(S) \subset \mathcal{F}$. This means that $\mathcal{F}$ shatters S, and every subset of S. □

Theorem 13 was proved in 1972 in reply to a question Erdős posed in 1967 and 1970. Given a family $\mathcal{F} \subset \mathcal{P}(Z)$, write $f_{\mathcal{F}}(n)$ for the maximal cardinality of the trace of $\mathcal{F}$ on an n-set. Here Z and $\mathcal{F}$ are taken to be infinite. Erdős wondered about the growth of $f_{\mathcal{F}}(n)$. Could it grow faster than any polynomial of n but slower than an exponential function of n? We conclude this section with a resounding (and very simple) answer to this question.

Corollary 14. *Let $\mathcal{F} \subset \mathcal{P}(Z)$ be infinite. Then either $f_{\mathcal{F}}(n) = 2^n$ for every $n \geq 1$ or there is an integer k such that $f_{\mathcal{F}}(n) \leq n^k$ for every n.*

Proof. If for every $k \geq 3$ there is a natural number n_k such that

$$|\mathcal{F} \cap [n_k]| > n_k^{k-1}$$

then $f_{\mathcal{F}}(k) = 2^k$. □

A slightly less precise variant of the Sauer-Shelah-Perles lemma was proved simultaneously and independently by Vapnik and Červonenkis, with other applications in mind. In particular, they used the result to introduce what is now called the *VC-dimension* of a set system, and we have called its trace number. The concept of VC-dimension has turned out to be very useful discrete and computational geometry, statistical learning theory, and other areas.