JOURNAL OF COMBINATORIAL THEORY, Series B 37, 79–91 (1984)

Regular Subgraphs of Almost Regular Graphs

N. ALON*

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts

S. FRIEDLAND

Institute of Mathematics, Hebrew University of Jerusalem, Jerusalem, Israel

AND

G. KALAI*

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts

Communicated by the Managing Editors

Received July 25, 1983

Suppose every vertex of a graph G has degree k or $k+1$ and at least one vertex has degree $k+1$. It is shown that if $k \geqslant 2q-2$ and q is a prime power then G contains a q-regular subgraph (and hence an r-regular subgraph for all $r < q$, $r \equiv q \pmod 2$). It is also proved that every simple graph with maximal degree $\Delta \geqslant 2q-2$ and average degree $d > ((2q-2)/(2q-1))(\Delta+1)$, where q is a prime power, contains a q-regular subgraph (and hence an r-regular subgraph for all $r < q$, $r \equiv q \pmod 2$). These results follow from Chevalley's and Olson's theorems on congruences.

1. INTRODUCTION

In this paper we use the theorems of Chevalley [5] and Olson [9, 10] (and some extensions) on congruences, to prove the existence of regular subgraphs of certain graphs.

All graphs considered are finite, undirected, and contain no loops, unless otherwise stated. Note that we allow multiple edges. A *simple* graph is a graph without multiple edges.

* The contribution of these authors was supported in part by the Weizmann Fellowship for Scientific Research.

0095-8956/84 $3.00

582b/37/1-6

A graph H is *q-divisible* if q divides the degree of every vertex of H. Define $f(n, q)$ to be the maximal number of edges of a graph G on n vertices, that contains no nonempty q-divisible subgraph. In Section 3 we prove that

$$f(n, q) \leqslant (q-1)\, n,$$

provided q is an odd prime power. If q is a power of 2, then

$$f(n, q) \leqslant (q-1)\, n - q/2.$$

We further show that in both inequalities equality holds for all $n \geqslant 3$ and that a graph on $n \geqslant 3$ vertices and $e > f(n, q)$ edges contains at least $2^{e-f(n,q)} - 1$ nonempty q-divisible subgraphs. Note that for $q = 2$ this is just the well-known fact that the dimension of the cycle space of G is at least $e - n + 1$.

For $k < s$ a graph G is of *type* (k, s) if the degree $d(v)$ of every vertex of it satisfies $k \leqslant d(v) \leqslant s$ and G is not k-regular. In Section 4 we show that if q is a prime power, $q \geqslant r$, $q \equiv r \pmod 2$ and $k \geqslant 2q - 2$ then every graph G of type $(k, k+1)$ contains an r-regular subgraph. In particular:

Every 4-regular graph plus one edge contains a 3-regular subgraph. (1.1)

This result is closely related to a well-known conjecture of Berge and Sauer (see, e.g., [4, p. 246]) that asserts that every 4-regular *simple* graph has a 3-regular subgraph. Some positive results about this conjecture can be found in [6], and in [11] Taŝkinov announced that he verified it. However, the Berge–Sauer conjecture is false for graphs with parallel edges; (every graph obtained from an odd cycle by replacing every edge by two parallel edges forms a counterexample). Therefore, the "plus one edge" cannot be omitted in (1.1). A short derivation of (1.1) from Chevalley's theorem appears separately in [1].

In Section 4 we also show that if q is a prime-power, $q \geqslant r$ and $q \equiv r \pmod 2$ then every simple graph G with maximal degree $\Delta \geqslant 2q - 2$ and average degree $d > ((2q-2)/(2q-1))(\Delta + 1)$ contains an r-regular subgraph. In particular, every simple graph with maximal degree $\Delta \geqslant 4$ and average degree $d > \frac{4}{5}(\Delta + 1)$ contains a 3-regular subgraph. This result may help in solving a long standing problem of Erdös and Sauer (see, e.g., [2, p. 399, problem 20]). They asked for an estimation of the maximal number of edges of a simple graph on n vertices that contains no 3-regular subgraph.

Our paper is organized as follows. In Section 2 we describe the algebraic tools: we quote the theorem of Olson, show how it is related to the classical theorem of Chevalley, and obtain a simple corollary. In the Appendix we prove an extension of Olson's theorem and apply it to graph theory. Our proof is different from Olson's proof and is somewhat similar to the proof of

Chevalley's theorem given in [5]. In Section 3 we derive the results on q-divisible subgraphs and in Section 4 we combine these with known results of Petersen, Taŝkinov, Thomassen, Tutte, and Vizing to obtain our results on regular subgraphs.

