Combinatorics, Probability and Computing (1999) 8, 7–29. Printed in the United Kingdom

Combinatorial Nullstellensatz

NOGA ALON†

Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences,
Tel Aviv University, Tel Aviv, Israel
and
Institute for Advanced Study, Princeton, NJ 08540, USA
(e-mail: noga@math.tau.ac.il)

We present a general algebraic technique and discuss some of its numerous applications in combinatorial number theory, in graph theory and in combinatorics. These applications include results in additive number theory and in the study of graph colouring problems. Many of these are known results, to which we present unified proofs, and some results are new.

1. Introduction

Hilbert's Nullstellensatz (see, for instance, [60]) is the fundamental theorem that asserts that if F is an algebraically closed field, and $f, g_1, \ldots, g_m$ are polynomials in the ring of polynomials $F[x_1, \ldots, x_n]$, where f vanishes over all common zeros of $g_1, \ldots, g_m$, then there is an integer k and polynomials $h_1, \ldots, h_m$ in $F[x_1, \ldots, x_n]$ so that

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

In the special case $m = n$, where each g_i is a univariate polynomial of the form $\prod_{s \in S_i}(x_i - s)$, a stronger conclusion holds, as follows.

Theorem 1.1. *Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty subsets of F and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If f vanishes over all the common zeros of $g_1, \ldots, g_n$ (that is, if $f(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$), then there are polynomials $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ satisfying* $\deg(h_i) \leqslant \deg(f) - \deg(g_i)$ *so*

† Research supported in part by a grant from the Israel Science Foundation, by a Sloan Foundation grant No. 96-6-2, by an NEC Research Institute grant, and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

that

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

Moreover, if $f, g_1, \ldots g_n$ *lie in* $R[x_1, \ldots, x_n]$ *for some subring* R *of* F *then there are polynomials* $h_i \in R[x_1, \ldots, x_n]$ *as above.*

As a consequence of the above one can prove the following.

Theorem 1.2. *Let* F *be an arbitrary field, and let* $f = f(x_1, \ldots, x_n)$ *be a polynomial in* $F[x_1, \ldots, x_n]$. *Suppose the degree* $\deg(f)$ *of* f *is* $\sum_{i=1}^{n} t_i$, *where each* t_i *is a nonnegative integer, and suppose the coefficient of* $\prod_{i=1}^{n} x_i^{t_i}$ *in* f *is nonzero. Then, if* $S_1, \ldots, S_n$ *are subsets of* F *with* $|S_i| > t_i$, *there are* $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ *so that*

$$f(s_1, \ldots, s_n) \neq 0.$$

In this paper we prove these two theorems, which may be called *Combinatorial Nullstellensatz*, and describe several combinatorial applications of them. After presenting the (simple) proofs of the above theorems in Section 2, we show in Section 3 that the classical theorem of Chevalley and Warning on roots of systems of polynomials and the basic theorem of Cauchy and Davenport on the addition of residue classes follow as simple consequences. We proceed to describe additional applications in additive number theory and in graph theory and combinatorics in Sections 4, 5, 6, 7 and 8. Many of these applications are known results, proved here in a unified way, and some are new. There are several known results that assert that a combinatorial structure satisfies a certain combinatorial property if and only if an appropriate polynomial associated with it lies in a properly defined ideal. In Section 9 we apply our technique and obtain several new results of this form. Finally, Section 10 contains some concluding remarks and open problems.

2. The proofs of the two basic theorems

To prove Theorem 1.1 we need the following simple lemma proved, for example, in [13]. For the sake of completeness we include the short proof.

Lemma 2.1. *Let* $P = P(x_1, x_2, \ldots, x_n)$ *be a polynomial in* n *variables over an arbitrary field* F. *Suppose that the degree of* P *as a polynomial in* x_i *is at most* t_i *for* $1 \leqslant i \leqslant n$, *and let* $S_i \subset F$ *be a set of at least* $t_i + 1$ *distinct members of* F. *If* $P(x_1, x_2, \ldots, x_n) = 0$ *for all* n*-tuples* $(x_1, \ldots, x_n) \in S_1 \times S_2 \times \cdots \times S_n$, *then* $P \equiv 0$.

Proof. We apply induction on n. For $n = 1$, the lemma is simply the assertion that a nonzero polynomial of degree t_1 in one variable can have at most t_1 distinct zeros. Assuming that the lemma holds for $n - 1$, we prove it for n ($n \geqslant 2$). Given a polynomial $P = P(x_1, \ldots, x_n)$ and sets S_i satisfying the hypotheses of the lemma, let us write P as a polynomial in x_n, that is,

$$P = \sum_{i=0}^{t_n} P_i(x_1, \ldots, x_{n-1})x_n^i,$$

where each P_i is a polynomial with x_j-degree bounded by t_j. For each fixed $(n-1)$-tuple

$$(x_1, \ldots, x_{n-1}) \in S_1 \times S_2 \times \cdots \times S_{n-1},$$

the polynomial in x_n obtained from P by substituting the values of $x_1, \ldots, x_{n-1}$ vanishes for all $x_n \in S_n$, and is thus identically 0. Thus $P_i(x_1, \ldots, x_{n-1}) = 0$ for all $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$. Hence, by the induction hypothesis, $P_i \equiv 0$ for all i, implying that $P \equiv 0$. This completes the induction and the proof of the lemma. □

Proof of Theorem 1.1. Define $t_i = |S_i| - 1$ for all i. By assumption,

$$f(x_1, \ldots, x_n) = 0 \quad \text{for every } n\text{-tuple} \quad (x_1, \ldots, x_n) \in S_1 \times S_2 \times \cdots \times S_n. \tag{2.1}$$

For each i, $1 \leqslant i \leqslant n$, let

$$g_i(x_i) = \prod_{s \in S_i}(x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij}x_i^j.$$

Observe that,

$$\text{if } x_i \in S_i, \text{ then } g_i(x_i) = 0; \text{ that is, } x_i^{t_i+1} = \textstyle\sum_{j=0}^{t_i} g_{ij}x_i^j. \tag{2.2}$$

Let $\overline{f}$ be the polynomial obtained by writing f as a linear combination of monomials and replacing, repeatedly, each occurrence of $x_i^{f_i}$ ($1 \leqslant i \leqslant n$), where $f_i > t_i$, by a linear combination of smaller powers of x_i, using the relations (2.2). The resulting polynomial $\overline{f}$ is clearly of degree at most t_i in x_i, for each $1 \leqslant i \leqslant n$, and is obtained from f by subtracting from it products of the form $h_i g_i$, where the degree of each polynomial $h_i \in F[x_1, \ldots, x_n]$ does not exceed $\deg(f) - \deg(g_i)$ (and where the coefficients of each h_i are in the smallest ring containing all coefficients of f and $g_1, \ldots, g_n$). Moreover, $\overline{f}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, for all $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$, since the relations (2.2) hold for these values of $x_1, \ldots, x_n$. Therefore, by (2.1), $\overline{f}(x_1, \ldots, x_n) = 0$ for every n-tuple $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$ and hence, by Lemma 2.1, $\overline{f} \equiv 0$. This implies that $f = \sum_{i=1}^n h_i g_i$, and completes the proof. □

Proof of Theorem 1.2. Clearly we may assume that $|S_i| = t_i + 1$ for all i. Suppose the result is false, and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. By Theorem 1.1 there are polynomials $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ satisfying $\deg(h_j) \leqslant \sum_{i=1}^n t_i - \deg(g_j)$ so that

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

By assumption, the coefficient of $\prod_{i=1}^n x_i^{t_i}$ in the left-hand side is nonzero, and hence so is the coefficient of this monomial in the right-hand side. However, the degree of $h_i g_i = h_i \prod_{s \in S_i}(x_i - s)$ is at most $\deg(f)$, and if there are any monomials of degree $\deg(f)$ in it they are divisible by $x_i^{t_i+1}$. It follows that the coefficient of $\prod_{i=1}^n x_i^{t_i}$ in the right-hand side is zero, and this contradiction completes the proof. □

3. Two classical applications

The following theorem, conjectured by Artin in 1934, was proved by Chevalley in 1935 and extended by Warning in 1935. Here we present a very short proof using our Theorem 1.2 above. For simplicity, we restrict ourselves to the case of finite prime fields, though the proof easily extends to arbitrary finite fields.

Theorem 3.1 (e.g., [53]). *Let p be a prime, and let*

$$P_1 = P_1(x_1, \dots, x_n),\ P_2 = P_2(x_1, \dots, x_n), \dots,\ P_m = P_m(x_1, \dots, x_n)$$

be m polynomials in the ring $Z_p[x_1, \dots, x_n]$. If $n > \sum_{i=1}^{m} \deg(P_i)$ and the polynomials P_i have a common zero $(c_1, \dots, c_n)$, then they have another common zero.

