the coordinate functions $(x_1, \ldots, x_m) \mapsto x_i$. Show that the multilinear monomials $\prod_{i \in I} x_i$, $I \subset [1, m]$ constitute a basis of $F^{\{0,1\}^m}$, viewed as a vector space over F. (Hint: to establish linear independence, use Theorem 9.2.) In the case $F = \mathbf{C}$ or $F = \mathbf{R}$, show that this result also follows from (4.4) applied to the group $\mathbf{Z}_2^m$.

9.2 Restricted sum sets

We now apply the combinatorial Nullstellensatz to obtain lower bounds for sum sets, and restricted sum sets. We begin with a general lemma which gives a criterion for when such lower bounds on restricted sum sets can be attained.

Lemma 9.3 *[11] Let F be a field, let $n \geq 1$, and let $h \in F[t_1, \ldots, t_n]$ be a polynomial. Let $K \geq 0$, and let $A_1, \ldots, A_n$ be additive sets in F_p such that $\sum_{i=1}^n |A_i| = K + n + \deg(h)$. Suppose also that the polynomial $(t_1 + \cdots + t_n)^K h(t_1, \ldots, t_n)$ contains a non-zero coefficient at $t_1^{|A_1|-1} \cdots t_n^{|A_n|-1}$. Then*

$$|\{a_1 + \cdots + a_n : a_i \in A_i \text{ for all } 1 \leq i \leq n; h(a_1, \ldots, a_n) \neq 0\}| \geq K + 1. \quad (9.1)$$

Proof Suppose for contradiction that (9.1) failed; then one can find a set $B \subseteq F$ of cardinality $|B| = K$ which contains the set in (9.1). Let $P \in F[t_1, \ldots, t_n]$ be the polynomial

$$P(t_1, \ldots, t_n) := h(t_1, \ldots, t_n) \prod_{b \in B} (t_1 + \cdots + t_n - b).$$

Observe that $\deg(P) = K + \deg(h)$. On the other hand, by construction of B we see that P vanishes on contains $A_1 \times \cdots \times A_n$. But this contradicts the combinatorial Nullstellensatz. □

This powerful lemma allows one to reduce the task of establishing lower bounds on restricted sum sets to that of verifying that a single coefficient of an explicit polynomial is non-zero in the field F. As two quick applications of this lemma we reprove the Cauchy–Davenport inequality (Theorem 5.4) and then derive a variant, first conjectured by Erdős and Heilbronn, concerning the restricted sums $A \hat{+} B := \{a + b : a \in A, b \in B, a \neq b\}$.

Theorem 9.4 (Cauchy–Davenport inequality, again) *[47], [68] Let $F = F_p$ be a finite field of prime order. If A, B are two additive sets in F, then*

$$|A + B| \geq \min(|A| + |B| - 1, p).$$

We shall give a third proof of this theorem via the Fourier transform in Section 9.8.

Proof The claim is trivial when $|A| + |B| > p$ (see Exercise 2.1.6) so let us take $|A| + |B| \leq p$. We apply Lemma 9.3 with $n = 2$, $(A_1, A_2) = (A, B)$, $h \equiv 1$, and $K := |A| + |B| - 2$; we will be done as soon as we verify that $(t_1 + t_2)^K$ has a non-zero coefficient at $t_1^{|A|-1} t_2^{|B|-1}$ in F_p. But this coefficient is simply $\binom{K}{|A|-1} \bmod p$, which is non-zero since $K < p$. □

As a special case of the Cauchy–Davenport inequality we see that $|A + A| \geq \min(2|A| - 1, p)$ for any additive set A in F_p. The analogous result for restricted sums $A \hat{+} A$ took much longer to prove. It is easy to see that $|A \hat{+} A| = p$ when $2|A| - 3 \geq p$ (Exercise 9.2.1). In 1964, Erdős and Heilbronn (see [89]) conjectured that $|A \hat{+} A| \geq \min(2|A| - 3, p)$; this bound is easily seen to be optimal (Exercise 9.2.3). This innocuous-seeming variant of the Cauchy–Davenport inequality resisted attempts at solution for about thirty years; the e-transform methods in Section 5.1 do not appear to be able to prove the Erdős–Heilbronn conjecture. The conjecture was finally solved in 1994 by da Silva and Hamidoune [66] who confirmed it using a general result concerning Grassman spaces. We now give a short proof due to Alon, Nathanson, and Ruzsa [11] using the combinatorial Nullstellensatz, which demonstrates the power and simplicity of this method. Indeed one can prove slightly more:

Theorem 9.5 *[11] Let $F = F_p$ for some prime p, and let let A, B be two additive sets in F. Then*

$$|A \hat{+} B| \geq \min(|A| + |B| - 3, p).$$

Furthermore, if $|A| \neq |B|$, then we can improve the above bound to

$$|A \hat{+} B| \geq \min(|A| + |B| - 2, p).$$

Proof The case $|A| + |B| - 2 \geq p$ is easy (Exercise 9.2.1), so suppose $|A| + |B| - 2 < p$. The cases $|A| = 1$ or $|B| = 1$ are also trivial (Exercise 9.2.2), so assume $|A|, |B| \geq 2$. By deleting one element from A or B if necessary it suffices to obtain the latter bound in the case $|A| \neq |B|$.

We now apply Lemma 9.3 with $n = 2$, $(A_1, A_2) = (A, B)$, $h(t_1, t_2) := t_1 - t_2$, and $K = |A| + |B| - 3$. We will be done as soon as we verify that $(t_1 - t_2) \times (t_1 + t_2)^K$ contains a non-zero coefficient at $t_1^{|A|-1} t_2^{|B|-1}$. But this quantity can be computed as

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

Since $|A| + |B| - 2 < p$, we see that this quantity is non-zero, and we are done. □

Clearly one can obtain further applications of Lemma 9.3; see for instance Exercise 9.2.4. But when one considers restricted sums of multiple sets one begins to need to study the coefficients of increasingly complicated polynomials, frequently involving such expressions as Vandermonde determinants. We shall therefore turn our attention next to the study of such polynomials and their coefficients. Our computations here shall be completely abstract, valid for indeterminates $x_1, \ldots, x_n$ taking values in any field F.

Definition 9.6 (Vandermonde determinant) If $n \geq 1$ and $x_1, \ldots, x_n$ are indeterminates, we define the *Vandermonde determinant* to be the expression

$$\Delta_n(x_1, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_j - x_i) = (-1)^{\binom{n}{2}} \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

It is easy to verify the symmetries

$$\begin{aligned} \Delta_n(x_1 + y, \ldots, x_n + y) &= \Delta_n(x_1, \ldots, x_n); \\ \Delta_n(\lambda x_1, \ldots, \lambda x_n) &= \lambda^{\binom{n}{2}} \Delta_n(x_1, \ldots, x_n); \\ \Delta_n(\pi(x)) &= \mathrm{sgn}(\pi) \Delta_n(x) \end{aligned} \tag{9.2}$$

for any variables λ, y and $x = (x_1, \ldots, x_n)$, and any permutation $\pi \in S_n$. In fact this effectively determines Δ_n up to constants, see Exercise 9.2.5. The quantity $\Delta_n(1, \ldots, n) = \prod_{i=1}^{n} (i-1)!$ is sometimes called the *superfactorial* of n.

The following well-known fact will be left as an exercise:

Lemma 9.7 *Let $n \geq 1$, and for each $1 \leq i \leq n$ let $P_i(x)$ be a monic polynomial of degree $i - 1$. Then for any variables $x_1, \ldots, x_n$ we have the identity*

$$\begin{aligned} \det(P_i(x_j))_{1 \leq i,j \leq n} &= \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} P_{\pi(i)}(x_i) \\ &= \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} P_i\big(x_{\pi(i)}\big) \\ &= \Delta_n(x_1, \ldots, x_n). \end{aligned}$$

In particular we have

$$\Delta_n(x_1, \ldots, x_n) = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} x_i^{\pi(i)-1}. \tag{9.3}$$

The formula (9.3) computes the coefficients of $\Delta_n(x_1, \ldots, x_n)$ exactly. Multiplying it with the multinomial formula

$$(x_1 + \cdots + x_n)^K = \sum_{c_1, \cdots, c_n \geq 0 : c_1 + \ldots + c_n = K} \frac{K!}{c_1! \cdots c_n!} \prod_{i=1}^{n} x_i^{c_i}$$

we obtain the formula

$$(x_1 + \cdots + x_n)^K \Delta_n\big(x_1^m, \ldots, x_n^m\big) = \sum_{c_1,\ldots,c_n \geq 0 : c_1+\cdots+c_n = K + m\binom{n}{2}} \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \frac{K!}{\prod_{i=1}^n (c_i - \pi(i)m + m)!} \prod_{i=1}^n x_i^{c_i} \quad (9.4)$$

where we adopt the convention that $1/k! = 0$ when k is a negative integer.

