A talk given at the 3rd China-Japan Seminar on Number Theory (Xi'an, Feb. 13, 2004)

RECENT PROGRESS ON ZERO-SUM PROBLEMS AND SNEVILY'S CONJECTURE

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093, P. R. China
E-mail: zwsun@nju.edu.cn
Homepage: http://pweb.nju.edu.cn/zwsun

Abstract. This is a survey of recent advances on zero-sum problems and Snevily's conjecture concerning finite abelian groups. In particular, we will introduce Reiher's recent solution to the Kemnitz conjecture and our simplification.

1. On Zero-sum Problems

The theory of zero-sums began with the following celebrated theorem.

The Erdős-Ginzburg-Ziv Theorem [Bull. Research Council. Israel, 1961]. *For any $c_1, \cdots, c_{2n-1} \in \mathbb{Z}$, there is an $I \subseteq [1, 2n-1] = \{1, \cdots, 2n-1\}$ with $|I| = n$ such that $\sum_{i\in I} c_i \equiv 0 \pmod n$. In other words, given $2n-1$ (not necessarily distinct) elements of $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, we can select n of them with the sum vanishing.*

The EGZ theorem can be deduced from the well-known Chevalley-Warning theorem or the Cauchy-Davenport theorem.

For a finite abelian group G (written additively), the *Davenport constant* $D(G)$ is defined as the smallest positive integer l such that any

sequence $\{c_i\}_{i=1}^l$ (repetition allowed) of elements of G has a subsequence $c_{i_1},\cdots,c_{i_k}$ $(i_1<\cdots<i_k)$ with zero-sum (i.e. $c_{i_1}+\cdots+c_{i_k}=0$). In 1966 Davenport showed 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 used the knowledge of group rings to determine the Davenport constant of any abelian group of prime power order.

Olson's Theorem [J. Number Theory, 1969]**.** *Let p be a prime and let G be an additive abelian p-group isomorphic to $\mathbb{Z}_{p^{\alpha_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{\alpha_r}}$. Set $l=1+\sum_{s=1}^r(p^{\alpha_s}-1)$. Then for any $c_1,\cdots,c_l\in G$ there exists a nonempty $I\subseteq[1,l]$ with $\sum_{i\in I}c_i=0$.*

Over thirty years have passed, no one else can give an alternate proof of Olson's theorem without using group rings.

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 Kemnitz [Ars Combin.] conjectured that $s(\mathbb{Z}_n^2)=4n-3$, and the conjecture can be reduced to the case with n a prime. In 1993 Alon and Dubiner showed that $s(\mathbb{Z}_n^2)\leqslant 6n-5$. In 2000 Rónyai [Combinatorica] was able to prove that $s(\mathbb{Z}_p^2)\leqslant 4p-2$ for every prime p; in 2001 W. D. Gao [J. Combin. Theory Ser. A] used Olson's group ring approach to deduce that $s(\mathbb{Z}_q^2)\leqslant 4q-2$ 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 $c_1, \cdots, c_{3q}$ be elements of $\mathbb{Z}_q^2$ with $c_1 + \cdots + c_{3q} = 0$. Then there is an $I \subseteq [1, 3q]$ with $|I| = q$ such that $\sum_{i\in I} c_i = 0$.*

In March 2003 I found a powerful formula which implies both the EGZ theorem and Olson's theorem. From the formula I deduced the following result concerning the Kemnitz conjecture.

Theorem 1 [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 $i = 1, \cdots, 4p^h - 2$.*

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

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

(ii) *Suppose that*

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

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 a recent paper "*On Kemnitz's conjecture concerning lattice points in the plane*" by C. Reiher, the author completely proved the Kemnitz conjecture which had been open for 20 years! I'm much impressed by Reiher's cleverness, and I think his 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 Theorem 1(i) with $a_{4p-2}=b_{4p-2}=0$.

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

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

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 $i=1,\cdots,4p-3$. Set*

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

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

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

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

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

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 1(i), we immediately obtain the following result of Reiher.