2. The Algebraic Tools

Our main algebraic tool in this paper is the following result of Olson [9].

THEOREM 2.1 (Olson). *Let p be a prime and suppose $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n \geqslant 0$. For $1 \leqslant i \leqslant m$ let $a^{(i)} = (a_1^{(i)}, a_2^{(i)}, \ldots, a_n^{(i)})$ be a vector with integer coordinates. If*

$$m > \sum_{j=1}^{n} (p^{d_j} - 1)$$

then there exists a subset $\emptyset \neq I \subset \{1, 2, \ldots, m\}$ such that

$$\sum \{a_j^{(i)} : i \in I\} \equiv 0 \pmod{p^{d_j}}, \qquad j = 1, \ldots, n. \tag{2.1}$$

It is worth noting that for $d_1 = d_2 = \cdots = d_n = 1$ it is possible to derive this result from the classical theorem of Chevalley (see, e.g., [5]). Indeed consider the following system of polynomial equations

$$\sum_{i=1}^{m} a_j^{(i)} x_i^{p-1} \equiv 0 \pmod{p}, \qquad j = 1, \ldots, n.$$

Clearly $x_i = 0$ is a solution. Since the left-hand side of each equation is of degree $p-1$ at most, the Chevalley's theorem ensures a nontrivial solution if $m > (p-1)n$. As $x^{p-1} \equiv 1 \pmod{p}$ for $x \not\equiv 0 \pmod{p}$, the existence of a nontrivial solution implies the assertion of Theorem 2.1 in this case.

In the Appendix we prove a generalization of Olson's theorem. Our proof is different from Olson's proof and is somewhat similar to the proof of Chevalley's theorem given in [5].

COROLLARY 2.2. *Suppose $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n \geqslant 1$ and let p and $a^{(i)}$ $(1 \leqslant i \leqslant m)$ be as in Theorem 2.1. If*

$$\sum_{j=1}^{n} a_j^{(i)} \equiv 0 \pmod{p} \qquad \text{for} \quad i = 1, 2, \ldots, m$$

and

$$m > p^{d_n - 1} - 1 + \sum_{j=1}^{n-1} (p^{d_j} - 1)$$

then the conclusion of Theorem 2.1 *holds.*

Proof. For every $1 \leqslant i \leqslant m$, define a vector $b^{(i)} = (b_1^{(i)}, \ldots, b_n^{(i)})$ as follows: $b_j^{(i)} = a_j^{(i)}$ for $1 \leqslant j \leqslant n-1$ and $b_n^{(i)} = 1/p \sum_{j=1}^{n} a_j^{(i)}$. Applying Theorem 2.1 to the vectors $b^{(i)}$, we conclude that there exists a subset $\emptyset \neq I \subset \{1, \ldots, m\}$ such that

$$\sum \{a_j^{(i)} : i \in I\} = \sum \{b_j^{(i)} : i \in I\} \equiv 0 \pmod{p^{d_j}} \qquad \text{for } 1 \leqslant j \leqslant n-1,$$

and

$$\frac{1}{p} \sum \left\{ \sum_{j=1}^{n} a_j^{(i)} : i \in I \right\} = \sum \{b_n^{(i)} : i \in I\} \equiv 0 \pmod{p^{d_n - 1}},$$

i.e., $\sum \{\sum_{j=1}^{n} a_j^{(i)} : i \in I\} \equiv 0 \pmod{p^{d_n}}$. Since $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n$, we conclude that $\sum \{a_j^{(i)} : i \in I\} \equiv 0 \pmod{p^{d_j}}$ for all $1 \leqslant j \leqslant n$. ∎

It is worth noting that both Theorem 2.1 and Corollary 2.2 are best possible. Indeed, let $e^{(j)}$ be the standard vector $(\delta_{j1}, \ldots, \delta_{jn})$, $j = 1, \ldots, n$. A set of $p^{d_j} - 1$ copies of $e^{(j)}$ for $1 \leqslant j \leqslant n$ shows that Theorem 2.1 is best possible. A set of $p^{d_j} - 1$ copies of $e^{(j)} - e^{(n)}$ for $1 \leqslant j \leqslant n-1$ plus $p^{d_n - 1} - 1$ copies of $pe^{(n)}$ shows that Corollary 2.2 is best possible.

