Combinatorics, Probability and Computing (1999) 8, 1–6.

A Selection of Problems and Results in Combinatorics

PAUL ERDŐS†

Mathematical Institute of the Hungarian Academy of Sciences,
13–15 Reáltanoda utca, 1053 Budapest, Hungary

In this note, I will present some new problems, and also some old ones which, in my opinion, have been undeservedly forgotten or neglected.

In this note, I present a number of problems in combinatorics that have attracted my attention recently. Some are new, while others are old but seem worthy of a fresh look.

1. This problem was started by Hajnal and myself in 1958. First, a few definitions from set theory. Let $\mathscr{S}$ be a set; to every finite subset $\mathscr{S}'$ of $\mathscr{S}$ we assign an element $f(\mathscr{S}') = x$ of $\mathscr{S}$ such that $x \notin \mathscr{S}'$. A subset $\mathscr{S}'$ of $\mathscr{S}$ is called *independent* or *free* if, for every subset $\mathscr{S}''$ of $\mathscr{S}'$, we have $f(\mathscr{S}'') \notin \mathscr{S}'$. In our first paper with Hajnal [8], we proved that if $|\mathscr{S}| < \aleph_\omega$ we can always find a mapping f from the set of finite subsets of $\mathscr{S}$ to $\mathscr{S}$ such that there is no infinite independent set. We could not decide whether there is always an infinite independent set if $|\mathscr{S}| = \aleph_\omega$. This problem is perhaps undecidable.

In a more recent paper [9], Hajnal and I investigated the following finite version of the problem. Let $|\mathscr{S}| = n < \aleph_0$ and let $h(n)$ be the largest integer such that, for every f, there is an independent subset $\mathscr{S}' \subset \mathscr{S}$, $|\mathscr{S}'| = h(n)$. Further, let $H(n)$ be the smallest integer for which there is a function f such that, for every $\mathscr{S}'' \subset \mathscr{S}$, $|\mathscr{S}''| \geqslant H(n)$, $F[\mathscr{S}''] = \mathscr{S}$, where $F[\mathscr{S}'']$ is the union of all the elements $f(\mathscr{S}''')$, with $\mathscr{S}''' \subset \mathscr{S}''$.

We proved

$$\frac{\log n}{\log 2} < H(n) < \frac{\log n}{\log 2} + \frac{(3 + o(1)) \log\log n}{\log 2}.$$

We observed that

$$h(n) < \frac{\log n + 3\log\log n}{\log 2} + o(\log\log n),$$

but we only had a very poor lower bound for $h(n)$. Three years later Spencer and I [11] proved

$$h(n) > \frac{\log n - \log\log n}{\log 2} + o(\log\log n).$$

† This is the very last paper that Paul Erdős worked on before his death in Warsaw on 20 September 1996.

I think the problem was completely forgotten until a few days ago, when Gyárfás and I took up the problem again. We wanted to prove that

$$H(n) - \frac{\log n}{\log 2} \to \infty. \tag{1}$$

As far as I know (1) is still open; we could not even prove that, for $n = 2^k$,

$$H(n) \geqslant k + 1. \tag{2}$$

We first tried to prove that, for a set $\mathscr{S}$ of size 2^k, there is always a set $A \subset \mathscr{S}$ with $|A| = k$ such that

$$F[A] < 2^k - k. \tag{3}$$

It is easy to see that (3) implies (2), but we could not prove (3). In fact, we are sure that

$$F[A] < 2^k - k^c$$

for every c, if $n = 2^k$ is sufficiently large. It is not impossible that there is a set A of size k such that $F[A] < n(1-\varepsilon)$ or even $F[A] = o(n)$.

2. Here is a recent problem that we formulated with Ralph Faudree. Let $G(2n)$ be a regular graph of $2n$ vertices and degree $n+1$. Is it true that our $G(2n)$ has $c_1 2^{2n}$ subsets that are on a cycle? It is easy to see that there are at least $\left(\frac{1}{2} + o(1)\right) 2^{2n}$ sets that are not on a cycle. Also, if the regularity is replaced by the condition that the minimum degree is $n+1$, the conjecture no longer holds.

