COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA 20 (4) (2000) 569–573

# ON A CONJECTURE OF KEMNITZ

LAJOS RÓNYAI[1]

Received August 23, 1999

A classic theorem of Erdős, Ginzburg and Ziv states that in a sequence of $2n-1$ integers there is a subsequence of length $n$ whose sum is divisble by $n$. This result has led to several extensions and generalizations. A multi-dimensional problem from this line of research is the following. Let $Z_n$ stand for the additive group of integers modulo $n$. Let $s(n,d)$ denote the smallest integer $s$ such that in any sequence of $s$ elements from $Z_n^d$ (the direct sum of $d$ copies of $Z_n$) there is a subsequence of length $n$ whose sum is 0 in $Z_n^d$. Kemnitz conjectured that $s(n,2)=4n-3$. In this note we prove that $s(p,2)\leq 4p-2$ holds for every prime $p$. This implies that the value of $s(p,2)$ is either $4p-3$ or $4p-2$. For an arbitrary positive integer $n$ it follows that $s(n,2)\leq(41/10)n$. The proof uses an algebraic approach.

## 1. Introduction

In 1961 Erdős, Ginzburg and Ziv [6] proved that in a sequence of $2n-1$ integers there is a subsequence of length $n$ whose sum is divisble by $n$. This result has led to several extensions and generalizations (see for example [2] and the survey paper [5]). A multi-dimensional problem from this line of research is to determine (estimate) the numbers $s(n,d)$ defined as follows. Let $Z_n$ denote the additive group of integers modulo $n$ and $s(n,d)$ be the smallest integer $s$ such that in any sequence of $s$ elements from $Z_n^d$ (the direct sum of $d$ copies of $Z_n$) there is a subsequence of length $n$ whose sum

*Mathematics Subject Classification (1991):* 11B50, 11P21

[1] Research supported in part by grants OTKA 030132, 27569, NWO-OTKA 048.011.002, FKFP 0612/1997 and AKP 98-19.

is 0 in $Z_n^d$. Harborth [7] proved that

$$(n-1)2^d+1 \le s(n,d) \le (n-1)n^d+1 \tag{1}$$

and that the lower bound in (1) is attained if either $d=1$; or $d=2$ and $n$ is of form $n=2^k3^l$. The inequalities in (1) are easy: in a sequence of $(n-1)n^d+1$ vectors form $Z_n^d$ one must appear at least $n$ times; as for the lower bound one can take a sequence consisting of $n-1$ copies of the 0,1-vectors from $Z_n^d$. Note that the Erdős-Ginzburg-Ziv Theorem can be formulated as $s(n,1)=2n-1$.

Alon and Dubiner [3] proved that $s(n,d)\le c(d)n$, where $c(d)$ is a constant independent of $n$. Their proof uses expansion properties of Cayley graphs and additive number theory.

Kemnitz [8] conjectured that the lower bound is sharp for $d=2$, i.e. that $s(n,2)=4n-3$, and verified it in the cases when the prime factors of $n$ are from the set $\{2,3,5,7\}$. In [2] Alon and Dubiner proved that $s(n,2)\le 6n-5$ and sketched an argument which gives $s(p,2)\le 5p-2$ for sufficiently large primes $p$.

The result of this note is the following.

**Theorem 1.1.** *For every prime $p$ we have $s(p,2)\le 4p-2$.*

This, together with the lower bound in (1) implies that the value of $s(p,2)$ is either $4p-3$ or $4p-2$. The proof is based on an algebraic technique developed mostly by Alon and his co-authors. In fact, our argument can be considered as an application of his beautiful Nonvanishing Theorem (Theorem 1.2 from [1]).

For an arbitrary positive integer $n$ the theorem implies that $s(n,2)\le (41/10)n$. This is certainly true if $n$ is prime or if the prime factors of $n$ are all less than 11. For a general $n$ one can proceed by induction on the number of primes dividing $n$: assume that $n=mp$, where $p\ge 11$ is a prime and $s(m,2)\le(41/10)m$. We use the inequality (cf. Harborth [7]) below:

$$s(mk,d)\le s(m,d)+m(s(k,d)-1).$$

We obtain that

$$s(mp,2)\le \frac{41}{10}m+m(4p-3)=\frac{11}{10}m+4mp\le\frac{mp}{10}+4mp=\frac{41}{10}mp.$$

## 2. The proof

We need the following easy fact about polynomial functions on Boolean hypercubes, which has had many applications in combinatorics (see for example Section 5.4 of [4], or [2]). We include a simple proof for the reader's convenience.

**Lemma 2.2.** *Let $F$ be a field and $m$ a positive integer. Then the (multilinear) monomials $\prod_{i\in I} x_i$, $I \subseteq \{1,2,\dots,m\}$ constitute a basis of the $F$-linear space of all functions from $\{0,1\}^m$ to $F$. (Here 0 and 1 are viewed as elements of $F$.)*

**Proof.** The monomials $\prod_{i\in I} x_i$, $I \subseteq \{1,2,\dots,m\}$ span a linear space of dimension $2^m$ over $F$. This is also the dimension of the space of functions from $\{0,1\}^m$ to $F$, therefore it suffices to verify that every function from the latter set can be expressed as an $F$-linear combination of the monomials $\prod_{i\in I} x_i$. The space of functions is clearly spanned by the characteristic functions $\chi_u$, $u \in \{0,1\}^m$, where $\chi_u(u)=1$ and $\chi_u(v)=0$ if $v \neq u$, hence it is enough to establish the required representation for characteristic functions. Write $u=(u_1,u_2,\dots,u_m)$ and let $U \subseteq \{1,2,\dots,m\}$ be the set of coordinate positions $j$ where $u_j=1$ and $\overline{U}$ be the set of indices $j$ with $u_j=0$. Then we have

$$\chi_u(x_1,x_2,\dots,x_m) = \prod_{j\in U} x_j \cdot \prod_{j\in \overline{U}} (1-x_j)$$

as functions on $\{0,1\}^m$. By expanding the right hand side we obtain an expression of the desired form. This proves the assertion. ∎

The following lemma was found by Alon and Dubiner ([2], Lemma 3.2). They proved it by using the Chevalley-Warning Theorem (see also the concluding remark).