Theorem 2.1 and Corollary 2.2 can be used to prove the existence of one $\emptyset \neq I \subset \{1, 2, \ldots, m\}$ that satisfies (2.1). Combining them with the following proposition of Olson [10] we conclude that if m is large enough there are many such Is.

PROPOSITION 2.3 (Olson). *Let H be an abelian group and suppose that for every $h_1, \ldots, h_{g+1} \in H$ there exists a subset $\emptyset \neq I \subset \{1, \ldots, g+1\}$ such that*

$$\sum \{h_i : i \in I\} = 0. \tag{2.2}$$

If $h_1, \ldots, h_{g+l} \in H$ and $l \geqslant 1$, then there exist at least $2^l - 1$ distinct subsets I, $\emptyset \neq I \subset \{1, \ldots, g+l\}$ that satisfy (2.2).

3. q-DIVISIBLE SUBGRAPHS

Our main task in this section is to estimate the function $f(n, q)$ defined in Section 1. Recall that $f(n, q)$ is the maximum number of edges of a graph G

on n vertices that contains no nontrivial q-divisible subgraph. Clearly $f(n, 1) = 0$ and $f(n, 2) = n - 1$. The following theorem is an easy consequence of Theorem 2.1 and Corollary 2.2.

THEOREM 3.1.

$$\begin{aligned} f(n, q) &\leqslant (q-1) \cdot n && \text{if } q = p^d \text{ where } p \text{ is an odd prime} \\ &\leqslant (q-1) \cdot n - (q/2) && \text{if } q = 2^d. \end{aligned} \tag{3.1}$$

Proof. Suppose $q = p^d$, where p is an odd prime, and let $G = (V, E)$ be a graph with $|V| = n$ and $|E| = m > (q-1) \cdot n$. We must show that G contains a nontrivial q-divisible subgraph H.

For $v \in V$ and $e \in E$, define $a_v^{(e)} = 1$ if $v \in e$ and $a_v^{(e)} = 0$ otherwise. Put $V = \{v_1, v_2, \ldots, v_n\}$ and define, for $e \in E$, $a^{(e)} = (a_{v_1}^{(e)}, \ldots, a_{v_n}^{(e)})$. By Theorem 2.1 with $d_1 = d_2 = \cdots = d_n = d$ there exists a set E', $\emptyset \neq E' \subset E$ such that $\sum\{a_{v_j}^{(e)}; e \in E'\} \equiv 0 \pmod{q}$ for all $1 \leqslant j \leqslant n$. The graph $H = (V, E')$ is a nontrivial q-divisible subgraph of G. This proves the theorem for odd q. If $q = 2^d$, we use the same argument with Corollary 2.2 instead of Theorem 2.1. ∎

We now show that Theorem 3.1 is best possible for all $n \geqslant 3$. Define

$$\begin{aligned} g(n, k) &= (k-1) \cdot n && \text{if } k \text{ is odd,} \\ &= (k-1) \cdot n - (k/2) && \text{if } k \text{ is even.} \end{aligned}$$

For an odd integer $k > 1$ let $G_0(k)$ denote the Shannon triangle obtained from a triangle by replacing each edge by $k-1$ parallel edges. Similarly, for even k, let $G_0(k)$ be the graph obtained from a triangle by replacing two edges by $k-1$ parallel edges each and the third edge by $(k/2)-1$ parallel edges. For $n \geqslant 3$ let $G_k = (V_k, E_k)$ be a graph obtained from $G_0(k)$ by adding to it $n-3$ new vertices and joining each by $k-1$ edges to vertices of G_0. Clearly $|V_k| = n$ and $|E_k| = g(n, k)$. One can easily check that G_k contains no nontrivial k-divisible subgraph. Combining this with Theorem 3.1 we obtain

PROPOSITION 3.2. (i) *For $n \geqslant 3$ and every k, $f(n, k) \geqslant g(n, k)$.*

(ii) *If q is a prime power then $f(n, q) = g(n, q)$.*

There is some interest in considering separately the case of simple graphs. Thus we define $f_s(n, q)$ as the maximal number of edges of a simple graph G on n vertices that contains no nontrivial q-divisible subgraphs. Clearly $f_s(n, q) \leqslant f(n, q)$. The next proposition shows that for an odd prime power q and $n \geqslant q^2 - 1$ equality holds.