Proof. Suppose this is false, and define

$$f = f(x_1, \dots, x_n) = \prod_{i=1}^{m} (1 - P_i(x_1, \dots, x_n)^{p-1}) - \delta \prod_{j=1}^{n} \prod_{c \in Z_p, c \neq c_j} (x_j - c),$$

where δ is chosen so that

$$f(c_1, \dots, c_n) = 0. \tag{3.1}$$

Note that this determines the value of δ, and this value is nonzero. Note also that

$$f(s_1, \dots, s_n) = 0 \tag{3.2}$$

for all $s_i \in Z_p$. Indeed, this is certainly true, by (3.1), if $(s_1, \dots, s_n) = (c_1, \dots, c_n)$. For other values of $(s_1, \dots, s_n)$, there is, by assumption, a polynomial P_j that does not vanish on $(s_1, \dots, s_n)$, implying that $1 - P_j(s_1, \dots, s_n)^{p-1} = 0$. Similarly, since $s_i \neq c_i$ for some i, the product $\prod_{c \in Z_p, c \neq c_i} (s_i - c)$ is zero and hence so is the value of $f(s_1, \dots, s_n)$.

Define $t_i = p - 1$ for all i and note that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is $-\delta \neq 0$, since the total degree of

$$\prod_{i=1}^{m} (1 - P_i(x_1, \dots, x_n)^{p-1})$$

is $(p-1) \sum_{i=1}^{m} \deg(P_i) < (p-1)n$. Therefore, by Theorem 1.2 with $S_i = Z_p$ for all i, we conclude that there are $s_1, \dots, s_n \in Z_p$ for which $f(s_1, \dots, s_n) \neq 0$, contradicting (3.2) and completing the proof. □

The Cauchy–Davenport theorem, which has numerous applications in additive number theory, is the following.

Theorem 3.2 ([21]). *If p is a prime, and A, B are two nonempty subsets of Z_p, then*

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}.$$

Cauchy proved this theorem in 1813, and applied it to give a new proof to a lemma of Lagrange in his well-known 1770 paper that shows that any integer is a sum of four squares. Davenport formulated the theorem as a discrete analogue of a conjecture of Khintchine (which was proved a few years later by H. Mann) about the Schnirelman density of the sum of two sequences of integers. There are numerous extensions of this result: see, for instance, [46]. The proofs of Theorem 3.2 given by Cauchy and Davenport are based on the same combinatorial idea, and apply induction on $|B|$. A different, algebraic, proof has recently been found by the authors of [10] and [11], and its main advantage is that it extends easily and gives several related results. As shown below, this proof can be described as a simple application of Theorem 1.2.

Proof of Theorem 3.2. If $|A|+|B| > p$ the result is trivial, since in this case for every $g \in Z_p$ the two sets A and $g - B$ intersect, implying that $A + B = Z_p$. Assume, therefore, that $|A| + |B| \leqslant p$ and suppose the result is false and $|A + B| \leqslant |A| + |B| - 2$. Let C be a subset of Z_p satisfying $A + B \subset C$ and $|C| = |A| + |B| - 2$. Define $f = f(x, y) = \prod_{c \in C}(x + y - c)$ and observe that, by the definition of C,

$$f(a, b) = 0 \text{ for all } a \in A, b \in B. \tag{3.3}$$

Put $t_1 = |A| - 1, t_2 = |B| - 1$ and note that the coefficient of $x^{t_1}y^{t_2}$ in f is the binomial coefficient $\binom{|A|+|B|-2}{|A|-1}$ which is nonzero in Z_p, since $|A| + |B| - 2 < p$. Therefore, by Theorem 1.2 (with $n = 2, S_1 = A, S_2 = B$), there is an $a \in A$ and a $b \in B$ so that $f(a, b) \neq 0$, contradicting (3.3) and completing the proof. $\square$

4. Restricted sums

The first theorem in this section is a general result, first proved in [11]. Here we observe that it is a simple consequence of Theorem 1.2 above. We also describe some of its applications, proved in [11], which are extensions of the Cauchy–Davenport theorem.

Let p be a prime. For a polynomial $h = h(x_0, x_1, \ldots, x_k)$ over Z_p and for subsets $A_0, A_1, \ldots, A_k$ of Z_p, define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + a_1 + \cdots + a_k : a_i \in A_i, \quad h(a_0, a_1, \ldots, a_k) \neq 0\}.$$

Theorem 4.1 ([11]). *Let p be a prime and let $h = h(x_0, \ldots, x_k)$ be a polynomial over Z_p. Let $A_0, A_1, \ldots, A_k$ be nonempty subsets of Z_p, where $|A_i| = c_i+1$, and define $m = \sum_{i=0}^{k} c_i - \deg(h)$. If the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in*

$$(x_0 + x_1 + \cdots + x_k)^m h(x_0, x_1, \ldots, x_k)$$

is nonzero (in Z_p), then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geqslant m + 1$$

(*and hence $m < p$*).

Proof. Suppose the assertion is false, and let E be a (multi-) set of m (not necessarily distinct) elements of Z_p that contains the set $\oplus_h \sum_{i=0}^k A_i$. Let $Q = Q(x_0, \ldots, x_k)$ be the polynomial defined as follows:

$$Q(x_0, \ldots, x_k) = h(x_0, x_1, \ldots x_k) \prod_{e \in E} (x_0 + \cdots + x_k - e).$$

Note that

$$Q(x_0, \ldots, x_k) = 0 \quad \text{for all} \quad (x_0, \ldots, x_k) \in (A_0, \ldots, A_k). \tag{4.1}$$

This is because, for each such $(x_0, \ldots, x_k)$, either $h(x_0, \ldots, x_k) = 0$ or $x_0 + \cdots + x_k \in \oplus_h \sum_{i=0}^k A_i \subset E$. Note also that $\deg(Q) = m + \deg(h) = \sum_{i=0}^k c_i$ and hence the coefficient of the monomial $x_0^{c_0} \cdots x_k^{c_k}$ in Q is the same as that of this monomial in the polynomial $(x_0 + \cdots + x_k)^m h(x_0, \ldots, x_k)$, which is nonzero, by assumption.

By Theorem 1.2 there are $x_0 \in A_0,\ x_1 \in A_1, \ldots, x_k \in A_k$ such that $Q(x_0, x_1, \ldots, x_k) \neq 0$, contradicting (4.1) and completing the proof. □

One of the applications of the last theorem is the following.

Proposition 4.2. *Let p be a prime, and let $A_0, A_1, \ldots, A_k$ be nonempty subsets of the cyclic group Z_p. If $|A_i| \neq |A_j|$ for all $0 \leqslant i < j \leqslant k$ and $\sum_{i=0}^k |A_i| \leqslant p + \binom{k+2}{2} - 1$, then*

$$|\{a_0 + a_1 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \text{ for all } \ i \neq j\}| \geqslant \sum_{i=0}^k |A_i| - \binom{k+2}{2} + 1.$$

Note that the very special case of this proposition in which $k = 1$, $A_0 = A$ and $A_1 = A - \{a\}$ for an arbitrary element $a \in A$ implies that, if $A \subset Z_p$ and $2|A| - 1 \leqslant p + 2$, then the number of sums $a_1 + a_2$ with $a_1, a_2 \in A$ and $a_1 \neq a_2$ is at least $2|A| - 3$. This easily implies the following theorem, conjectured by Erdős and Heilbronn in 1964 (see, for instance, [26]). Special cases of this conjecture have been proved by various researchers [50, 44, 51, 30] and the full conjecture has recently been proved by Dias da Silva and Hamidoune [22], using some tools from linear algebra and the representation theory of the symmetric group.

Theorem 4.3 ([22]). *If p is a prime, and A is a nonempty subset of Z_p, then*

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geqslant \min\{p, 2|A| - 3\}.$$

In order to deduce Proposition 4.2 from Theorem 4.1 we need the following lemma, which can be easily deduced from the known results about the Ballot problem (see, for instance, [45]), as well as from the known connection between this problem and the hook formula for the number of Young tableaux of a given shape. A simple, direct proof is given in [11].