3. An older problem which we posed before 1980 goes as follows. Every graph of $m \geqslant 2n+1 \geqslant 7$ vertices and $\binom{2n+1}{2} - \binom{n}{2} - 1$ edges is the union of a bipartite graph and a graph of maximal degree at most $n-1$. Faudree found a very nice proof if the number of vertices is exactly $2n+1$, but the proof fails if the number of vertices is greater than $2n+1$, and the problem is still open.

Let $\mathscr{C}_n$ denote the family of all cycles of lengths between 3 and $n+3$ inclusive. In a paper that will soon appear, Faudree and I prove that, for $n \geqslant 2$,

$$r^*(\mathscr{C}_n, K_{1,n}) = \binom{2n+1}{2} - \binom{n}{2}. \tag{4}$$

In human language, if $G(2n+1, \binom{2n+1}{2} - \binom{n}{2})$ is a graph with $2n+1$ vertices and $\binom{2n+1}{2} - \binom{n}{2}$ edges, then, if we colour the edges of our graph G red and blue, then either there is a red cycle C_m for every $3 \leqslant m \leqslant n+3$ or there is a vertex incident with n blue edges.

Equation (4) is best possible. Our paper with Faudree [2] contains many further problems and results, but I have to leave these for the interested reader.

4. The next two problems arise from recent joint work of Gallai, Tuza and myself. Perhaps the most striking problem we have [5] is as follows. For G a graph, let $\alpha_1(G)$ denote the maximum cardinality of a set of edges that contains at most one edge from

every triangle of G (if G is triangle-free then $\alpha_1(G) = |E|$, the number of edges of G). Similarly, let $\tau_1(G)$ be the minimum cardinality of a set of edges containing at least one edge from every triangle of G. If G is triangle-free then $\tau_1(G) = 0$.

Is it true that, for every graph G on n vertices,

$$\alpha_1(G) + \tau_1(G) \leqslant \left[\frac{n^2}{4}\right]? \tag{5}$$

If true, (5) is probably quite difficult to prove. One difficulty seems to be that there are several graphs of different structure for which there is equality in (5). Three examples are: the complete graph $K(n)$, the complete bipartite graph $K(m,m)$, and the graph obtained from $K(m,m)$ by adding one new vertex joined to every other.

In our paper [5], we prove several other interesting results and state some other problems. We have tried to formulate related problems where the triangle is replaced by a $K(r)$, $r > 3$, but so far we have not been quite successful.

5. In another triple paper with Gallai and Tuza [4], we investigate the following problems. Define a *clique* of G to be a maximal complete subgraph of G. The *clique transversal number* $\tau_C(G)$ is the smallest integer for which there is a set of $\tau_C(G)$ vertices that intersects every clique of G. Our first problem was as follows. Let G run through all graphs of n vertices: what is the maximum possible value of $\tau_C(G)$? Denote this maximum by $f(n)$.

We conjecture that

$$f(n) = n - r(n), \tag{6}$$

where $r(n)$ is the largest integer such that every triangle-free graph contains an independent set of $r(n)$ vertices. It is immediate that $f(n) \geqslant n - r(n)$; indeed, if we take a triangle-free $G(n)$ with largest independent set of size $r(n)$, then we need to find a set intersecting all the edges of our $G(n)$, which has size at least $n - r(n)$. The results of Ajtai, Komlós, Szemerédi [1] and Kim [13] imply that

$$c_1(n \log n)^{1/2} < r(n) < c_2(n \log n)^{1/2}.$$

However, we could only prove

$$f(n) \leqslant n - (2n)^{1/2} + \frac{1}{2}. \tag{7}$$

As a first step we tried to prove

$$f(n) < n - s(n)n^{1/2},$$

for some function $s(n)$ tending to infinity. So far we have not been successful and in fact we could not improve (7).

