

A talk given at the University of California at Irvine on Jan. 19, 2006.

A SURVEY OF ZERO-SUM PROBLEMS ON ABELIAN GROUPS

ZHI-WEI SUN

Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
zwsun@nju.edu.cn
<http://pweb.nju.edu.cn/zwsun>

ABSTRACT. Let G be a finite abelian group. A zero-sum problem on G asks for the smallest positive integer k such that for any sequence a_1, \dots, a_k of elements of G there exists a subsequence of required length the sum of whose terms vanishes. In this talk we will give a survey of problems and results in this field. In particular, we will talk about Olson's theorem on the Davenport constant of an abelian p -group, Reiher's celebrated proof of the Kemnitz conjecture, and the speaker's extension of the Erdős-Ginzburg-Ziv theorem involving covers of \mathbb{Z} .

1. BASIC CONCEPTS AND RESULTS ON ZERO-SUMS

Let G be an (additive) abelian group of order n . If $a_1, \dots, a_n \in G$, then by the pigeonhole principle the following elements (of G)

$$s_0 = 0, \quad s_1 = a_1, \quad s_2 = a_1 + a_2, \quad \dots, \quad s_n = a_1 + \dots + a_n$$

cannot be pairwise distinct, thus for some $0 \leq i < j \leq n$ we have

$$\sum_{i < r \leq j} a_r = s_j - s_i = 0.$$

If $a_1, \dots, a_{n^2-n+1} \in G$, then for some $a \in G$ the set $J = \{1 \leq i \leq n^2-n+1 : a_i = a\}$ has cardinality at least n , therefore for $I \subseteq J$ with $|I| = n$ we have $\sum_{i \in I} a_i = na = 0$. (Recall that $|G| = n$ and so the additive order of a divides n .)

of equations over F . Then p divides N , in particular $N \neq 1$.

Now we explain why the EGZ theorem holds when n is a prime. Let p be a prime and F be a field of order p . Let $a_1, \dots, a_{2p-1} \in F$,

$$f_1(x_1, \dots, x_{2p-1}) = \sum_{k=1}^{2p-1} x_k^{p-1} \text{ and } f_2(x_1, \dots, x_{2p-1}) = \sum_{k=1}^{2p-1} a_k x_k^{p-1}.$$

Note that $\deg f_1 + \deg f_2 < 2p - 1$ and $f_1(0, \dots, 0) = f_2(0, \dots, 0) = 0$. By the Chevalley-Warning theorem, there are $x_1, \dots, x_{2p-1} \in F$ such that

$$f_1(x_1, \dots, x_{2p-1}) = f_2(x_1, \dots, x_{2p-1}) = 0 \text{ and } I = \{1 \leq k \leq 2p - 1 : x_k \neq 0\} \neq \emptyset.$$

As $0 = f_1(x_1, \dots, x_{2p-1}) = \sum_{i \in I} x_i^{p-1} = |I|1$, we must have $p \mid |I|$ and hence $|I| = p$ since $0 < |I| < 2p$. Now that $f_2(x_1, \dots, x_{2p-1}) = 0$, we also have $\sum_{i \in I} a_i = 0$.

Observe that $S(\mathbb{Z}_n) = 2n - 1 = D(\mathbb{Z}_n) + n - 1$. In 1996 W. D. Gao [J. Number Theory, 58(1996)] proved that $S(G) = D(G) + |G| - 1$ for any finite abelian group G .

Davenport constants are named after H. Davenport who showed in 1966 that if K is an algebraic number field with ideal class group G , then $D(G)$ is the maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible integer in K . In 1969 Olson [J. Number Theory, 1969] used the knowledge of group rings to determine the Davenport constant of any abelian group of prime power order.