Lemma 4.4. *Let $c_0, \ldots, c_k$ be nonnegative integers and suppose that $\sum_{i=0}^{k} c_i = m + \binom{k+1}{2}$, where m is a nonnegative integer. Then the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in the polynomial*

$$(x_0 + x_1 + \cdots + x_k)^m \prod_{k \geqslant i > j \geqslant 0} (x_i - x_j)$$

is

$$\frac{m!}{c_0!c_1!\ldots c_k!} \prod_{k \geqslant i > j \geqslant 0} (c_i - c_j).$$

□

Let p be a prime, and let $A_0, A_1, \ldots, A_k$ be nonempty subsets of the cyclic group Z_p. Define

$$\oplus_{i=0}^{k} A_i = \{a_0 + a_1 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \quad \text{for all} \quad i \neq j\}.$$

In this notation, the assertion of Proposition 4.2 is that if $|A_i| \neq |A_j|$ for all $0 \leqslant i < j \leqslant k$ and $\sum_{i=0}^{k} |A_i| \leqslant p + \binom{k+2}{2} - 1$ then

$$|\oplus_{i=0}^{k} A_i| \geqslant \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Proof of Proposition 4.2. Define

$$h(x_0, \ldots, x_k) = \prod_{k \geqslant i > j \geqslant 0} (x_i - x_j),$$

and note that, for this h, the sum $\oplus_{i=0}^{k} A_i$ is precisely the sum $\oplus_h \sum_{i=0}^{k} A_i$. Suppose $|A_i| = c_i + 1$ and put

$$m = \sum_{i=0}^{k} c_i - \binom{k+1}{2} \quad \left(= \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} \right).$$

By assumption $m < p$ and by Lemma 4.4, the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in

$$h \cdot (x_0 + \cdots + x_k)^m$$

is

$$\frac{m!}{c_0!c_1!\ldots c_k!} \prod_{k \geqslant i > j \geqslant 0} (c_i - c_j),$$

which is nonzero modulo p, since $m < p$ and the numbers c_i are pairwise distinct. Since $m = \sum_{i=0}^{k} c_i + \deg(h)$, the desired result follows from Theorem 4.1. □

An easy consequence of Proposition 4.2 is the following. See [11] for the detailed proof.

Theorem 4.5. *Let p be a prime, and let $A_0, \ldots, A_k$ be nonempty subsets of Z_p, where $|A_i| = b_i$, and suppose $b_0 \geqslant b_1 \ldots \geqslant b_k$. Define $b'_0, \ldots, b'_k$ by*

$$b'_0 = b_0 \quad \text{and} \quad b'_i = \min\{b'_{i-1} - 1, b_i\}, \text{ for } 1 \leqslant i \leqslant k. \tag{4.2}$$

If $b'_k > 0$ *then*

$$|\oplus_{i=0}^{k} A_i| \geqslant \min\left\{p, \sum_{i=0}^{k} b'_i - \binom{k+2}{2} + 1\right\}.$$

Moreover, the above estimate is sharp for all possible values of $p \geqslant b_0 \geqslant \cdots \geqslant b_k$.

The following result of Dias da Silva and Hamidoune [22] is a simple consequence of (a special case of) the above theorem.

Theorem 4.6 ([22]). *Let* p *be a prime and let* A *be a nonempty subset of* Z_p. *Let* $s^\wedge A$ *denote the set of all sums of* s *distinct elements of* A. *Then* $|s^\wedge A| \geqslant \min\{p, s|A| - s^2 + 1\}$.

Proof. If $|A| < s$ there is nothing to prove. Otherwise put $s = k+1$ and apply Theorem 4.5 with $A_i = A$ for all i. Here $b'_i = |A| - i$ for all $0 \leqslant i \leqslant k$ and hence

$$\begin{aligned} |(k+1)^\wedge A| = |\oplus_{i=0}^{k} A_i| &\geqslant \min\left\{p, \sum_{i=0}^{k}(|A| - i) - \binom{k+2}{2} + 1\right\} \\ &= \min\left\{p, (k+1)|A| - \binom{k+1}{2} - \binom{k+2}{2} + 1\right\} \\ &= \min\{p, (k+1)|A| - (k+1)^2 + 1\}. \end{aligned}$$

□

Another easy application of Theorem 4.1 is the following result, proved in [10].

Proposition 4.7. *If* p *is a prime and* A, B *are two nonempty subsets of* Z_p, *then*

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

The proof is by applying Theorem 4.1 with $k = 1$, $h = x_0 x_1 - 1$, $A_0 = A$, $A_1 = B$, and $m = |A| + |B| - 4$. It is also shown in [10] that the above estimate is tight in all nontrivial cases. Additional extensions of the above proposition appear in [11].

5. Set addition in vector spaces over prime fields

A triple (r, s, n) of positive integers satisfies the *Hopf–Stiefel condition* if

$$\binom{n}{k} \text{ is even for every integer } k \text{ satisfying } \; n - r < k < s.$$

This condition arises in topology. However, studying the combinatorial aspects of the well-known Hurwitz problem, Yuzvinsky [61] showed that it has an interesting relation to a natural additive problem. He proved that in a vector space of infinite dimension over $GF(2)$, there exist two subsets $A, B \subset V$ satisfying $|A| = r$, $|B| = s$ and $|A + B| \leqslant n$ if and only if the triple (r, s, n) satisfies the Hopf–Stiefel condition.

Eliahou and Kervaire [24] have shown very recently that this can be proved using the algebraic technique of [10] and [11], and generalized this result to an arbitrary prime p, thus obtaining a common generalization of Yuzvinsky's result and the Cauchy–Davenport theorem. Here is a description of their result, and a quick derivation of it from Theorem 1.2. It is worth noting that the same result also follows from the main result of Bollobás and Leader in [19], proved by a different, more combinatorial, approach.

Let us say that a triple (r, s, n) of positive integers satisfies the *Hopf–Stiefel condition with respect to a prime p* if

$$\binom{n}{k} \text{ is divisible by } p \text{ for every integer } k \text{ satisfying } \; n - r < k < s. \tag{5.1}$$

Let $\beta_p(r, s)$ denote the smallest integer n for which the triple (r, s, n) satisfies (5.1). We note that it is not difficult to give a recursive formula for $\beta_p(r, s)$, which enables one to compute it quickly, given the representation of r and s in basis p.

Theorem 5.1 ([24]). *If A and B are two finite nonempty subsets of a vector space V over $GF(p)$, and $|A| = r$, $|B| = s$, then $|A + B| \geqslant \beta_p(r, s)$.*

Proof. We may assume that V is finite, and identify it with the finite field F_q of the same cardinality over $GF(p)$. Viewing A and B as subsets of F_q, define $C = A + B$, and assume the assertion is false and $|C| = n < \beta_p(r, s)$. As in the previous section, define

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

where Q is a polynomial over F_q, and observe that $Q(a, b) = 0$ for all $a \in A, b \in B$. By the definition of $\beta_p(r, s)$, there is some k satisfying $n - r < k < s$ such that $\binom{n}{k}$ is not divisible by p. Therefore, the coefficient of $x^{n-k}y^k$ in the above polynomial is not zero, and since $|A| = r > n - k$, $|B| = s > k$, there are, by Theorem 1.2, $a \in A$ and $b \in B$ such that $Q(a, b) \neq 0$: a contradiction. This completes the proof. $\square$

The authors of [24] have also shown that the estimate in Theorem 5.1 is sharp for all possible r and s. In fact, if A is the set of r vectors whose coordinates correspond to the p-adic representation of the integers $0, 1, \ldots, r - 1$, and B is the set of s vectors whose coordinates correspond to the p-adic representation of the integers $0, 1, \ldots, s - 1$, it is not too difficult to check that $A + B$ is the set of of all vectors whose coordinates correspond to the p-adic representation of the integers $0, 1, \ldots, \beta_p(r, s) - 1$. For more details and several extensions, see [24].

6. Graphs, subgraphs and cubes

A well-known conjecture of Berge and Sauer, proved by Taśkinov [54], asserts that any simple 4-regular graph contains a 3-regular subgraph. This assertion is easily seen to be false for graphs with multiple edges, but, as shown in [6], one extra edge suffices to ensure a 3-regular subgraph in this more general case as well. This follows from the case $p = 3$ in the following result, which, as shown below, can be derived quickly from Theorem 1.2.

Theorem 6.1 ([6]). *For any prime p, any loopless graph $G = (V, E)$ with average degree bigger than $2p - 2$ and maximum degree at most $2p - 1$ contains a p-regular subgraph.*

Proof. Let $(a_{v,e})_{v\in V,e\in E}$ denote the incidence matrix of G defined by $a_{v,e}=1$ if $v\in e$ and $a_{v,e}=0$ otherwise. Associate each edge e of G with a variable x_e and consider the polynomial

$$F=\prod_{v\in V}\left[1-\left(\sum_{e\in E}a_{v,e}x_e\right)^{p-1}\right]-\prod_{e\in E}(1-x_e),$$

over $GF(p)$. Notice that the degree of F is $|E|$, since the degree of the first product is at most $(p-1)|V|<|E|$, by the assumption on the average degree of G. Moreover, the coefficient of $\prod_{e\in E}x_e$ in F is $(-1)^{|E|+1}\neq 0$. Therefore, by Theorem 1.2, there are values $x_e\in\{0,1\}$ such that $F(x_e:e\in E)\neq 0$. By the definition of F, the above vector $(x_e:e\in E)$ is not the zero vector, since for this vector $F=0$. In addition, for this vector, $\sum_{e\in E}a_{v,e}x_e$ is zero modulo p for every v, since otherwise F would vanish at this point. Therefore, in the subgraph consisting of all edges $e\in E$ for which $x_e=1$ all degrees are divisible by p, and since the maximum degree is smaller than $2p$ all positive degrees are precisely p, as needed. □

The assertion of Theorem 6.1 is proved in [6] for prime powers p as well, but it is not known if it holds for every integer p. Combining this result with some additional combinatorial arguments, one can show that for every $k\geqslant 4r$, every loopless k-regular graph contains an r-regular subgraph. For more details and additional results, see [6].