**Lemma 2.3.** *Let $p$ be prime and*

$$v_1, v_2, \dots, v_{3p}$$

*be a sequence of vectors from $Z_p \oplus Z_p$ such that $\sum_{i=1}^{3p} v_i = (0,0)$. Then there is a subset $J$ of $\{1,2,\dots,3p\}$, $|J|=p$ such that $\sum_{j\in J} v_j = (0,0)$.* ∎

**Proof of the Theorem.** The assertion is obvious for $p=2$, hence we may assume that $p$ is an odd prime. Put $m=4p-2$.

Let

$$v_1 = (a_1,b_1), v_2 = (a_2,b_2), \dots, v_m = (a_m,b_m)$$

be a sequence of vectors from $Z_p \oplus Z_p$. We have to prove that there exists a subset $J$ of $\{1,2,\dots,m\}$, $|J|=p$ such that $\sum_{j\in J} v_j = (0,0)$.

Let $\sigma(x_1,x_2,\dots,x_m) := \sum_{I\subset\{1,2,\dots,m\},|I|=p} \prod_{i\in I} x_i$ denote the $p$-th elementary symmetric polynomial of the variables $x_1,x_2,\dots,x_m$. By Lemma 2.3 it is enough to prove that there is a subset $J$ of $\{1,2,\dots,m\}$, with $|J|=p$

or $|J| = 3p$ such that $\sum_{j\in J} v_j = (0,0)$. Assume for contradiction that this statement is false and consider the polynomial $P$ over the prime field $F_p$

$$P := \left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right)$$
$$\left(\left(\sum_{i=1}^{m} x_i\right)^{p-1} - 1\right)\left(\sigma(x_1,x_2,\ldots,x_m) - 2\right).$$

We claim that $F$ vanishes on all vectors $u\in\{0,1\}^m$, except on the all 0 vector $\mathbf{0}$, where $F(\mathbf{0}) = 2$. Indeed, the third factor vanishes on $u$ unless it has Hamming weight (the number of ones) divisible by $p$. If the Hamming weight of $u$ is $2p$ then $\sigma(u) = \binom{2p}{p} = 2$ in $F_p$, hence the last factor vanishes on $u$. Finally, if the Hamming weight of $u$ is $p$ or $3p$ then

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

is 0 on $u$ by the indirect hypothesis. We obtained that $P = 2\chi_{\mathbf{0}}$ as functions on $\{0,1\}^m$. Note also that $\deg P \le 3(p-1)+p = 4p-3$. Now reduce $P$ into a linear combination of multilinear monomials by using the relations $x_i^2 = x_i$ (which are valid on $\{0,1\}^m$), and let $Q$ denote the resulting expression. Clearly we have $Q = 2\chi_{\mathbf{0}}$ as functions on $\{0,1\}^m$ and $\deg Q \le 4p-3$, because reduction can not increase the degree. But this is in contradiction with the uniqueness part of Lemma 2.2, for the multilinear representative of $2\chi_{\mathbf{0}} = 2(1-x_1)(1-x_2)\cdots(1-x_m)$ has degree $m = 4p-2$. The contradiction establishes the Theorem. ∎

**Remark.** Lemma 2.3 can be proved in a way similar to the preceding argument. Put $m = 3p$, $v_i = (a_i, b_i)$ and just take the first three factors of $P$:

$$P' := \left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} x_i\right)^{p-1} - 1\right).$$

If the statement of the Lemma is false, then we can infer that $P' = -\chi_{\mathbf{0}} - \chi_{\mathbf{1}}$ and this leads to contradiction ($\deg P'$ is too small), as before. This, however, is merely a reformulation with Boolean variables of the original reasoning of Alon and Dubiner [2]. They employed variables ranging over $F_p$.

**Acknowledgement.** I thank Imre Z. Ruzsa for pointing out to me that Theorem 1.1 implies the general bound $s(n,2) \le (41/10)n$.

## References

[1] N. Alon: Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, **8** (1999), 7–29.

[2] N. Alon, M. Dubiner: Zero-sum sets of prescribed size, *Combinatorics, Paul Erdős is Eighty*, János Bolyai Math. Soc., Budapest, 1993, 33–50.

[3] N. Alon, M. Dubiner: A lattice point problem and additive number theory, *Combinatorica*, **15** (1995), 301–309.

[4] L. Babai, P. Frankl: *Linear algebra methods in combinatorics*, manuscript, September 1992.

[5] Y. Caro: Zero-sum problems — a survey, *Discrete Mathematics*, **152** (1996), 93–113.

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

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

[8] A. Kemnitz: On a lattice point problem, *Ars Combinatoria*, **16b**, (1983) 151–160.

Lajos Rónyai

*Computer and Automation Institute,*
*Hungarian Academy of Sciences*
*Budapest, Hungary*
lajos@nyest.ilab.sztaki.hu