In certain cases, the expression on the right-hand side of (9.4) can be simplified. For instance, in the $m = 1$ case we have

Lemma 9.8 *Let $n, K \geq 0$. Then we have*

$$(x_1 + \cdots + x_n)^K \Delta_n(x_1, \ldots, x_n) = \sum_{c_1,\ldots,c_n \geq 0 : c_1+\cdots+c_n = K + \binom{n}{2}} \frac{K!}{c_1! \cdots c_n!} \Delta_n(c_1, \ldots, c_n) x_1^{c_1} \cdots x_n^{c_n}. \quad (9.5)$$

Proof By (9.4), it suffices to establish the identity

$$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \frac{K!}{\prod_{i=1}^n (c_i - \pi(i) + 1)!} = \frac{K!}{c_1! \cdots c_n!} \Delta_n(c_1, \ldots, c_n).$$

If we introduce the *falling factorial*

$$(x)_n := x(x-1)\cdots(x-n+1), \quad (9.6)$$

then from Lemma 9.7 we have

$$\Delta_n(c_1, \ldots, c_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^n (c_i)_{\pi(i)-1} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^n \frac{c_i!}{(c_i - \pi(i) + 1)!}$$

and the claim follows. □

This Lemma already gives a generalization of the Erdős–Heilbronn conjecture; see Exercises 9.2.9 and 9.2.10.

In a similar spirit we have

Lemma 9.9 *Let $n, m, K, k \geq 0$ be such that*

$$(k-1) + \cdots + (k-n) = K + m\binom{n}{2}.$$

Then the coefficient of $x_1^{k-n} \cdots x_n^{k-1}$ in $(x_1 + \cdots + x_n)^K \Delta_n(x_1^m, \ldots, x_n^m)$ is

$$\frac{K!}{\prod_{i=1}^n (k - 1 - (i-1)m)!} m^{\binom{n}{2}} \Delta_n(1, \ldots, n).$$

Proof By (9.4), it suffices to establish the identity

$$\sum_{\pi\in S_n} \mathrm{sgn}(\pi) \frac{K!}{\prod_{i=1}^n (k-n-1+i-\pi(i)m+m)!}$$
$$= \frac{K!}{\prod_{i=1}^n (k-1-(i-1)m)!} m^{\binom{n}{2}} \Delta_n(1,\dots,n).$$

Relabeling i by $\pi(i)$ and using the fact that $\mathrm{sgn}(\pi) = \mathrm{sgn}(\pi^{-1})$, the left-hand side can be rewritten as

$$\sum_{\pi\in S_n} \mathrm{sgn}(\pi) \frac{K!}{\prod_{i=1}^n (k-n-1+\pi(i)-(i-1)m)!}$$

which can be rewritten further using the falling factorial (9.6) as

$$\frac{K!}{\prod_{i=1}^n (k-1-(i-1)m)!} \sum_{\pi\in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^n (k-1-(i-1)m)_{n-\pi(i)}.$$

Writing $n-\pi(i) = \alpha(i)-1$ and noting that $\mathrm{sgn}(\pi) = (-1)^{\binom{n}{2}}\mathrm{sgn}(\alpha)$, we rewrite this further as

$$\frac{K!}{\prod_{i=1}^n (k-1-(i-1)m)!} (-1)^{\binom{n}{2}} \sum_{\alpha\in S_n} \mathrm{sgn}(\alpha) \prod_{i=1}^n (k-1-(i-1)m)_{\alpha(i)-1}$$

which by Lemma 9.7 becomes

$$\frac{K!}{\prod_{i=1}^n (k-1-(i-1)m)!} (-1)^{\binom{n}{2}} \Delta_n(k-1, k-1-m, \dots, k-1-(n-1)m).$$

The claim now follows from (9.2). □

As a consequence of this computation, we have the following additive combinatorial consequence concerning multiple restricted addition where the restrictions are of the form $P_i(a_i) \neq P_j(a_j)$ for polynomials P_i, P_j.