PROPOSITION 3.3. (i) *For every odd integer $k > 1$ and every $n \geqslant k^2 - 1$*

$$f_s(n, k) \geqslant g(n, k) = (k-1) \cdot n.$$

(ii) *If q is an odd prime power and $n \geqslant q^2 - 1$ then*

$$f_s(n, q) = g(n, q) = (q-1) \cdot n.$$

Proof. Part (ii) follows immediately from (i) and Theorem 3.1. To prove part (i) we construct a suitable example.

Let tG denote the disjoint union of t copies of the graph G. Let $G + H$ denote the join of the graphs G and H, i.e., the graph obtained from their disjoint union by joining each vertex of G to each vertex of H. Let E_{k-1} be the graph consisting of $k-1$ isolated vertices, let $K_{1,k-1}$ denote the star with $k-1$ edges and define

$$G_0 = E_{k-1} + (k-1) K_{1,k-1}.$$

Suppose $n \geqslant k^2 - 1$. Let $G = (V, E)$ be a graph obtained from G_0 by adding to it $n - (k^2 - 1)$ new vertices and joining each of them to $k-1$ vertices of G_0. One can easily check that $|V| = n$ and $|E| = (k-1) \cdot n$. In order to complete the proof we must show that G contains no nontrivial k-divisible subgraph. Clearly it is enough to show that G_0 contains no such graph. G_0 has vertices of three different types: let us call these of degree $k(k-1)$ vertices of type 1, these of degree $2k-2$- of type 2, and these of degree k- of type 3. Suppose G_0 has a nontrivial k-divisible subgraph $H = (V', E')$, where $d_H(v) > 0$ for all $v \in V'$.

We claim that V' contains all $k-1$ vertices of type 1. Indeed, otherwise V' contains no vertex of type 3 (since its degree in H is $< k$) and thus no vertex of type 2, which is impossible. Similar reasoning shows that if V' contains some vertex of type 3 then it must contain all its k neighbours, and in particular its unique neighbour of type 2. Let $x_1, x_2, \ldots, x_r$ $(r \leqslant k-1)$ be all the type 2 vertices in V' and let q_i be the number of type 3 vertices of H adjacent to x_i $(1 \leqslant i \leqslant r)$. Since each type 3 vertex in H is adjacent to all type 1 vertices we conclude that the degrees (in H) of any two type 1 vertices can differ by at most $r \leqslant k-1$. Since all degrees are divisible by k this shows that all these degrees are equal. Thus the number N of edges from the type 1 vertices to all other vertices of H is $0 \pmod{k(k-1)}$.

However, the degrees of all type 2 and type 3 vertices of H (in H) is exactly k. Therefore $N = \sum_{i=1}^{r}(k - q_i) + \sum_{i=1}^{r}(k-1) q_i$. Reducing modulo k we conclude that $-2 \sum_{i=1}^{r} q_i \equiv 0 \pmod{k}$ and since k is odd and $1 \leqslant q_i < k$ this implies that $\sum_{i=1}^{r} q_i = l \cdot k$ for some l, $0 < l < r \leqslant k-1$, which implies $\sum_{i=1}^{r} q_i \equiv l \pmod{k-1}$. Reducing the equation for N modulo $k-1$ (recall that $k-1 \mid N$) we conclude that $\sum_{i=1}^{r} q_i \equiv r \pmod{k-1} \not\equiv l \pmod{k-1}$, which is the desired contradiction. This completes the proof. ∎

By Proposition 3.2 if q is a prime power then $f(n, q) = g(n, q)$. The next theorem considers the extremal examples.

THEOREM 3.4. *Let $G = (V, E)$ be a graph with n vertices and $g(n, q)$ edges. Suppose G contains no nontrivial q-divisible subgraph. If q is an odd prime power, then for every integral vector $f = (f_1, \ldots, f_n) \neq 0$, G contains a subgraph H such that*

$$\deg_H(v_i) \equiv f_i \pmod{q} \qquad \text{for} \quad i = 1, \ldots, n. \tag{3.2}$$

If $q = 2^k$, (3.2) holds if $f_1 + \cdots + f_n$ is even.

Proof. Let $A = \{a^{(e)}, e \in E\}$ be the set of vectors defined in the proof of Theorem 3.1. Our theorem follows by applying Theorem 2.1 and Corollary 2.2 to the set of vectors $A \cup \{-f\}$ and by using the assumption that G contains no nontrivial q-divisible subgraph. ∎

Combining Theorem 2.1, Corollary 2.2, and Proposition 2.3 one can easily obtain the following stronger version of Theorem 3.1.