Olson's Theorem. *Let p be a prime and let G be an additive abelian p -group isomorphic to $\mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_r}}$. Let $a_1, \dots, a_k \in G$ with $k \geq 1 + \sum_{s=1}^r (p^{\alpha_s} - 1)$. Then there exists a nonempty $I \subseteq [1, k]$ such that $\sum_{i \in I} a_i = 0$, moreover for any $a \in G$ we have the congruence*

$$\sum_{\substack{I \subseteq [1, k] \\ \sum_{i \in I} a_i = a}} (-1)^{|I|} \equiv 0 \pmod{p}.$$

Olson's theorem essentially says that if p is a prime and $\alpha_1, \dots, \alpha_r \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ then

$$D(\mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_r}}) = 1 + \sum_{s=1}^r (p^{\alpha_s} - 1).$$

For, the sequence of elements of $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_r}}$ consisting of $p^{\alpha_1} - 1$ copies of $\langle 1, 0, \dots, 0 \rangle, \dots, p^{\alpha_r} - 1$ copies of $\langle 0, \dots, 0, 1 \rangle$, does not have a nonempty zero-sum subsequence.

Olson's theorem implies the EGZ theorem. In fact, if $a, a_1, \dots, a_{2p-1} \in \mathbb{Z}_p$ where p is a prime, then by Olson's theorem for \mathbb{Z}_p^2 we have

$$\left| \left\{ I \subseteq [1, 2p-1] : |I| = p \text{ and } \sum_{i \in I} a_i = a \right\} \right| \equiv \begin{cases} 1 \pmod{p} & \text{if } a = 0, \\ 0 \pmod{p} & \text{if } a \neq 0. \end{cases}$$

In 1994 W. R. Alford, A. Granville and C. Pomerance [Ann. Math.] employed an upper bound for the Davenport constant of the unit group of the ring \mathbb{Z}_n to prove that there are infinitely many Carmichael numbers which are those composites m such that $a^{m-1} \equiv 1 \pmod{m}$ for any $a \in \mathbb{Z}$ with $(a, m) = 1$.

2. AN ANALYSIS OF REIHER'S PROOF OF THE KEMNITZ CONJECTURE

What is the smallest integer $l = s(\mathbb{Z}_n^2)$ such that every sequence of l elements in $\mathbb{Z}_n^2 = \mathbb{Z}_n \oplus \mathbb{Z}_n$ contains a zero-sum subsequence of length n ?

In 1983 A. Kemnitz [Ars Combin.] posed the following conjecture.

Kemnitz's conjecture. *For any $a_1, \dots, a_{4n-3} \in \mathbb{Z}_n \oplus \mathbb{Z}_n$, there exists an $I \subseteq \{1, \dots, 4n-3\}$ with $|I| = n$ such that $\sum_{i \in I} a_i = 0$.*

Kemnitz's conjecture is equivalent to the equality $s(\mathbb{Z}_n^2) = 4n-3$ because $4n-3$ is the above conjecture cannot be replaced by a smaller number. In fact, let

$$\begin{aligned} a_1 = \dots = a_{n-1} &= (0, 0), & a_n = \dots = a_{2n-2} &= (0, 1), \\ a_{2n-1} = \dots = a_{3n-3} &= (1, 0), & a_{3n-2} = \dots = a_{4n-4} &= (1, 1), \end{aligned}$$

then there is no $I \subseteq \{1, \dots, 4n - 4\}$ with $|I| = n$ such that $\sum_{i \in I} a_i = (0, 0)$. The Kemnitz conjecture can be reduced to the case with n a prime.

In 1993 Alon and Dubiner showed that $s(\mathbb{Z}_n^2) \leq 6n - 5$. In 2000 Rónyai [Combinatorica] was able to prove that $s(\mathbb{Z}_p^2) \leq 4p - 2$ for every prime p ; in 2001 W. D. Gao [J. Combin. Theory Ser. A] used Olson's group ring approach to deduce that $s(\mathbb{Z}_q^2) \leq 4q - 2$ for any prime power q . All these results were obtained by various ingenious algebraic methods.