Theorem 9.10 *[234] Let k, m, n be positive integers such that the quantity $K := (k-1)n - (m+1)\binom{n}{2}$ is non-negative. Let F be a field whose characteristic is either zero or is a prime number greater than* $\max(K, m, n-1)$. *Let $A_1, \dots, A_n$ be subsets of F for which $|A_i| \geq k-n+i$ for all $1 \leq i \leq n$. Let $P_1, \dots, P_n \in F[t]$ be monic polynomials of degree m. Then*

$$|\{a_1 + \cdots + a_n | a_i \in A_i, P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geq K+1.$$

Proof Without loss of generality, we can assume that $|A_i| = k-n+i = k_i$. Let $f \in F[t_1, \dots, t_n]$ be the polynomial

$$f(t_1, \dots, t_n) := \prod_{1\leq i<j\leq n} (P_j(t_j) - P_i(t_i)).$$

Since $k_i = k - n + i$ we have

$$\sum_{i=1}^{n}(k_i - 1) = (k-1)n - \binom{n}{2} = K + \deg(f).$$

Thus, the coefficient of $t_1^{k_1-1}\cdots t_n^{k_n-1}$ in the polynomial $(t_1 + \cdots + t_n)^K \times f(t_1, \ldots, t_n)$ is the same as the coefficient of $t_1^{k-n}\cdots t_n^{k-1}$ in

$$(t_1 + \cdots + t_n)^K \prod_{1\le i<j\le n}\left(t_j^m - t_i^m\right) = (t_1 + \cdots + t_n)^K \Delta_n\left(t_1^m, \ldots, t_n^m\right).$$

Applying Lemma 9.3 and Lemma 9.9, we reduce to showing that

$$\frac{K!}{\prod_{i=1}^{n}(k-1-(i-1)m)!} m^{\binom{n}{2}} \Delta_n(1, \ldots, n)\cdot 1 \neq 0.$$

But since the characteristic of F is either 0 or exceeds $\max(K, n-1, m)$, the claim is easily verified. □

Next we consider what happens if we raise the factors $(x_j - x_i)$ in $\Delta_n(x_1, \ldots, x_n)$ to arbitrary powers. A useful result in this regard is

Theorem 9.11 (Dyson's conjecture) *Let $a_1, \ldots, a_n$ be positive integers. The coefficient of $\prod_{i=1}^{n} x_i^{(n-1)a_i}$ in*

$$\prod_{i,j\in[1,n]:i\neq j}(x_j - x_i)^{a_j}$$

is

$$\frac{(a_1 + \cdots + a_n)!}{a_1!\cdots a_n!}.$$

This result was conjectured by Dyson [74] based on a problem in particle physics. It was verified by Gunson [165] and independently by Wilson [383] in 1962. We present a short and elegant proof due to Good [135].

Proof Let $x = (x_1, \ldots, x_n)$, $a = (a_1, \ldots, a_n)$ and

$$F(x, a) = \prod_{i,j\in[1,n]:i\neq j}\left(1 - \frac{x_i}{x_j}\right)^{a_j},$$

and let $F_0(a)$ denote the constant term in $F(x, a)$. It will suffice to prove that $F_0(a) = \frac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}$ whenever the a_i are non-negative integers.

We induce on n. The claim is trivial when $n = 0$, so suppose $n \geq 1$ and the claim has already been proven for $n-1$. We can then assume that none of the a_i are zero since we can simply eliminate that variable (noting that in that case the x_i variable only appears with a positive exponent) and apply the induction hypothesis. Thus $a_i \geq 1$ for all $i \in [1, n]$.

Let $e_1, \ldots, e_n$ be the standard basis vectors of $\mathbf{Z}^n$. It will suffice to prove the recursion

$$F_0(a) = \sum_{i=1}^{n} F_0(a - e_i)$$

whenever $a_i \geq 1$, since the claim then follows from the multinomial Pascal identity and an easy induction on $\sum_{i=1}^{n} a_i$.