It seemed to us that if all cliques of G are large, then $\tau_C(G)$ will be smaller. For instance, for $c > 0$, we would like estimates for the least $k_c(n)$ such that, if every clique of a graph $G(n)$ has size $k_c(n)$, then $\tau_C(G(n)) < n(1 - c)$.

We proved that $k_c(n) > n^{c'(\log\log n)}$ is certainly needed to ensure $\tau_C(G(n)) < n(1-c)$. Perhaps $k(n) = n^{\alpha}$ will imply $\tau_C(G(n)) = o(n)$, but we did not prove anything about this. We did succeed in proving that, if every clique of $G(n)$ has size greater than k, then

$$\tau_C(G(n)) \leqslant n - (kn)^{1/2}.$$

Bollobás and I proved that if every clique has size at least $n+3-\lceil 2\sqrt{n}\rceil$ then $\tau_C(G(n)) = 1$, and that the value $n+3-\lceil 2\sqrt{n}\rceil$ is best possible.

Several further interesting problems are stated in our paper. Here I only state one of them. Let $G(n)$ be $K(4)$-free. How large a triangle-free induced subgraph must our $G(n)$ contain? An old result of Erdős and Szekeres [12] implies that our $G(n)$ contains an independent set of size $cn^{1/3}$, but perhaps it contains a much larger triangle-free induced subgraph. Several interesting related problems can be posed, but we must leave them to the interested reader. (I hope this set will not be empty.)

6. Now we discuss some problems of Gyárfás, Ruszinkó and myself [7]. Let $G(n)$ be a triangle-free graph of order n. We want to add as few edges to our $G(n)$ as possible, keeping it triangle-free, so as to make the diameter of the new graph equal to 2 (*i.e.*, so that no more edges can be added without creating a triangle). Denote by $h(G(n))$ the smallest number of edges having this property. We hoped that, if every vertex of $G(n)$ has degree $o(n^{1/2})$, then

$$h(G(n))/n^2 \to 0. \tag{8}$$

Simonovits showed that if the maximal degree is allowed to be $cn^{1/2}$ then (8) need not hold.

A few days ago we started to investigate the following related problem. Let $h_r(n)$ be the smallest integer such that, for every connected triangle-free graph $G(n)$, we can add a set of at most $h_r(n)$ edges to $G(n)$ and obtain a triangle-free graph of diameter at most r. We proved that

$$n - c\sqrt{n} \leqslant h_3(n) \leqslant n,$$

and later improved the lower bound to $n-c$. It is easy to see that $h_4(n) < n$, but we could not decide whether

$$h_4(n) < n(1-\varepsilon)$$

is true. To show that $h_5(n) < n(1-\varepsilon)$ is relatively easy, and we proved that $h_5(n) \leqslant \frac{n-1}{2}$.

7. Gyárfás and I have another paper [6] that will soon appear, and that I feel contains many interesting problems and results. Here is one of our favourite conjectures. If $r \geqslant 3$ and the edges of a $K(r^2+1)$ are coloured with r colours, then there exist $r+1$ vertices with at least one colour not appearing on the edges they span. Clearly the conjecture fails for $r = 2$; we prove it for $r = 3$ and $r = 4$ – the proof is not quite trivial.

It is easy to show that, for infinitely many r, a $K(r^2)$ can be coloured with r colours so that every set of $r+1$ vertices spans all the colours.

8. In a recent paper [10], Hajnal, Tuza and I returned to a type of problem that Gallai and I considered many years ago.

Let X be a finite or infinite set, and $\mathscr{F}$ a system of subsets of X. We say that $\mathscr{F}$ is *r-uniform* if all elements E of $\mathscr{F}$ have $|E| = r$. We say that a subset T of X *represents* $\mathscr{F}$ if $T \cap E \neq \emptyset$ for all $E \in \mathscr{F}$. The *transversal number* (or *covering number*) of $\mathscr{F}$ is the minimum cardinality $\tau(\mathscr{F})$ of a set T which represents $\mathscr{F}$.