The following lemma plays an indispensable role in the study of the Kemnitz conjecture.

The Alon-Dubiner Lemma. *Let q be a prime power, and let a_1, \dots, a_{3q} be elements of \mathbb{Z}_q^2 with $a_1 + \dots + a_{3q} = 0$. Then there is an $I \subseteq [1, 3q]$ with $|I| = q$ such that $\sum_{i \in I} a_i = 0$.*

Let us recall a useful formula due to Zhi-Wei Sun which was motivated by Sun's study of covers of \mathbb{Z} and the polynomial method.

Theorem 2.1 [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003); arXiv:math.NT/0305369]. *Let R be a ring with identity, and let $f(x_1, \dots, x_k)$ be a polynomial over R . If $J \subseteq [1, k]$ and $|J| \geq \deg f$, then we have the formula*

$$\sum_{I \subseteq J} (-1)^{|J| - |I|} f([1 \in I], \dots, [k \in I]) = \left[\prod_{j \in J} x_j \right] f(x_1, \dots, x_k)$$

where $[x_1^{i_1} \dots x_k^{i_k}] f(x_1, \dots, x_k)$ denotes the coefficient of the monomial $x_1^{i_1} \dots x_k^{i_k}$ in the polynomial $f(x_1, \dots, x_k)$, and we let $[i \in I]$ be 1 or 0 according to whether $i \in I$ or not.

The EGZ theorem and Olson's theorem **are easy consequences of the above formula!**

By using the powerful formula and the Alon-Dubiner lemma, Sun [Electron.

Res. Announc. Amer. Math. Soc. 9(2003); [arXiv:math.NT/0305369](#)] obtained the following result concerning the Kemnitz conjecture.

Theorem 2.2 [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003), 51-60; [arXiv:math.NT/0305369](#)]. *Let p be a prime and let $h > 0$ be an integer. Let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \dots, 4p^h - 2$.*

(i) *Set $\mathcal{I} = \{I \subseteq [1, 4p^h - 2]: \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p^h}\}$. Then*

$$|\{I \in \mathcal{I}: |I| = p^h\}| \equiv |\{I \in \mathcal{I}: |I| = 3p^h\}| + 2 \pmod{p}.$$

(ii) *Suppose that*

$$\sum_{\substack{I, J \subseteq [1, 4p^h - 3] \\ |I| = |J| = p^h - 1 \\ I \cap J = \emptyset}} \left(\prod_{i \in I} a_i \right) \left(\prod_{j \in J} b_j \right) \not\equiv 2 \pmod{p}.$$

Then there exists an $I \subseteq [1, 4p^h - 3]$ with $|I| = p^h$ such that $\sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p^h}$.

In 2003 C. Reiher released a preprint “*On Kemnitz’s conjecture concerning lattice points in the plane*”, in which he completely proved the Kemnitz conjecture which had been open for 20 years! This work represents one of the most important achievements in the theory of zero-sums.

Reiher’s paper has 4 pages. Pages 1–3 are devoted to 5 sophisticated corollaries to the Chevalley-Warning theorem which are needed later. Actually this can be significantly simplified by using the first part of the above theorem with $a_{4p-2} = b_{4p-2} = 0$.

A Consequence of Theorem 2.2(i). *Let p be a prime and let $h > 0$ be an integer. Let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \dots, 4p^h - 3$. Set $\mathcal{I} = \{I \subseteq [1, 4p^h - 3]: \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p^h}\}$. Then*

$$\begin{aligned} & |\{I \in \mathcal{I}: |I| = p^h\}| + |\{I \in \mathcal{I}: |I| = p^h - 1\}| \\ & \equiv |\{I \in \mathcal{I}: |I| = 3p^h\}| + |\{I \in \mathcal{I}: |I| = 3p^h - 1\}| + 2 \pmod{p}. \end{aligned}$$

On the last page of his paper, C. Reiher provided a key lemma which is obtained by a combinatorial method rather than an algebraic method.