By applying Lagrange's interpolation formula (Exercise 9.2.8) to the function $f(x) \equiv 1$ we have the identity

$$1 = \sum_{j=1}^{n} \prod_{i \in [1,n]: i \neq j} (x_j - x_i)^{-1}(y - x_i)$$

for all y. Setting $y = 0$ we have

$$1 = \sum_{j=1}^{n} \prod_{i \in [1,n]: i \neq j} \left(1 - \frac{x_i}{x_j}\right)^{-1}. \tag{9.7}$$

By multiplying both sides of (9.7) with $F(x, a)$, we see that if $a_j > 0$ for all $1 \leq j \leq n$ then we have the recursion

$$F(x, a) = \sum_{j=1}^{n} F(x, a - e_j)$$

and the claim follows by extracting the constant coefficient. □

As one particular consequence of Theorem 9.11, we see that the coefficient of $\prod_{i=1}^{n} x_i^{(n-1)m}$ in $\Delta_n(x_1, \ldots, x_n)^{2m}$ is $(nm)!/(m!)^n$. Using this fact and some additional arguments, Hou and Sun [186] proved the following generalization.

Lemma 9.12 *Let $n, m, k \geq 0$, and let $s := k + m(n-1)$. Then the coefficient of $x_1^s \cdots x_n^s$ in $(x_1 + \cdots + x_n)^{km} \Delta_n(x_1, \ldots, x_n)^{2m}$ is*

$$(-1)^{m\binom{n}{2}} \frac{(km!)}{(m!)^n} \prod_{j=1}^{n} \frac{(jm)!}{(s - (j-1)m)!}.$$

The proof of this theorem is somewhat technical and we refer the reader to [186] for details. As an additive combinatorial consequence, we can control restricted sum sets where the differences $a_i - a_j$ are required to avoid certain specified sets.

Theorem 9.13 *[186] Let k, m, n be positive integers and F be a field of characteristic p where p is zero or p is a prime satisfying*

$$p \geq n \max\{m, n + m - mk - 1\}.$$

Let $A_1, \ldots, A_k$ be subsets of F with cardinality at least n. For any $i, j \in \{1, \ldots, k\}, i \neq j$ let S_{ij} be a subset of F with cardinality at most m. Then the set

$$C := \{a_1 + \cdots + a_k | a_i \in A_i, a_i - a_j \notin S_{ij} \text{ if } i \neq j\}$$

has cardinality at least

$$|C| \geq (n + m - mk - 1)k + 1.$$

Proof We first need the following variant of Theorem 9.3, whose proof we leave to Exercise 9.2.11.

Lemma 9.14 *Let $A_1, \ldots, A_k$ be finite subsets of a field F. Assume that $|A_i| \geq n_i$. Let $\lambda, \mu \in F[t_1, \ldots, t_k]$ be such that* $\deg(\mu) > 0$. *Define*

$$C := \{\mu(a_1, \ldots, a_k) | a_i \in A_i, \lambda(a_1, \ldots, a_k) \neq 0\}.$$

Then there is no polynomial $\omega \in F[t_1, \ldots, t_n]$ such that the polynomial $\lambda\omega\mu^{|C|}$ has degree $\sum_{i=1}^{k}(n_i - 1)$ and the coefficient of $x_1^{n_1-1} \cdots x_k^{n_k-1}$ in this polynomial is non-zero.

To prove Theorem 9.13, we can assume, without loss of generality, that $|A_i| = n$ and $|S_{ij}| = m$ for all i, j. Let $l := n + m = mk - 1$. Assume, for contradiction, that $|C| < ln$. Let $\lambda, \mu, \omega \in F[t_1, \ldots, t_k]$ be the polynomials

$$\lambda(t_1, \ldots, t_k) := \prod_{1 \leq i \neq j \leq k} \prod_{c_{ij} \in S_{ij}} (t_i - t_j - c_{ij})$$

$$\mu(t_1, \ldots, t_k) := t_1 + \cdots + t_k,$$

$$\omega := \mu^{kl-|C|}.$$

The polynomial $\lambda\omega\mu^{|C|}$ has total degree $mk(k-1) + lk = k(n-1) = \sum_{i=1}^{k}(|A_i| - 1)$. Moreover, the coefficient of $t_1^{n-1} \cdots t_k^{n-1}$ in this polynomial is the same as that in

$$\prod_{1 \leq i < j \leq k} (t_i - t_j)^{2m} \mu^{kl} = \Delta_k(t_1, \ldots, t_k)^{2m}(t_1 + \cdots + t_k)^{kl}.$$