Erdős and Sauer (see, for instance, [17], page 399) raised the problem of estimating the maximum number of edges in a simple graph on n vertices that contains no 3-regular subgraph. They conjectured that for every positive ϵ this number does not exceed $n^{1+\epsilon}$, provided n is sufficiently large as a function of ϵ. This has been proved by Pyber [48], using Theorem 6.1. He proved that any simple graph on n vertices with at least $200n\log n$ edges contains a subgraph with maximum degree 5 and average degree more than 4. This subgraph contains, by Theorem 6.1, a 3-regular subgraph. On the other hand, Pyber, Rödl and Szemerédi [49] proved, by probabilistic arguments, that there are simple graphs on n vertices with at least $\Omega(n\log\log n)$ edges that contain no 3-regular subgraphs. Thus Pyber's estimate is not far from being best possible.

Here is another application of Theorem 1.2, which is not very natural, but demonstrates its versatility.

Proposition 6.2. *Let p be a prime, and let $G=(V,E)$ be a graph on a set of $|V|>d(p-1)$ vertices. Then there is a nonempty subset U of vertices of G such that the number of cliques of d vertices of G that intersect U is 0 modulo p.*

Proof. For each subset I of vertices of G, let $K(I)$ denote the number of copies of K_d in G that contain I. Associate each vertex $v\in V$ with a variable x_v, and consider the polynomial

$$F=\prod_{v\in V}(1-x_v)-1+G,$$

where

$$G = \left[\sum_{\emptyset \neq I \subset V} (-1)^{|I|+1} K(I) \prod_{i \in I} x_i\right]^{p-1}$$

over $GF(p)$. Since $K(I)$ is obviously zero for all I of cardinality bigger than d, the degree of this polynomial is $|V|$, as the degree of G is at most $d(p-1) < |V|$. Moreover, the coefficient of $\prod_{v \in V} x_v$ in F is $(-1)^{|V|} \neq 0$. Therefore, by Theorem 1.2, there are $x_v \in \{0, 1\}$ for which $F(x_v : v \in V) \neq 0$. Since F vanishes on the all zero vector, it follows that not all numbers x_v are zero, and hence that $G(x_v : v \in V) \neq 1$, implying, by Fermat's Little Theorem, that

$$\sum_{\emptyset \neq I \subset V} (-1)^{|I|+1} K(I) \prod_{i \in I} x_i \equiv 0 (\text{mod } p).$$

However, the left-hand side of the last congruence is precisely the number of copies of K_d that intersect the set $U = \{v : x_v = 1\}$, by the Inclusion-Exclusion formula. Since U is nonempty, the desired result follows. □

The assertion of the last proposition can be proved for prime powers p as well. See also [8] and [4] for some related results. Some versions of these results arise in the study of the minimum possible degree of a polynomial that represents the OR function of n variables in the sense discussed in [56] and its references.

We close this section with a simple geometric result, proved in [7], answering a question of Komjáth. As shown below, this result is also a simple consequence of Theorem 1.2.

Theorem 6.3 ([7]). *Let $H_1, H_2, \ldots, H_m$ be a family of hyperplanes in R^n that cover all vertices of the unit cube $\{0, 1\}^n$ but one. Then $m \geqslant n$.*

Proof. Clearly we may assume that the uncovered vertex is the all zero vector. Let $(a_i, x) = b_i$ be the equation defining H_i, where $x = (x_1, x_2, \ldots, x_n)$, and (a, b) is the inner product between the two vectors a and b. Note that for every i, $b_i \neq 0$, since H_i does not cover the origin. Assume the assertion is false and $m < n$, and consider the polynomial

$$P(x) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) - \prod_{i=1}^{m} [(a_i, x) - b_i].$$

The degree of this polynomial is clearly n, and the coefficient of $\prod_{i=1}^{n} x_i$ in it is

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j \neq 0.$$

Therefore, by Theorem 1.2 there is a point $x \in \{0, 1\}^n$ for which $P(x) \neq 0$. This point is not the all zero vector, as P vanishes on it, and therefore it is some other vertex of the cube. But in this case $(a_i, x) - b_i = 0$ for some i (as the vertex is covered by some H_i), implying that P does vanish on this point: a contradiction. □

The above result is clearly tight. Several extensions are proved in [7].

7. Graph colouring

Graph colouring is arguably the most popular subject in graph theory. An interesting variant of the classical problem of colouring properly the vertices of a graph with the minimum possible number of colours arises when one imposes some restrictions on the colours available for every vertex. This variant received a considerable amount of attention that led to several fascinating conjectures and results, and its study combines interesting combinatorial techniques with powerful algebraic and probabilistic ideas. The subject, initiated independently by Vizing [59] and by Erdős, Rubin and Taylor [28], is usually known as the study of the *choosability* properties of a graph. Tarsi and the author developed in [13] an algebraic technique that has already been applied by various researchers to solve several problems in this area as well as problems dealing with traditional graph colouring. In this section we observe that the basic results of this technique can be derived from Theorem 1.2, and describe various applications. More details on some of these applications can be found in the survey [2].

We start with some notation and background. A *vertex colouring* of a graph G is an assignment of a colour to each vertex of G. The colouring is *proper* if adjacent vertices receive distinct colours. The *chromatic number* $\chi(G)$ of G is the minimum number of colours used in a proper vertex colouring of G. An *edge colouring* of G is, similarly, an assignment of a colour to each edge of G. It is *proper* if adjacent edges receive distinct colours. The minimum number of colours in a proper edge colouring of G is the *chromatic index* $\chi'(G)$ of G. This is clearly equal to the chromatic number of the line graph of G.

If $G = (V, E)$ is a (finite, directed or undirected) graph, and f is a function that assigns to each vertex v of G a positive integer $f(v)$, we say that G is f-*choosable* if, for every assignment of sets of integers $S(v) \subset Z$ to all the vertices $v \in V$, where $|S(v)| = f(v)$ for all v, there is a proper vertex colouring $c : V \mapsto Z$ so that $c(v) \in S(v)$ for all $v \in V$. The graph G is k-*choosable* if it is f-choosable for the constant function $f(v) \equiv k$. The *choice number* of G, denoted $\mathrm{ch}(G)$, is the minimum integer k such that G is k-choosable. Obviously, this number is at least the classical chromatic number $\chi(G)$ of G. The choice number of the line graph of G, which we denote here by $\mathrm{ch}'(G)$, is usually called the *list chromatic index* of G, and it is clearly at least the chromatic index $\chi'(G)$ of G.

As observed by various researchers, there are many graphs G for which the choice number $\mathrm{ch}(G)$ is strictly larger than the chromatic number $\chi(G)$. A simple example demonstrating this fact is the complete bipartite graph $K_{3,3}$. If $\{u_1, u_2, u_3\}$ and $\{v_1, v_2, v_3\}$ are its two vertex-classes and $S(u_i) = S(v_i) = \{1, 2, 3\} \setminus \{i\}$, then there is no proper vertex colouring assigning to each vertex w a colour from its class $S(w)$. Therefore, the choice number of this graph exceeds its chromatic number. In fact, it is not difficult to show that, for any $k \geqslant 2$, there are bipartite graphs whose choice number exceeds k. Moreover, in [2] it is proved, using probabilistic arguments, that for every k there is some finite $c(k)$ so that the choice number of every simple graph with minimum degree at least $c(k)$ exceeds k.

In view of this, the following conjecture, suggested independently by various researchers including Vizing, Albertson, Collins, Tucker and Gupta, but apparently first published by Bollobás and Harris ([18]), is somewhat surprising.

Conjecture 7.1 (The List Colouring Conjecture). *For every graph G, $\mathrm{ch}'(G) = \chi'(G)$.*

This conjecture asserts that for *line graphs* there is no gap at all between the choice number and the chromatic number. Many of the most interesting results in the area are proofs of special cases of this conjecture, which is still wide open. An asymptotic version of it, however, has been proven by Kahn [39] using probabilistic arguments: for simple graphs of maximum degree d, $\mathrm{ch}'(G) = (1 + o(1))d$, where the $o(1)$-term tends to zero as d tends to infinity. Since in this case $\chi'(G)$ is either d or $d + 1$, by Vizing's theorem [58], this shows that the List Colouring Conjecture is asymptotically nearly correct.