Reiher's Lemma. *Let p be a prime and let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \dots, 4p - 3$. Set*

$$\mathcal{I} = \left\{ I \subseteq [1, 4p - 3] : \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p} \right\}.$$

Then, either $\{I \in \mathcal{I} : |I| = p\} \neq \emptyset$ or

$$|\{I \in \mathcal{I} : |I| = p - 1\}| \equiv |\{I \in \mathcal{I} : |I| = 3p - 1\}| \pmod{p}.$$

Sketch of the Proof. For $J \subseteq [1, 4p - 3]$ and $n = 1, 2, \dots$ let

$$(n, J) := \left| \left\{ I \subseteq J : |I| = n \ \& \ \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p} \right\} \right|.$$

It is easy to show that if $|J| \in \{3p - 1, 3p - 2\}$ then $(2p, J) \equiv (p, J) - 1 \pmod{p}$.

Now assume that $\{I \in \mathcal{I} : |I| = p\} = \emptyset$, i.e., $(p, J) = 0$ for any $J \subseteq [1, 4p - 3]$.

Let N denote the number of partitions $[1, 4p - 3] = I_1 \cup I_2 \cup I_3$ satisfying

$$|I_1| = p - 1, \quad |I_2| = p - 2, \quad |I_3| = 2p$$

and furthermore

$$\sum_{i \in I_1} a_i \equiv \sum_{i \in I_1} b_i \equiv 0 \pmod{p}, \quad \sum_{i \in I_3} a_i \equiv \sum_{i \in I_3} b_i \equiv 0 \pmod{p}$$

(and hence $\sum_{i \in [1, 4p - 3] \setminus I_2} a_i \equiv \sum_{i \in [1, 4p - 3] \setminus I_2} b_i \equiv 0 \pmod{p}$). We count N in two ways. Observe that

$$N = \sum_{I_1} (2p, [1, 4p - 3] \setminus I_1) \equiv \sum_{I_1} (-1) = -(p - 1, [1, 4p - 3]) \pmod{p}.$$

On the other hand,

$$N = \sum_{I_2} (2p, [1, 4p - 3] \setminus I_2) \equiv \sum_{[1, 4p - 3] \setminus I_2} (-1) = -(3p - 1, [1, 4p - 3]) \pmod{p}.$$

So we have the congruence $(p - 1, [1, 4p - 3]) \equiv (3p - 1, [1, 4p - 3]) \pmod{p}$. \square

We remark that the prime power version of this lemma also holds.

Combining Reiher's Lemma, the Alon-Dubiner lemma and the above consequence of Theorem 2.2(i), we immediately obtain the following result of Reiher.

The Kemnitz-Reiher Theorem. *The Kemnitz conjecture is true.*

What does Reiher's solution teach us? When we apply a powerful algebraic method in combinatorics, we should also realize its disadvantage and should not forget combinatorial methods. **A combination of algebraic methods and combinatorial methods might be more powerful!**

3. FURTHER EXTENSIONS AND SOME OPEN PROBLEMS

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, let $a(n)$ represent the residue class

$$a + n\mathbb{Z} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

A finite system $A = \{a_s(n_s)\}_{s=1}^k$ of residue classes is said to be an m -cover of \mathbb{Z} (with $m \in \mathbb{Z}^+$) if $w_A(x) \geq m$ for all $x \in \mathbb{Z}$, where

$$w_A(x) = |\{1 \leq s \leq k : x \in a_s(n_s)\}|.$$

In 2003 Z. W. Sun established connections between covers of \mathbb{Z} and some classical theorems on zero-sums such as $D(\mathbb{Z}_m) = m$, the EGZ theorem, the Alon-Dubiner lemma and Olson's theorem. The following theorem in the case $n_1 = \dots = n_k = 1$ reduces to known results on zero-sums.