THEOREM 3.5. *If q is a prime power and G is a graph with n vertices and $e = g(n, q) + l$ edges, where $l \geqslant 1$, then G contains at least $2^l - 1$ nontrivial q-divisible subgraphs.* ∎

Note that since a 2-divisible subgraph is just an Eulerian-subgraph, for $q = 2$ the last theorem is the well-known fact that the dimension of the cycle space of G is at least $e - n + 1$.

Remark 3.6. Let $G = (V, E)$ be a directed graph. For $e \in E$ and $v \in V$ put $a_v^{(e)} = +1$ (-1) if e goes out of (into) v and $a_v^{(e)} = 0$ otherwise. If $V = \{v_1, \ldots, v_n\}$ define $a^{(e)} = (a_{v_1}^{(e)}, \ldots, a_{v_n}^{(e)})$. Since $\sum_{j=1}^{n} a_{v_j}^{(e)} = 0$, one can apply Theorem 2.1 to the vectors $(a_{v_1}^{(e)}, \ldots, a_{v_{n-1}}^{(e)})$ and show that if q is a prime power (even or odd) and $|E| > (q-1) \cdot (n-1)$, then G contains a subgraph H such that $q \mid d_H^+(v) - d_H^-(v)$ for all $v \in V$. This easily implies that every bipartite graph G with n vertices and more than $(q-1)(n-1)$ edges contains a nontrivial q-divisible subgraph.

We close this section with a conjecture.

Conjecture 3.7. For every $n \geqslant 3$ and every k

$$f(n, k) \leqslant (k-1) \cdot n.$$

4. Regular Subgraphs of Almost Regular Graphs

Recall the definition of a graph of type (k, s) given in Section 1. Here we prove the following.

THEOREM 4.1. *Let G be a graph of type $(k, k+1)$ and let r be an integer. If q is a prime power, $q \geqslant r$, $q \equiv r \pmod 2$, and $k \geqslant 2q-2$ then G contains an r-regular subgraph.*

THEOREM 4.2. *Let G be a graph of type $(k, k+2)$ and let r be an integer. If q is a prime power, $q \geqslant r$, $q \equiv r \pmod 2$, and $k \geqslant 2q-1$ then G contains an r-regular subgraph.*

Note that by Bertrand's postulate (for every r there is a prime between r and $2r$), Theorem 4.2 implies that if $k \geqslant 4r$ then every graph of type $(k, k+2)$ contains an r-regular subgraph. In fact, the known improvements of Bertrand's postulate (see, e.g., [2, p. xx]) enable one to show that Theorem 4.2 implies that for every $\varepsilon > 0$ if $r > r(\varepsilon)$ is *odd* and $k \geqslant (2+\varepsilon)r$ then every graph of type $(k, k+2)$ contains an r-regular subgraph. Shannon's triangle obtained by replacing each edge of a triangle by $r-1$ parallel edges shows that this is close to being best possible.

For simple graphs we prove

THEOREM 4.3. *If q is a prime power, $q \geqslant r$, and $q \equiv r \pmod 2$ then every simple graph G with maximal degree $\Delta \geqslant 2q-2$ and average degree $d > ((2q-2)/(2q-1))(\Delta+1)$ contains an r regular subgraph.*

These theorems are proved by combining Theorem 3.1 with results of Petersen, Taŝkinov, Thomassen, Tutte, and Vizing. In what follows we state these results and prove our theorems.

LEMMA 4.4 (Thomassen [12], a somewhat weaker version was proved by Tutte [13].). *Let G be a graph of type $(k, k+1)$ and suppose $0 \leqslant r < k$. Then G contains a spanning subgraph of type $(r, r+1)$.*

LEMMA 4.5 (Proved by Petersen [4, p. 75] for even k, and by Taŝkinov [11] for odd k.). *If $k \geqslant r$, $k \equiv r \pmod 2$, then every k regular graph contains an r regular subgraph.*

Proof of Theorem 4.1. By Lemma 4.4, G contains a (spanning) subgraph $L = (V, E)$ of type $(2q-2, 2q-1)$. Clearly $|E| > \frac{1}{2} \cdot |V|\ (2q-2) = (q-1) \cdot |V|$. Therefore, by Theorem 3.1, L contains a nontrivial q-divisible subgraph H. However, for every $v \in V$ $\deg_H(v) \leqslant \deg_L(v) \leqslant 2q-1$ and thus H is q regular. The result now follows from Lemma 4.5. ∎