The *graph polynomial* $f_G = f_G(x_1, x_2, \ldots, x_n)$ of a directed or undirected graph $G = (V, E)$ on a set $V = \{v_1, \ldots, v_n\}$ of n vertices is defined by $f_G(x_1, x_2, \ldots, x_n) = \Pi\{(x_i - x_j) : i < j,\ \{v_i, v_j\} \in E\}$. This polynomial has been studied by various researchers, starting with Petersen [47] in 1891. See also, for example, [52] and [41].

A subdigraph H of a directed graph D is called *Eulerian* if the in-degree $d_H^-(v)$ of every vertex v of H is equal to its out-degree $d_H^+(v)$. Note that we do not assume that H is connected. H is *even* if it has an even number of edges; otherwise, it is *odd*. Let $EE(D)$ and $EO(D)$ denote the numbers of even and odd Eulerian subgraphs of D, respectively. (For convenience we agree that the empty subgraph is an even Eulerian subgraph.) The following result is proved in [13].

Theorem 7.2. *Let $D = (V, E)$ be an orientation of an undirected graph G, denote $V = \{1, 2, \ldots, n\}$ and define $f : V \mapsto Z$ by $f(i) = d_i + 1$, where d_i is the out-degree of i in D. If $EE(D) \neq EO(D)$, then D is f-choosable.*

Proof (sketch). For $1 \leqslant i \leqslant n$, let $S_i \subset Z$ be a set of $d_i + 1$ distinct integers. The existence of a proper colouring of D assigning to each vertex i a colour from its list S_i is equivalent to the existence of colours $c_i \in S_i$ such that $f_G(c_1, c_2, \ldots, c_n) \neq 0$.

Since the degree of f_G is $\sum_{i=1}^n d_i$, it suffices to show that the coefficient of $\prod_{i=1}^n x_i^{d_i}$ in f_G is nonzero in order to deduce the existence of such colours c_i from Theorem 1.2. This can be done by interpreting this coefficient combinatorially.

It is not too difficult to see that the coefficients of the monomials that appear in the standard representation of f_G as a linear combination of monomials can be expressed in terms of the orientations of G as follows. Call an orientation D of G *even* if the number of its directed edges (i, j) with $i > j$ is even; otherwise call it *odd*. For nonnegative integers $d_1, d_2, \ldots, d_n$, let $DE(d_1, \ldots, d_n)$ and $DO(d_1, \ldots, d_n)$ denote, respectively, the sets of all even and odd orientations of G in which the out-degree of the vertex v_i is d_i, for $1 \leqslant i \leqslant n$. In this notation, one can check that

$$f_G(x_1, \ldots, x_n) = \sum_{d_1, \ldots, d_n \geqslant 0} \left(\left|DE(d_1, \ldots, d_n)\right| - \left|DO(d_1, \ldots, d_n)\right|\right) \Pi_{i=1}^n x_i^{d_i}.$$

Consider, now, the given orientation D which lies in $DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$. For any orientation $D_2 \in DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$, let $D \oplus D_2$ denote the set of all oriented edges of D whose orientation in D_2 is in the opposite direction. Since the out-degree of every vertex in D is equal to its out-degree in D_2, it follows that $D \oplus D_2$ is an Eulerian subgraph of D. Moreover, $D \oplus D_2$ is even as an Eulerian subgraph if and only if D and D_2 are both even or both odd. The mapping $D_2 \longrightarrow D \oplus D_2$ is clearly a bijection between $DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$ and the set of all Eulerian subgraphs of D. In the case where D is even, it maps even orientations to even (Eulerian) subgraphs, and odd orientations to odd subgraphs. Otherwise, it maps even orientations to odd subgraphs, and odd orientations to even subgraphs. In any case,

$$\Big| \big|DE(d_1, \ldots, d_n)\big| - \big|DO(d_1, \ldots, d_n)\big| \Big| = \big|EE(D) - EO(D)\big|.$$

Therefore, the absolute value of the coefficient of the monomial $\Pi_{i=1}^{n} x_i^{d_i}$ in the standard representation of $f_G = f_G(x_1, \ldots, x_n)$ as a linear combination of monomials, is $\big|EE(D) - EO(D)\big|$. In particular, if $EE(D) \neq EO(D)$, then this coefficient is not zero and the desired result follows from Theorem 1.2. □

An interesting application of Theorem 7.2 has been obtained by Fleischner and Stiebitz in [29], solving a problem raised by Du, Hsu and Hwang in [23], as well as a strengthening of it suggested by Erdős.

Theorem 7.3 ([29]). *Let G be a graph on $3n$ vertices, whose set of edges is the disjoint union of a Hamilton cycle and n pairwise vertex-disjoint triangles. Then the choice number and the chromatic number of G are both* 3.

The proof is based on a subtle parity argument that shows that, if D is the digraph obtained from G by directing the Hamilton cycle as well as each of the triangles cyclically, then $EE(D) - EO(D) \equiv 2 (\mathrm{mod}\ 4)$. The result thus follows from Theorem 7.2.

Another application of Theorem 7.2 together with some additional combinatorial arguments is the following result, which solves an open problem from [28].

Theorem 7.4 ([13]). *The choice number of every planar bipartite graph is at most* 3.

This is tight, since $\mathrm{ch}(K_{2,4}) = 3$.

Recall that the List Colouring Conjecture (Conjecture 7.1) asserts that $\mathrm{ch}'(G) = \chi'(G)$ for every graph G. In order to try to apply Theorem 7.2 for tackling this problem, it is useful to find a more convenient expression for the difference $EE(D) - EO(D)$, where D is the appropriate orientation of a given line graph. Such an expression is described in [2] for line graphs of d-regular graphs of chromatic index d. This expression is the sum, over all proper d-edge colourings of the graph, of an appropriately defined *sign* of the colouring. See [2] for more details, and [36] for a related discussion. Combining this with a known result of [57] (which asserts that for planar cubic graphs of chromatic index 3 all proper 3-edge colourings have the same sign), and with the Four Colour Theorem, the following result, observed by F. Jaeger and M. Tarsi, follows immediately.

Corollary 7.5. *For every 2-connected cubic planar graph G,* $\mathrm{ch}'(G) = 3$.

Note that the above result is a strengthening of the Four Colour Theorem, which is well known to be equivalent to the fact that the chromatic index of any such graph is 3.

As shown in [25], it is possible to extend this proof to any d-regular planar multigraph with chromatic index d.

Another interesting application of the algebraic method described above appears in [34], where the authors apply it to show that the List Colouring Conjecture holds for complete graphs with an odd number of vertices, and to improve the error term in the asymptotic estimate of Kahn for the maximum possible list chromatic index of a simple graph with maximum degree d. Finally we mention that Galvin [31] recently proved that the List Colouring Conjecture holds for any bipartite multigraph, by an elementary, non-algebraic method.

8. The Permanent Lemma

The following lemma is a slight extension of a lemma proved in [12]. As shown below, it is an immediate corollary of Theorem 1.2 and has several interesting applications.

Lemma 8.1 (The Permanent Lemma). *Let $A = (a_{ij})$ be an $n \times n$ matrix over a field F, and suppose its permanent* $\mathrm{Per}(A)$ *is nonzero (over F). Then, for any vector $b = (b_1, b_2, \ldots, b_n) \in F^n$ and for any family of sets $S_1, S_2, \ldots, S_n$ of F, each of cardinality* 2, *there is a vector $x \in S_1 \times S_2 \times \cdots \times S_n$ such that, for every i, the ith coordinate of Ax differs from b_i.*

Proof. The polynomial

$$P(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} \left[\sum_{j=1}^{n} a_{ij} x_j - b_j \right]$$

is of degree n and the coefficient of $\prod_{i=1}^{n} x_i$ in it is $\mathrm{Per}(A) \neq 0$. The result thus follows from Theorem 1.2. □

Note that, in the special case $S_i = \{0, 1\}$ for every i, the above lemma asserts that, if the permanent of A is nonzero, then for any vector b there is a subset of the column-vectors of A whose sum differs from b in all coordinates.

A conjecture of Jaeger asserts that, for any field with more than 3 elements and for any nonsingular $n \times n$ matrix A over the field, there is a vector x so that both x and Ax have nonzero coordinates. Note that for the special case of fields of characteristic 2 this follows immediately from the Permanent Lemma. Simply take b to be the zero vector, let each S_i be an arbitrary subset of size 2 of the field that does not contain zero, and observe that in characteristic 2 the permanent and the determinant coincide, implying that $\mathrm{Per}(A) \neq 0$. With slightly more work relying on some simple properties of the permanent function, the conjecture is proved in [12] for every non-prime field. It is still open for prime fields and, in particular, for $p = 5$.