Theorem 3.1 [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003); arXiv:math.NT/0305369]. *Let $A = \{a_s(n_s)\}_{s=1}^k$ and let q be a prime power.*

(i) *If A forms a q -cover of \mathbb{Z} , then for any $m_1, \dots, m_k \in \mathbb{Z}$ there exists a nonempty $I \subseteq [1, k]$ such that $\sum_{s \in I} m_s/n_s \in q\mathbb{Z}$.*

(ii) *If $\{w_A(x) : x \in \mathbb{Z}\} \subseteq \{2q - 1, 2q\}$, then for any $c_1, \dots, c_k \in \mathbb{Z}_q$ there exists an $I \subseteq [1, k]$ such that $\sum_{s \in I} 1/n_s = q$ and $\sum_{s \in I} c_s = 0$.*

(iii) *If A is an exact $3q$ -cover of \mathbb{Z} , then for any $c_1, \dots, c_k \in \mathbb{Z}_q^2$ with $c_1 + \dots + c_k = 0$, there exists an $I \subseteq [1, k]$ such that $\sum_{s \in I} 1/n_s = q$ and $\sum_{s \in I} c_s = 0$.*

(iv) Let G be an additive abelian group of order q . Write $G \cong \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ with p a prime, and set $d(G) = 1 + \sum_{i=1}^r (p^{\alpha_i} - 1)$. Suppose that A is a $d(G)$ -cover of \mathbb{Z} . Then, for any $m_1, \dots, m_k \in \mathbb{Z}$ and $c_1, \dots, c_k \in G$, there is a nonempty $I \subseteq [1, k]$ such that $\sum_{s \in I} c_s = 0$ and $\sum_{s \in I} m_s/n_s \in \mathbb{Z}$.

The following conjecture of Zhi-Wei Sun seems very difficult.

Sun's Conjecture. *If we replace the prime power q in Theorem 3.1 by a general positive integer, and use $D(G)$ instead of $d(G)$ in part (iii), then the new version of Theorem 3.1 still holds.*

It seems that we cannot have a similar extension of the Kemnitz-Reiher theorem.

The following weighted EGZ theorem was conjectured by Y. Caro in the early 1990s and proved by D. Gryniewicz completely in 2005.

Theorem 3.2 [D. J. Gryniewicz, *Combinatorica*, to appear]. *Let w_1, \dots, w_m be integers with $w_1 + \cdots + w_m \equiv 0 \pmod{n}$ where $n \in \mathbb{Z}^+$. Then, for any $a_1, \dots, a_{m+n-1} \in \mathbb{Z}$ there are distinct $i_1, \dots, i_m \in [1, m+n-1]$ such that*

$$w_1 a_{i_1} + \cdots + w_m a_{i_m} \equiv 0 \pmod{n}.$$

When $m = n$ and $w_1 = \cdots = w_m = 1$, this reduces to the well-known EGZ theorem. Kneser's theorem on sumsets plays a central role in Gryniewicz's proof of Theorem 3.2. Before Gryniewicz's conclusive work, Theorem 3.2 was proved by N. Alon in the case $m = n = p$ with p a prime, by Y. O. Hamidoune [*Discrete Math.* 162(1996)] in the case where w_1, \dots, w_m are all relatively prime to n .

J. E. Olson gave an extension of the EGZ theorem to any finite group.

Theorem 3.3 [J. E. Olson, *J. Number Theory* 8(1976)]. *Let G be any additive group of order n . Then, for any $a_1, \dots, a_{2n-1} \in G$ there are distinct indices i_1, \dots, i_n such that $a_{i_1} + \cdots + a_{i_n} = 0$.*

Olson even conjectured that we can require further that the indices i_1, \dots, i_n are in increasing order.

Let $1 \leq k \leq n$, and let $f(n, k)$ be the least positive integer l such that if $a_1, \dots, a_l \in \mathbb{Z}_n$ and $|\{a_1, \dots, a_l\}| = k$ then $\sum_{i \in I} a_i = 0$ for some $I \subseteq [1, l]$ with $|I| = n$. By the EGZ theorem, $f(n, k) \leq 2n - 1$. To determine $f(n, k)$ is a subtle problem.