But this is non-zero thanks to Lemma 9.9 and the hypotheses on the characteristic p. This contradicts Lemma 9.14, completing the proof. □

Exercises

9.2.1 Let Z be any finite additive group of odd order, and let A, B be additive sets in Z. Show that if $|A| + |B| - 2 \geq |Z|$, then $A \hat{+} B = Z$. (Compare with Exercise 2.1.6.)

9.2.2 Verify Theorem 9.5 when $|A| = 1$ or $|B| = 1$.

9.2.3 Give examples to show that the bound $|A \hat{+} A| \geq \min(2|A| - 3, p)$ cannot be improved. What about the bound $|A \hat{+} B| \geq \min(|A| + |B| - 2, p)$ when $|A| \neq |B|$?

9.2.4 Let $F = F_p$ be a finite field of prime order, and let A, B be additive sets in F_p. Show that

$$|\{a + b | a \in A, b \in B, ab \neq 1\}| \geq \min(|A| + |B| - 3, p).$$

9.2.5 Verify the symmetries (9.2). Furthermore, show that if $P(x_1, \ldots, x_n)$ is any polynomial which obeys the same symmetries (9.2) as Δ_n, then P is a scalar multiple of Δ_n.

9.2.6 Prove Lemma 9.7. (Hint: one can use Gaussian elimination to reduce to the case $P_i(x) = x^{i-1}$. Then locate several linear factors of $V(x_1, \ldots, x_n)$ and use the factor theorem. Alternatively, use Exercise 9.2.5.)

9.2.7 Show that if $x_1, \ldots, x_n$ are integers, then $\Delta_n(x_1, \ldots, x_n)$ is a multiple of $\Delta_n(1, \ldots, n) = \prod_{i=1}^{n}(i-1)!$.

9.2.8 (Lagrange interpolation formula) Let F be a field, let $n \geq 0$, let $a_0, \ldots, a_n$ be $n+1$ distinct elements of F and let $b_0, \ldots, b_{n+1}$ be $n+1$ arbitrary elements of F. Show that there is exactly one polynomial $f \in F[t]$ with coefficients in F of degree at most n such that $f(a_i) = b_i$, and that this polynomial is given by

$$f(x) = \sum_{i=0}^{n} b_i \prod_{0 \leq j \neq i \leq n} (a_i - a_j)^{-1}(x - a_j).$$

9.2.9 [11] Let $F = F_p$ be a finite field of prime order, and let $A_1, \ldots, A_k$ be additive sets in F_p with $|A_1|, \ldots, |A_k|$ all distinct and $\sum_{i=1}^{k} |A_i| \leq p + \binom{k+1}{2} - 1$. Let B be the restricted sum set

$$B := \{a_1 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \text{ for all } 1 \leq i < j \leq k\}.$$

Using Theorem 9.3 and Lemma 9.8, establish the inequality $|B| \geq \{\sum_{i=1}^{k} |A_i| - \binom{k}{2} + 1, p\}$.

9.2.10 [66] (Generalized Erdős–Heilbronn conjecture) Let $F = F_p$ be a finite field of prime order, and let A be an additive set in F_p. Let $k \hat{} A := \{a_1 + \cdots + a_k : a_1, \ldots, a_k \in A, a_i \neq a_j \text{ for all } 1 \leq i < j \leq k\}$ be the set of k-fold sums of *distinct* elements of A. Show that $|k \hat{} A| \geq \min(p, k|A| - k^2 + 1)$. (Hint: use Exercise 9.2.9.)

9.2.11 Prove Lemma 9.14. (Hint: Apply the combinatorial Nullstellensatz to the polynomial $f := \lambda\omega \prod_{c \in C}(\mu - c)$.)