For the proof of Theorem 4.2 we need

LEMMA 4.6. *Let G be a graph of type $(k, k+2)$ and suppose $0 \leqslant r \leqslant k-2$. Then G contains a spanning subgraph of type $(r, r+2)$ with average degree strictly greater than $r+1$.*

Outline of Proof. The proof is very similar to the proof of Thomassen [12] to Lemma 4.4. His argument easily shows that G contains a spanning subgraph L of type $(r+2, r+4)$. The same argument shows that L contains a spanning subgraph H of type $(r+1, r+3)$ with at least one vertex of degree $r+2$, and that H has a spanning subgraph of type $(r, r+2)$ with more vertices of degree $r+2$ than vertices of degree r. We omit the details. ∎

Proof of Theorem 4.2. By Lemma 4.6, G contains a (spanning) subgraph $L = (V, E)$ of type $(2q-3, 2q-1)$ with $|E| > (q-1)|V|$. This subgraph, as is shown in the proof of Theorem 4.1, contains an r-regular subgraph. ∎

For the proof of Theorem 4.3 we need the following well-known result of Vizing (see, e.g., [2, pp. 230–232]).

LEMMA 4.7 (Vizing). *The edges of every simple graph with maximal degree Δ can be covered by $\Delta+1$ disjoint matchings.*

Proof of Theorem 4.3. By Lemma 4.7 the edges of $G = (V, E)$ can be covered by $\Delta+1$ disjoint matchings. Let $L = (V, E')$ be the graph on V consisting of the edges of the $2q-1$ biggest matchings. Clearly

$$|E'| \geqslant \frac{2q-1}{\Delta+1}|E| = \frac{2q-1}{\Delta+1} \cdot \frac{1}{2} \cdot d \cdot |V|$$

$$> \frac{(2q-1)}{2(\Delta+1)} \frac{(2q-2)}{(2q-1)} (\Delta+1)|V| = (q-1)|V|.$$

By Theorem 3.1, L contains a nontrivial q-divisible subgraph H, which is, as in the proof of Theorem 4.1, q-regular. The result follows from Lemma 4.5. ∎

Remark 4.8. (a) We can slightly improve the constant $(2q-1)/(2q-2)$ in Theorem 4.3 but this makes the proof somewhat more complicated.

(b) Remark 3.6 and König's theorem (see, e.g., [4, p. 93, Theorem 6.1]) enables us to obtain the following improvement of Theorem 4.3 for bipartite graphs: If q is a prime power, $q \geqslant r$ then every bipartite graph G with maximal degree Δ and average degree $d \geqslant ((2q-2)/(2q-1))\Delta$ contains an r-regular subgraph.

(c) Combining the result of [8] with Theorem 4.2 one can easily prove the following:

Let G be a graph of type $(k, k+s)$ and let r be an integer. If q is a prime power, $q \geqslant r$, $q \equiv r \pmod 2$, $k \geqslant 2q-1$, and $s/k \leqslant 2/(2q-1)$, then G contains an r-regular subgraph.

APPENDIX

In this Section we prove a generalization of Olson's theorem (Theorem 2.1), and apply it to graph theory.

Let Z be the set of integers. For $S \subseteq Z$ and $m \in Z$, let $\mathrm{card}_m(S)$ denote the number of distinct elements in S modulo m. The main result in this section is

THEOREM A.1. *Let p be a prime and let $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n$ be n positive integers. For $1 \leqslant j \leqslant n$ let $S_j \subseteq Z$ be a set of integers containing 0. For $1 \leqslant i \leqslant m$ let $a^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)})$ be a vector with integer coordinates. If*

$$m > \sum_{j=1}^{n} (p^{d_j} - \mathrm{card}_p(S_j)),$$

then there exists a subset $\emptyset \neq I \subset \{1, 2, \ldots, m\}$ and numbers $s_j \in S_j$ $(1 \leqslant j \leqslant n)$ such that

$$\sum \{a_j^{(i)} : i \in I\} \equiv s_j \pmod{p^{d_j}} \quad \text{for} \quad 1 \leqslant j \leqslant n. \tag{A.1}$$

In order to prove the theorem, we need two simple lemmas.