Theorem 3.4. *Let k and n be positive integers with $k \leq n$.*

(i) [Y. O. Hamidoune, O. Ordaz and A. Ortnno, *Combin. Probab. Comput.* 7(1998)] *We have $f(n, k) \leq 2n - k + 1$.*

(ii) [L. Gallardo, G. Grekos and J. Pihko, *Acta Arith.* 89(1999)] *If $n \geq 5$ and $1 + n/2 < k < n$ then $f(n, k) = n + 2$.*

(iii) [C. Wang, *Acta Arith.* 108(2003)] *If $k = 2m + 1 \geq 3$ is odd and $n \geq \max\{4m^2 - 4, m(m + 3)/2 + 2\}$, then $f(n, k) = 2n - m^2 - 1$. If $k = 2m \geq 3$ is even and $n \geq \max\{4m(m - 1) - 4, m(m + 1)/2 + 1\}$, then $f(n, k) = 2n - m(m - 1) - 1$.*

For the Davenport constant of a general finite abelian group, there are some known upper bounds.

Theorem 3.5. *Let G be a finite abelian group isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_r}$ with $1 < n_1 \mid n_2 \mid \dots \mid n_r$. (Thus, r is the rank of G and n_r is the exponent of G .)*

(i) [R. Meshulam, *Discrete Math.* 84(1990)] $D(G) \leq n_r(1 + \log(|G|/n_r))$.

(ii) [V. Dimitrov, 2003] $D(G) < (500r \log r)^r (1 + \sum_{i=1}^r (n_i - 1))$.

The Kemnitz-Reiher theorem indicates that $s(\mathbb{Z}_n^2) = 4n - 3$. What about $s(\mathbb{Z}_n^3)$? C. Elsholtz [*Combinatorica* 24(2004)] proved that $s(\mathbb{Z}_n^3) \geq 9n - 8$ for any odd $n > 1$. On the basis of this result, many zero-sum researchers (including the speaker) conjectured that $s(\mathbb{Z}_n^3) = 9n - 8$ for every odd integer $n = 3, 5, \dots$. (This seems very difficult.) In 2005 Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L.

Rackham showed that $S(\mathbb{Z}_n^4) \geq 20n - 19$ for all odd $n > 1$, and equality holds when n is a power of 3. C. Elsholtz [Combinatorica 24(2004)] proved that for $n = 3, 5, \dots$ and $k \geq 3$ we have

$$s(\mathbb{Z}_n^k) \geq 1.125^{\lfloor k/3 \rfloor} 2^k (n - 1) + 1;$$

on the other hand, Alon and Dubier [Combinatorica 15(1995)] showed that there is an absolute constant $M > 0$ such that

$$s(\mathbb{Z}_n^k) \leq (Mk \log_2 k)^k n \quad \text{for all } k, n \in \mathbb{Z}^+.$$

In 2005 A. Bialostocki posed the following interesting conjecture.

Bialostocki's Conjecture. *Let $n > 0$ be an even integer. If $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}_n$ and $a_1 + \dots + a_n = b_1 + \dots + b_n = 0$, then there is a permutation $\sigma \in S_n$ such that $\sum_{i=1}^n a_i b_{\sigma(i)} = 0$.*

The following conjecture is very challenging.

Olson's Conjecture. *For any $k, n \in \mathbb{Z}^+$ we have $D(\mathbb{Z}_n^k) = 1 + k(n - 1)$.*

The case $k = 1$ is trivial. J. E. Olson [J. Number Theory 1(1969)] confirmed the conjecture in the case where n is a prime power as well as the case $k = 2$. N. Alon, S. Friedland and G. Kalai [J. Combin. Theory Ser. B 37(1984)] mentioned the conjecture explicitly in their paper.