Let $f(n, d)$ denote the minimum possible number f so that every set of f lattice points in the d-dimensional Euclidean space contains a subset of cardinality n whose centroid is also a lattice point. The problem of determining or estimating $f(n,d)$ was suggested by Harborth [35], and studied by various authors.

It is convenient to reformulate the definition of $f(n,d)$ in terms of sequences of elements of the abelian group Z_n^d. In these terms, $f(n,d)$ is the minimum possible f so that every sequence of f members of Z_n^d contains a subsequence of size n, the sum of whose elements (in the group) is 0.

By an old result of Erdős, Ginzburg and Ziv [27], $f(n,1) = 2n-1$ for all n. The main part of the proof of this statement is its proof for prime values of $n = p$, as the general case can then be easily proved by induction.

Proposition 8.2 ([27]). *For any prime p, any sequence of $2p-1$ members of Z_p contains a subsequence of cardinality p, the sum of whose members is 0 (in Z_p).*

Proof. There are many proofs of this result. Here is one using the Permanent Lemma. Given $2p-1$ members of Z_p, renumber them $a_1, a_2, \ldots, a_{2p-1}$ such that $0 \leqslant a_1 \leqslant \cdots \leqslant a_{2p-1}$. If there is an $i \leqslant p-1$ such that $a_i = a_{i+p-1}$, then $a_i + a_{i+1} + \cdots + a_{i+p-1} = 0$, as needed. Otherwise, let A denote the $(p-1)\times(p-1)$ all one matrix, and define $S_i = \{a_i, a_{i+p-1}\}$ for all $1 \leqslant i \leqslant p-1$. Let $b_1, \ldots, b_{p-1}$ be the set of all elements of Z_p besides $-a_{2p-1}$. Since $\mathrm{Per}(A) = (p-1)! \neq 0$, by Lemma 8.1, there are $s_i \in S_i$ such that the sum $\sum_{j=1}^{p-1} s_i$ differs from each b_j and is thus equal to $-a_{2p-1}$. Hence, in Z_p,

$$a_{2p-1} + \sum_{i=1}^{p-1} s_i = 0,$$

completing the proof. $\square$

Kemnitz [40] conjectured that $f(n,2) = 4n-3$, observed that $f(n,2) \geqslant 4n-3$ for all n and proved his conjecture for $n = 2$, 3, 5 and 7. As in the one-dimensional case, it suffices to prove this conjecture for prime values p. In [5] it is shown that $f(p,2) \leqslant 6p-5$ for every prime p. The details are somewhat complicated, but the main tool is again the Permanent Lemma mentioned above.

An *additive basis* in a vector space Z_p^n is a collection C of (not necessarily distinct) vectors, so that for every vector u in Z_p^n there is a subset of C, the sum of whose elements is u. Motivated by the study of universal flows in graphs, Jaeger, Linial, Payan and Tarsi [37] conjectured that for every prime p there exists a constant $c(p)$, such that any union of $c(p)$ *linear* bases of Z_p^n contains an additive basis. This conjecture is still open, but in [9] it is shown that any union of $\lceil (p-1)\log_e n \rceil + p - 2$ linear bases of Z_p^n contains such an additive basis. Here, too, the Permanent Lemma plays a crucial role in the proof. The main idea is to observe how it can be applied to give equalities rather than inequalities (extending the very simple application described in the proof of Proposition 8.2 above). Here is the basic approach. For a vector v of length n over Z_p, let v^* denote the tensor product of v with the all one vector of length $p-1$. Thus v^* is a vector of length $(p-1)n$ obtained by concatenating $(p-1)$ copies of v. In this notation, the following result follows from the Permanent Lemma.

Lemma 8.3. *Let $S = (v_1, v_2, \ldots, v_{(p-1)n})$ be a sequence of $(p-1)n$ vectors of length n over Z_p, and let A be the $(p-1)n \times (p-1)n$ matrix whose columns are the vectors $v_1^*, v_2^*, \ldots, v_{(p-1)n}^*$. If* $\mathrm{Per}(A) \neq 0$ *(over Z_p), then the sequence S is an additive basis of Z_p^n.*

Proof. For any vector $b = (b_1, b_2, \ldots, b_n)$, let u_b be the concatenation of the $(p-1)$ vectors $b + j, b + 2j, \ldots, b + (p-1)j$, where j is the all one vector of length n. By the Permanent Lemma with all sets $S_i = \{0, 1\}$, there is a subset $I \subset \{1, 2, \ldots, (p-1)n\}$ such that the sum $\sum_{i \in I} v_i^*$ differs from u_b in all coordinates. This supplies $(p-1)$ forbidden values for every coordinate of the sum $\sum_{i \in I} v_i$, and hence implies that $\sum_{i \in I} v_i = b$. Since b was arbitrary, this completes the proof. □

In [9] it is shown that from any set consisting of all elements in the union of an appropriate number of linear bases of Z_p^n it is possible to choose $(p-1)n$ vectors satisfying the assumptions of the lemma. This is done by applying some properties of the permanent function. The details can be found in [9]. The following conjecture seems plausible, and would imply, if true, that the union of any set of p bases of Z_p^n is an additive basis.

Conjecture 8.4. *For any p nonsingular $n \times n$ matrices $A_1, A_2, \ldots, A_p$ over Z_p, there is an $n \times pn$ matrix C such that the $pn \times pn$ matrix*

$$M' = \begin{bmatrix} A_1 & A_2 & \ldots & A_{p-1} & A_p \\ A_1 & A_2 & \ldots & A_{p-1} & A_p \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ A_1 & A_2 & \ldots & A_{p-1} & A_p \\ & & C & & \end{bmatrix}$$

has a nonzero permanent over Z_p.

We close this section with a simple result about directed graphs. A *one-regular* subgraph of a digraph is a subgraph of it in which all out-degrees and all in-degrees are precisely 1 (that is, a spanning subgraph which is a union of directed cycles).

Proposition 8.5. *Let $D = (V, E)$ be a digraph containing a one-regular subgraph. Then, for any assignment of a set S_v of two reals for each vertex v of V, there is a choice $c(v) \in S_v$ for every v, so that for every vertex u the sum $\sum_{v:(u,v) \in E} c(v) \neq 0$.*

Proof. Let $A = (a_{u,v})$ be the adjacency matrix of D defined by $a_{u,v} = 1$ if and only if $(u, v) \in E$ and $a_{u,v} = 0$ otherwise. By the assumption, the permanent of A over the reals is strictly positive. The result thus follows from the Permanent Lemma. □

9. Ideals of polynomials and combinatorial properties

There are several known results that assert that a combinatorial structure satisfies a certain combinatorial property if and only if an appropriate polynomial associated with it lies in a properly defined ideal. Here are three known results of this type, all applying the graph polynomial defined in Section 7.

Theorem 9.1 (Li and Li [41]). *A graph G does not contain an independent set of $k+1$ vertices if and only if the graph polynomial f_G lies in the ideal generated by all graph polynomials of unions of k pairwise vertex disjoint complete graphs that span its set of vertices.*

Theorem 9.2 (Kleitman and Lovász [42, 43]). *A graph G is not k-colourable if and only if the graph polynomial f_G lies in the ideal generated by all graph polynomials of complete graphs on $k+1$ vertices.*

Theorem 9.3 (Alon and Tarsi [13]). *A graph G on the n vertices $\{1,2,\ldots,n\}$ is not k-colourable if and only if the graph polynomial f_G lies in the ideal generated by the polynomials $x_i^k - 1$, $(1 \leqslant i \leqslant n)$.*

Here is a quick proof of the last theorem, using Theorem 1.1.

Proof of Theorem 9.3. If f_G lies in the ideal generated by the polynomials $x_i^k - 1$ then it vanishes whenever each x_i attains a value which is a kth root of unity. This means that in any colouring of the vertices of G by the kth roots of unity, there is a pair of adjacent vertices that get the same colour, implying that G is not k-colourable.

Conversely, suppose G is not k-colourable. Then f_G vanishes whenever each of the polynomials $g_i(x_i) = x_i^k - 1$ vanishes, and thus, by Theorem 1.1, f_G lies in the ideal generated by these polynomials. $\square$

In [14] we show that a certain weighted sum over the proper k-colourings of G can be computed in a simple manner from its graph polynomial f_G. In the same note we also claim to provide a short proof of Theorem 9.2, based on the Hajós–Ore Theorem, but as pointed out by Bjarne Toft [55] this proof contains a subtle error. As described in Section 7, there are several interesting combinatorial consequences that can be derived from (some versions of) Theorem 9.3, but even without any consequences, such theorems are interesting in their own. One reason for this is that these theorems characterize $coNP$-complete properties, which, according to the common belief that the complexity classes NP and $coNP$ differ, cannot be checked by a polynomial time algorithm.