LEMMA A.2. *Let P be a multilinear polynomial in m variables $x_1, \ldots, x_m$ over a ring R, (i.e., $P = \sum \{a_U \prod_{i \in U} x_i : U \subset \{1, 2, \ldots, m\}\}$ where $a_U \in R$). If $P(x_1, \ldots, x_m) = 0$ for all $x_i \in \{0, 1\}$, then $P \equiv 0$.*

Proof. The result follows easily by induction on m. ∎

For a prime power $q = p^d$, $y \in Z$, and $T \subseteq Z$, define

$$u(y, q, T) = \prod \{(y - i) \mid i : 0 \leqslant i < q \text{ and } i \not\equiv t \pmod q \text{ for all } t \in T\}.$$

$$c(q) = \sum_{k=0}^{d-1} (p^k - 1).$$

LEMMA A.3. *Let $q = p^d$ be a prime power. Let $T \subseteq Z$ satisfy $\mathrm{card}_p(T) = |T|$. If $c = c(q)$, then for every integer y, $p^c \mid u(y, q, T)$ and $p^{c+1} \nmid u(y, q, T)$ iff $y \equiv t \pmod q$ for some $t \in T$.*

Proof. Consider the product $Q = \prod \{(y - i) : 0 \leqslant i < q\}$. This is a product of p^d consecutive integers. Clearly, exactly p^{d-j} of them are divisible

by p^j $(1 \leqslant j \leqslant d)$; $u(y, q, T)$ is just the product Q without $|T|$ factors. Since $|T| = \text{card}_p(T)$ at most one of these missing factors is a multiple of p. Therefore, in the product $u(y, q, T)$ at least $p^{d-j} - 1$ elements are divisible by p^j $(1 \leqslant j \leqslant d)$ and thus $p^c \mid u(y, q, T)$. Obviously $p^{c+1} \nmid u(y, q, T)$ iff exactly $p^{d-j} - 1$ of these elements are divisible by p^j $(1 \leqslant j \leqslant d)$, i.e., iff no element is divisible by p^d. This happens iff one of the missing factors is a multiple of p^d, i.e., iff $y \equiv t \pmod q$ for some $t \in T$. ∎

Proof of Theorem A.1. For $1 \leqslant j \leqslant n$ put $q_j = p^{d_j}$ and define $c = \sum_{j=1}^{n} c(q_j)$. Assume the assertion of the theorem is false and let S_j $(1 \leqslant j \leqslant n)$ and $a^{(i)}$ $(1 \leqslant i \leqslant m)$ be a counterexample. For $1 \leqslant j \leqslant n$ let $T_j \subseteq S_j$ satisfy $0 \in T_j$ and $|T_j| = \text{card}_p(T_j) = \text{card}_p(S_j)$. Consider the polynomial with the m variables $\{x_i : 1 \leqslant i \leqslant m\}$

$$P = P(x_1, x_2, \ldots, x_m) = \prod_{j=1}^{n} u\left(\sum_{i=1}^{m} a_j^{(i)} x_i, q_j, T_j\right).$$

Since $0 \in T_j$, Lemma A.3 implies that $p^{c+1} \nmid P(0, 0, \ldots, 0)$. Suppose $x_i \in \{0, 1\}$ are not all zeros. Since $a^{(i)}$ and S_j do not satisfy (A.1), there exists an index $1 \leqslant j \leqslant n$ such that $\sum_{i=1}^{m} a_j^{(i)} x_i \not\equiv t \pmod{q_j}$ for all $t \in T_j$ and thus, by Lemma A.3 $p^{c+1} \mid P(x_1, \ldots, x_m)$. Therefore, if R is the ring of integers modulo p^{c+1} and P is considered as a polynomial over R, then if $x_i \in \{0, 1\}$ are not all zeros, then $P(x_1, \ldots, x_m) = 0$ (in R) and $P(0, 0, \ldots, 0) = P_0 \neq 0$. Let $\bar{P}$ be the multilinear polynomial obtained from P by changing every monomial $a_U \prod_{i \in U} x_i^{\delta_i}$ in the standard representation of P to $a_U \prod_{i \in U} x_i$. Clearly if $x_i \in \{0, 1\}$, then $P(x_1, \ldots, x_m) = \bar{P}(x_1, \ldots, x_m)$. Therefore the multilinear polynomial $\bar{P} - P_0 \prod_{i=1}^{m} (1 - x_i)$ satisfies the hypotheses of Lemma A.2 and thus $\bar{P} = P_0 \prod_{i=1}^{m} (1 - x_i)$. However, this is impossible since

$$\deg \bar{P} \leqslant \deg P \leqslant \sum_{j=1}^{n} (q_j - |T_j|) = \sum_{j=1}^{n} (q_j - \text{card}_p(S_j)) < m$$

$$= \deg\left(P_0 \prod_{i=1}^{m} (1 - x_i)\right).$$

This contradiction establishes the theorem. ∎

Using Theorem A.1 instead of Theorem 2.1 and Corollary 2.2, one can prove the following generalization of Theorem 3.1.