Let p, r, s, t be integers. We write

$$(p, s) \longrightarrow_r t$$

if, whenever $\mathscr{F}$ is an r-uniform set system such that every subsystem $\mathscr{F}' \subset \mathscr{F}$ on at most p elements has $\tau(\mathscr{F}') \leqslant s$, then we have $\tau(\mathscr{F}) \leqslant t$.

The first results on this topic were due to Gallai and myself [3]: for instance, we proved that

$$(2t + 2, t) \longrightarrow_2 t \text{ and } (2t + 1, t) \not\longrightarrow_2 t.$$

For $r \geqslant 3$, Hajnal, Tuza and I proved:

$$(3r - 3, 1) \longrightarrow_r \left\lceil \frac{r}{5} \right\rceil.$$

This is reasonably close to the truth, since we also showed that

$$(3r - 3, 1) \not\longrightarrow_r \left\lfloor \frac{3}{16} r + \frac{7}{8} \right\rfloor,$$

but we did not decide the best possible result here.

Several further problems and results are in our paper, but they are somewhat technical and we have to stop.

References

[1] Ajtai, M., Komlós, J. and Szemerédi, E. (1980) A note on Ramsey numbers. *J. Combin. Theory Ser. A* **29** 354–360.

[2] Erdős, P. and Faudree, R. Restricted size Ramsey numbers for cycles and stars. *Discrete Math.* To appear.

[3] Erdős, P. and Gallai, T. (1961) On the maximal number of vertices representing the edges of a graph. *Magyar Tud. Akad. Mat. Kut. Inst. Közl.* **6** 181–203.

[4] Erdős, P., Gallai, T. and Tuza, Zs. (1992) Covering the cliques of a graph with vertices. *Discrete Math.* **108** 279–289.

[5] Erdős, P., Gallai, T. and Tuza, Zs. (1996) Covering and independence in triangle structures. *Discrete Math.* **150** 89–101.

[6] Erdős, P. and Gyárfás, A. Split and balanced colorings of complete graphs. *Discrete Math.* To appear.

[7] Erdős, P., Gyárfás, A. and Ruszinkó, M. How to decrease the diameter of triangle-free graphs? Submitted.

[8] Erdős, P. and Hajnal, A. (1958) On the structure of set mappings. *Acta Math. Acad. Sci. Hungar.* **9** 111–133.

[9] Erdős, P. and Hajnal, A. (1968) On a combinatorial problem. *Mat. Lapok* **19** 345–348. In Hungarian.

[10] Erdős, P., Hajnal, A. and Tuza, Zs. (1991) Local constraints ensuring small representing sets. *J. Combin. Theory Ser. A* **58** 78–84.
[11] Erdős, P. and Spencer, J. (1971) On a problem of Erdős and Hajnal. *Mat. Lapok* **22** 1–2. In Hungarian.
[12] Erdős, P. and Szekeres, G. (1935) A combinatorial problem in geometry. *Compositio Math.* **2** 463–470.
[13] Kim, J. H. (1995) The Ramsey number $R(3,t)$ has order of magnitude $t^2/\log t$. *Random Structures and Algorithms* **7** 173–207.

Combinatorics, Probability and Computing (1999) 8, 7–29.

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,

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

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*

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

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

Proof. Suppose this is false, and define

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

where δ is chosen so that

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

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

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

for all $s_i \in Z_p$. Indeed, this is certainly true, by (3.1), if $(s_1,\ldots,s_n) = (c_1,\ldots,c_n)$. For other values of $(s_1,\ldots,s_n)$, there is, by assumption, a polynomial P_j that does not vanish on $(s_1,\ldots,s_n)$, implying that $1 - P_j(s_1,\ldots,s_n)^{p-1} = 0$. 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 $f(s_1,\ldots,s_n)$.

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

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

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 $s_1,\ldots,s_n \in Z_p$ for which $f(s_1,\ldots,s_n) \neq 0$, 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