Using Theorem 1.1 it is not difficult to generate results of this type. We illustrate this with two examples, described below. Many other results can be formulated and proved in a similar manner. It would be nice to deduce any interesting combinatorial consequences of these results or their relatives.

The *bandwidth* of a graph $G = (V,E)$ on n vertices is the minimum integer k such that there is a bijection $f : V \mapsto \{1,2,\ldots,n\}$ satisfying $|f(u) - f(v)| \leqslant k$ for every edge $uv \in E$. This invariant has been studied extensively by various researchers. See, for instance, [20] for a survey.

Proposition 9.4. *The bandwidth of a graph $G = (V, E)$ on a set $V = \{1, 2, \ldots, n\}$ of n vertices is at least $k + 1$ if and only if the polynomial*

$$Q_{G,k}(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) \prod_{ij \in E, i<j} \prod_{k < |l| < n} (x_i - x_j - l)$$

lies in the ideal generated by the polynomials

$$\left\{ g_i(x_i) = \prod_{j=1}^{n} (x_i - j), \quad 1 \leqslant i \leqslant n \right\}.$$

Proof. If $Q_{G,k}$ lies in the above-mentioned ideal, then it vanishes whenever we substitute a value in $\{1, 2, \ldots, n\}$ for each x_i. In particular, it vanishes when we substitute distinct values for these variables, implying that there is some edge $ij \in E$ for which $|x_i - x_j| > k$, and hence the bandwidth of G exceeds k.

Conversely, assume the bandwidth of G exceeds k. We claim that $Q_{G,k}(x_1, \ldots, x_n)$ vanishes whenever each x_i attains a value in $\{1, 2, \ldots, n\}$. Indeed, if two of the variables attain the same value, the first product ($\prod_{1 \leqslant i < j \leqslant n}(x_i - x_j)$) in the definition of $Q_{G,k}$ vanishes. Otherwise, the numbers x_i form a permutation of the members of $\{1, 2, \ldots, n\}$ and thus, by the assumption on the bandwidth, there is some edge $ij \in E$ for which $|x_i - x_j| > k$, implying that the polynomial vanishes in this case as well. Therefore, $Q_{G,k}$ vanishes whenever each x_i lies in $\{1, 2, \ldots, n\}$ and thus, by Theorem 1.1, it lies in the ideal generated by the polynomials $g_i(x_i)$, completing the proof. □

A *hypergraph* H is a pair (V, E), where V is a finite set, whose elements are called *vertices*, and E is a collection of subsets of V, called *edges*. It is k-*uniform* if each edge contains precisely k vertices. Thus, a 2-uniform hypergraph is simply a graph. H is 2-*colourable* if there is a vertex colouring of H with two colours so that no edge is monochromatic.

Proposition 9.5. *The* 3-*uniform hypergraph $H = (V, E)$ is not* 2-*colourable if and only if the polynomial*

$$\prod_{e \in E} \left[\left(\sum_{v \in e} x_v \right)^2 - 9 \right]$$

lies in the ideal generated by the polynomials $\{x_v^2 - 1 : v \in V\}$.

Proof. The proof is similar to the previous one. If the polynomial lies in that ideal, then it vanishes whenever each x_v attains a value in $\{-1, 1\}$, implying that some edge is monochromatic in each vertex colouring by $\{-1, 1\}$, and hence implying that H is not 2-colourable. Conversely, if H is not 2-colourable, then in every vertex colouring by the numbers -1 and $+1$ some edge is monochromatic, implying that the polynomial vanishes in each such point, and thus showing, by Theorem 1.1, that it lies in the above ideal. □

Note that, since the properties characterized in any of the theorems in this section are *coNP*-complete, it is possible to use the usual reductions and, for each *coNP*-complete problem, obtain a characterization in terms of some ideals of polynomials. In most cases, however, the known reductions are somewhat complicated, and would thus lead to cumbersome polynomials which are not likely to imply any interesting consequences. The results mentioned here are in terms of relatively simple polynomials, and are therefore more likely to be useful.

10. Concluding remarks

The discussion in Section 7, as well as that in Section 9, raises the hope that the polynomial approach might be helpful in the study of the Four Colour Theorem. This certainly deserves more attention. Further results in the study of the List Colouring Conjecture (Conjecture 7.1) using the algebraic technique are also desirable.

Most proofs presented in this paper are based on the two basic theorems, proved in Section 2, whose proofs are algebraic, and hence non-constructive in the sense that they supply no efficient algorithm for solving the corresponding algorithmic problems.

In the classification of algorithmic problems according to their complexity, it is customary to try and identify the problems that can be solved efficiently, and those that *probably* cannot be solved efficiently. A class of problems that can be solved efficiently is the class P of all problems for which there are deterministic algorithms whose running time is polynomial in the length of the input. A class of problems that probably cannot be solved efficiently are all the NP-complete problems. An extensive list of such problems appears in [32]. It is well known that if any of them can be solved efficiently, then so can all of them, since this would imply that the two complexity classes P and NP are equal.

Is it possible to modify the algebraic proofs given here so that they yield efficient ways of solving the corresponding algorithmic problems? It seems likely that such algorithms do exist. This is related to questions regarding the complexity of search problems that have been studied by several researchers. See, for instance, [38].

In the study of complexity classes like P and NP, one usually considers only decision problems, that is, problems for which the only two possible answers are 'yes' or 'no'. However, the definitions extend easily to the so-called 'search' problems, which are problems where a more elaborate output is sought. The search problems corresponding to the complexity classes P and NP are sometimes denoted by FP and FNP.

Consider, for example, the obvious algorithmic problem suggested by Theorem 6.1 (for $p = 3$, say). Given a simple graph with average degree that exceeds 4 and maximum degree 5, it contains, by this theorem, a 3-regular subgraph. Can we find such a subgraph in polynomial time?

It seems plausible that finding such a subgraph should not be a very difficult task. However, our proof provides no efficient algorithm for accomplishing this task. The situation is similar with many other algorithmic problems corresponding to the various results presented here. Can we, given an input graph satisfying the assumptions of Theorem 7.3 and given a list of three colours for each of its vertices, find, in polynomial time, a proper vertex colouring assigning each vertex a colour from its class? Similarly, can we colour properly the edges of any given planar cubic 2-connected graph using given lists of three colours per edge, in polynomial time?

These problems remain open. Note, however, that any efficient procedure that finds, for a given input polynomial that satisfies the assumptions of Theorem 1.2, a point $(s_1, s_2, \ldots, s_n)$ satisfying its conclusion, would provide efficient algorithms for most of these algorithmic problems. It would thus be interesting to find such an efficient procedure. See also [1] for a related discussion of other algorithmic problems.

Another computational aspect suggested by the results in Section 9 is the complexity of the representation of polynomials in the form that shows they lie in certain ideals. Thus, for example, by Proposition 9.5, a 3-uniform hypergraph is not 2-colourable if and only if the polynomial associated with it in that proposition is a linear combination with polynomial coefficients of the polynomials $x_v^2 - 1$. Since the problem of deciding whether such a given input hypergraph is not 2-colourable is $coNP$-complete, the existence of a representation like this that can be checked in polynomial time would imply that the complexity classes NP and $coNP$ coincide, and this is believed by most researchers not to be the case.

In this paper we have developed and discussed a technique in which polynomials are applied for deriving combinatorial consequences. There are several other known proof techniques in combinatorics that are based on properties of polynomials. The most common and successful one is based on a dimension argument. This is the method of proving an upper bound for the size of a collection of combinatorial structures satisfying certain prescribed properties by associating each structure with a polynomial in some space of polynomials, showing that these polynomials are linearly independent, and then deducing the required bound from the dimension of the corresponding space. There are many interesting results proved in this manner: see, for instance, [33], [15], [16] and [3] for surveys of results of this type.

References

[1] Alon, N. (1991) Non-constructive proofs in combinatorics. In *Proc. International Congress of Mathematicians, Kyoto 1990, Japan*, Springer, Tokyo, pp. 1421–1429.

[2] Alon, N. (1993) Restricted colorings of graphs. In *Surveys in Combinatorics*, *Proc. 14th British Combinatorial Conference*, Vol. 187 of *London Math. Soc. Lecture Notes* (K. Walker, ed.), Cambridge University Press, pp. 1–33.

[3] Alon, N. (1995) Tools from higher algebra. In *Handbook of Combinatorics* (R. Graham, M. Grötschel and L. Lovász, eds), Elsevier, pp. 1749–1783.

[4] Alon, N. and Caro, Y. (1993) On three zero-sum Ramsey-type problems. *J. Graph Theory* **17** 177–192.

[5] Alon, N. and Dubiner, M. (1993) Zero-sum sets of prescribed size. In *Combinatorics*: *Paul Erdős is Eighty*, Vol. 1, *Bolyai Society Math. Studies*, Keszthely, Hungary, pp. 33–50.