THEOREM A.4. *Let p be a prime, let $d_1, \ldots, d_n$ be positive integers and put $q_j = p^{d_j}$. For $1 \leqslant j \leqslant n$, let $S_j \subset Z$ be a set containing 0. Suppose $G = (V, E)$ is a graph with $V = \{v_1, \ldots, v_n\}$. If*

$$|E| > \sum_{j=1}^{n} (p^{d_j} - \text{card}_p(S_j)),$$

then G contains a nontrivial subgraph $H = (V, E')$ such that for $1 \leqslant j \leqslant n$,

$$\deg_H(v_j) \equiv s_j \pmod{q_j} \qquad \textit{for some} \quad s_j \in S_j.$$

We close the paper with the following conjecture that implies Conjecture 3.7.

Conjecture A.5. For $1 \leqslant i \leqslant m$, let $a^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)})$ be a vector with integer coordinates. Let k be a positive integer. If $m > (k-1)n$, then there exists a nonempty subset $I \subset \{1, \ldots, m\}$ such that

$$\sum \{a_j^{(i)} : i \in I\} \equiv 0 \pmod{k}$$

for $1 \leqslant j \leqslant n$.

Remark A.6. Baker and Schmidt [3] proved that the assertion of Conjecture A.5 holds if $m > c(k)\, n \cdot \log n$. This implies, of course, that $f(n, k) \leqslant c(k)\, n \cdot \log n$.

It is also worth noting that if $p_1, \ldots, p_n$ is a set of positive integers such that $p_j \mid p_{j-1}$ $(j = 2, \ldots, n)$, then it is possible that the system

$$\sum_{i=1}^{m} a_j^{(i)} x_i \equiv 0 \pmod{p_j}, \qquad j = 1, \ldots, n, x_i \in \{0, 1\},$$

will not have a nontrivial solution even if

$$m > \sum_{j=1}^{n} (p_j - 1).$$

See, for example, [7].

ACKNOWLEDGMENTS

We would like to thank N. Linial and R. Meshulam for fruitful discussions.

REFERENCES

1. N. ALON, S. FRIEDLAND, AND G. KALAI, Every 4-regular graph plus an edge contains a 3-regular subgraph, *J. Combin. Theory Ser. B* **37** (1984), 92–93.
2. B. BOLLOBÁS, "Extremal Graph Theory," Academic Press, New York, 1978.
3. R. C. BAKER AND W. M. SCHMIDT, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460–486.
4. J. A. BONDY AND U. S. R. MURTY, "Graph Theory with Applications," Macmillan & Co. London, 1976.

5. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Chap. 1, Academic Press, New York, 1966.
6. V. CHVÁTAL, H. FLEISCHNER, J. SHEEHAN, AND C. THOMASSEN, Three regular subgraphs of four regular graphs, *J. Graph Theory* **3** (1979), 371–386.
7. G. T. DIDERRICH AND H. B. MANN, Combinatorial problems in finite abelian groups, *in* "A Survey of Combinatorial Theory" (J. N. Srivastava *et al.*, Eds.), pp. 95–100, North-Holland, Amsterdam, 1973.
8. M. KANO AND A. SAITO, $[a, b]$ factors of graphs, *Discrete Math.* **47** (1983), 113–116.
9. J. E. OLSON, A combinatorial problem on finite abelian groups, *J. Number Theory* **1** (1969), 8–10.
10. J. E. OLSON, A combinatorial problem on finite abelian groups, II, *J. Number Theory* **1** (1969), 195–199.
11. V. A. TAŜKINOV, Regular subgraphs of regular graphs, *Soviet Math. Dokl.* **26** (1982), 37–38.
12. C. THOMASSEN, A remark on the factor theorems of Lovász and Tutte, *J. Graph Theory* **5** (1981), 441–442.
13. W. T. TUTTE, The subgraph problem, *Ann. Discrete Math.* **3** (1978), 289–295.