[6] Alon, N., Friedland, S. and Kalai, G. (1984) Regular subgraphs of almost regular graphs. *J. Combinatorial Theory Ser. B* **37** 79–91. Also: Alon, N., Friedland, S. and Kalai, G. (1984) Every 4-regular graph plus an edge contains a 3-regular subgraph. *J. Combinatorial Theory Ser. B* **37** 92–93.

[7] Alon, N. and Füredi, Z. (1993) Covering the cube by affine hyperplanes. *European J. Combinatorics* **14** 79–83.

[8] Alon, N., Kleitman, D., Lipton, R., Meshulam, R., Rabin, M. and Spencer, J. (1991), Set systems with no union of cardinality 0 modulo *m*. *Graphs and Combinatorics* **7** 97–99.

[9] Alon, N., Linial, N. and Meshulam, R. (1991) Additive bases of vector spaces over prime fields. *J. Combin. Theory Ser. A* **57** 203–210.

[10] Alon, N., Nathanson, M. B. and Ruzsa, I. Z. (1995) Adding distinct congruence classes modulo a prime. *Amer. Math. Monthly* **102** 250–255.

[11] Alon, N., Nathanson, M. B. and Ruzsa, I. Z. (1996) The polynomial method and restricted sums of congruence classes. *J. Number Theory* **56** 404–417.

[12] Alon, N. and Tarsi, M. (1989) A nowhere-zero point in linear mappings. *Combinatorica* **9** 393–395.

[13] Alon, N. and Tarsi, M. (1992) Colorings and orientations of graphs. *Combinatorica* **12** 125–134.

[14] Alon, N. and Tarsi, M. (1997) A note on graph colorings and graph polynomials. *J. Combin. Theory Ser. B* **70** 197–201.

[15] Babai, L. and Frankl, P. *Linear Algebra Methods in Combinatorics*. To appear.

[16] Blokhuis, A. (1993) Polynomials in finite geometries and combinatorics. In *Surveys in Combinatorics, Proc. 14th British Combinatorial Conference*, Vol. 187 of *London Math. Soc. Lecture Notes* (K. Walker, ed.), Cambridge University Press, pp. 35–52.

[17] Bollobás, B. (1978) *Extremal Graph Theory*, Academic Press.

[18] Bollobás, B. and Harris, A. J. (1985) List colorings of graphs. *Graphs and Combinatorics* **1** 115–127.

[19] Bollobás, B. and Leader, I. (1996) Sums in the grid. *Discrete Math.* **162** 31–48.

[20] Chung, F. R. K. (1988) Labelings of graphs. In *Selected Topics in Graph Theory*, Vol. 3, Academic Press, pp. 151–168.

[21] Davenport, H. (1935) On the addition of residue classes. *J. London Math. Soc.* **10** 30–32.

[22] Dias da Silva, J. A. and Hamidoune, Y. O. (1994) Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.* **26** 140–146.

[23] Du, D. Z., Hsu, D. F. and Hwang, F. K. (1993) The Hamiltonian property of consecutive-d digraphs. *Mathematical and Computer Modelling* **7** 61–63.

[24] Eliahou, S. and Kervaire, M. (1998) Sumsets in vector spaces over finite fields. *J. Number Theory* **71** 12–39.

[25] Ellingham, M. N. and Goddyn, L. (1996) List edge colorings of some 1-factorable multigraphs. *Combinatorica* **16** 343–352.

[26] Erdős, P. and Graham, R. L. (1980) *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Geneva.

[27] Erdős, P., Ginzburg, A. and Ziv, A. (1961) Theorem in the additive number theory. *Bull. Research Council Israel* **10F** 41–43.

[28] Erdős, P., Rubin, A. L. and Taylor, H. (1979) Choosability in graphs. In *Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing. Congressus Numerantium* **XXVI** 125–157.

[29] Fleischner, H. and Stiebitz, M. (1992) A solution to a coloring problem of P. Erdős. *Discrete Math.* **101** 39–48.

[30] Freiman, G. A., Low, L. and Pitman, J. (1993) The proof of Paul Erdős' conjecture of the addition of different residue classes modulo a prime number. In *Structure Theory of Set Addition*, CIRM Marseille, pp. 99–108.

[31] Galvin, F. (1995) The list chromatic index of a bipartite multigraph. *J. Combin. Theory Ser. B* **63** 153–158.

[32] Garey, M. R. and Johnson, D. S. (1979) *Computers and Intractability: A guide to the Theory of NP-Completeness*, W. H. Freeman and Company, New York.

[33] Godsil, C. (1995) Tools from linear algebra. In *Handbook of Combinatorics* (R. Graham, M. Grötschel and L. Lovász, eds), Elsevier, pp. 1705–1748.

[34] Häggkvist, R. and Janssen, J. (1997) New bounds on the list chromatic index of the complete graph and other simple graphs. *Combin. Probab. Comput.* **6** 295–313.

[35] Harborth, H. (1973) Ein Extremalproblem für Gitterpunkte. *J. Reine Angew. Math.* **262/263** 356–360.

[36] Jaeger, F. (1989) On the Penrose number of cubic diagrams. *Discrete Math.* **74** 85–97.
[37] Jaeger, F., Linial, N., Payan, C. and Tarsi, M. (1992) Group connectivity of graphs- a nonhomogeneous analogue of nowhere-zero flow. *J. Combin. Theory Ser. B* **56** 165–182.
[38] Johnson, D. S., Papadimitriou, C. H. and Yannakakis, M. (1988) How easy is local search? *JCSS* **37** 79–100.
[39] Kahn, J. (1996) Asymptotically good list colorings. *J. Combin. Theory Ser. A* **73** 1–59.
[40] Kemnitz, A. (1983) On a lattice point problem. *Ars Combinatoria* **16b** 151–160.
[41] Li, S. Y. R. and Li, W. C. W. (1981) Independence numbers of graphs and generators of ideals. *Combinatorica* **1** 55–61.
[42] Lovász, L. (1982) Bounding the independence number of a graph. In *Bonn Workshop on Combinatorial Optimization* (A. Bachem, M. Grötschel and B. Korte, eds), *Ann. Discrete Math.* **16**, North Holland, Amsterdam, pp. 213–223.
[43] Lovász, L. (1994) Stable sets and polynomials. *Discrete Math.* **124** 137–153.
[44] Mansfield, R. (1981) How many slopes in a polygon? *Israel J. Math.* **39** 265–272.
[45] Macmahon, M. P. A. (1915) *Combinatory Analysis*, Chelsea Publishing Company.
[46] Nathanson, M. B. (1996) *Additive Number Theory: Inverse Theorems and the Geometry of Sumsets*, Springer, New York.
[47] Petersen, J. (1891) Die Theorie der regulären Graphs. *Acta Math.* **15** 193–220.
[48] Pyber, L. (1985) Regular subgraphs of dense graphs. *Combinatorica* **5** 347–349.
[49] Pyber, L., Rödl, V. and Szemerédi, E. (1995) Dense graphs without 3-regular subgraphs. *J. Combin. Theory Ser. B* **63** 41–54.
[50] Rickert, U.-W. (1976) Über eine Vermutung in der additiven Zahlentheorie, PhD thesis, Tech. Univ. Braunschweig.
[51] Rödseth, Ö. J. (1994) Sums of distinct residues mod p. *Acta Arith.* **65** 181–184.
[52] Scheim, D. E. (1974) The number of edge 3-colorings of a planar cubic graph as a permanent. *Discrete Math.* **8** 377–382.
[53] Schmidt, W. (1976) *Equations over Finite Fields: An Elementary Approach*, Vol. 536 of *Lecture Notes in Mathematics*, Springer, Berlin.
[54] Taśkinov, V. A. (1982) Regular subgraphs of regular graphs. *Soviet Math. Dokl.* **26** 37–38.
[55] Toft, B. Private communication, July 1998.
[56] Tsai, S. C. (1996) Lower bounds on representing Boolean functions as polynomials in Z_m. *SIAM J. Discrete Math.* **9** 55–62.
[57] Vigneron, L. (1946) Remarques sur les réseaux cubiques de classe 3 associés au probléme des quatre couleurs. *C. R. Acad. Sc. Paris*, **223** 770–772.
[58] Vizing, V. G. (1964) On an estimate on the chromatic class of a p-graph. *Diskret. Analiz.* **3** 25–30. In Russian.
[59] Vizing, V. G. (1976) Coloring the vertices of a graph in prescribed colors (in Russian), *Diskret. Analiz.* No. 29, *Metody Diskret. Anal. v. Teorii Kodov i Shem* **101** 3–10.
[60] van der Waerden, B. L. (1931) *Modern Algebra*, Julius Springer, Berlin.
[61] Yuzvinsky, S. (1981) Orthogonal pairings of Euclidean spaces. *Michigan Math. J.* **28** 109–119.