Reiher's 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!**

By the way, I have established connections of the EGZ theorem, Olson's theorem and the Alon-Dubiner lemma to covering systems of $\mathbb{Z}$ by residue classes. But it seems that Reiher's theorem cannot be connected with covers of $\mathbb{Z}$.

2. On Snevily's Conjecture

Let $b_1,\cdots,b_n$ be (not necessarily distinct) elements of an additive abelian group G of order n. If both $\{a_i\}_{i=1}^n$ and $\{a_{\sigma(i)}+b_i\}_{i=1}^n$ are numberings of the elements of G (where σ belongs to the symmetric group S_n), then $\sum_{i=1}^n(a_{\sigma(i)}+b_i)=\sum_{i=1}^n a_i$ and hence $b_1+\cdots+b_n=0$. In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained the converse.

M. Hall's theorem. *Let $G=\{a_1,\cdots,a_n\}$ be an additive abelian group, and let $b_1,\cdots,b_n$ be elements of G with $b_1+\cdots+b_n=0$. Then there exists a permutation $\sigma\in S_n$ such that $a_{\sigma(1)}+b_1,\cdots,a_{\sigma(n)}+b_n$ are pairwise distinct.*

Hall's proof is highly technical. We cannot make a generalization by the special method.

Let n be a positive integer. If $\{a_1,\cdots,a_n\}$, $\{b_1,\cdots,b_n\}$ and $\{a_1+b_1,\cdots,a_n+b_n\}$ are all complete systems of residues modulo n, then

$$0+1+\cdots+(n-1)\equiv b_1+\cdots+b_n\equiv 0\ (\mathrm{mod}\ n)$$

and hence $2\nmid n$.

In 1999 H. S. Snevily [Amer. Math. Monthly] made the following interesting conjecture.

Snevily's Conjecture. *Let G be an additive abelian group with $|G|$ odd. Let A and B be subsets of G with cardinality $n > 0$. Then there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A and a numbering $\{b_i\}_{i=1}^n$ of the elements of B such that $a_1 + b_1, \cdots, a_n + b_n$ are pairwise distinct.*

To prove Snevily's conjecture for the additive group $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, Alon [Israel J. Math. 117(2000)] first showed that

$$\begin{aligned}&[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(x_j+b_j-(x_i+b_i))\\&=[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^2\neq 0\ \ (\text{in the field } \mathbb{Z}/p\mathbb{Z})\end{aligned}$$

(as usual $[x_1^{i_1}\cdots x_n^{i_n}]P(x_1,\cdots,x_n)$ denotes the coefficient of the monomial $x_1^{i_1}\cdots x_n^{i_n}$ in the polynomial $P(x_1,\cdots,x_n)$), and then employed the following famous Combinatorial Nullstellenstaz (CN Principle)

Combinatorial Nullstellenstaz [Alon, Comb. Probab. Comput. 1999]**.** *Let $k_1,\cdots,k_n$ be nonnegative integers and $A_1,\cdots,A_n$ be finite subsets of a field F with $|A_i| > k_i$ for $i = 1,\cdots,n$. If the coefficient of the monomial $x_1^{k_1}\cdots x_n^{k_n}$ in $f(x_1,\cdots,x_n) \in F[x_1,\cdots,x_n]$ is nonzero and $k_1+\cdots+k_n$ is the total degree of f, then there are $a_1 \in A_1,\cdots,a_n \in A_n$ such that $f(a_1,\cdots,a_n) \neq 0$.*

Q. H. Hou and I [Acta Arith. 102(2002)] obtained the following result further than the one of Alon: *If k, m, n are positive integers with $k - 1 \geqslant$*

$m(n-1)$, then

$$[x_1^{k-1}\cdots x_n^{k-1}](x_1+\cdots+x_n)^{(k-1-m(n-1))n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m}$$
$$=(-1)^{mn(n-1)/2}\frac{((k-1-m(n-1))n)!}{(m!)^n}\prod_{j=1}^n\frac{(jm)!}{(k-1-(j-1)m)!}.$$

Let $n>0$ be an odd integer. As $2^{\varphi(n)}\equiv 1\pmod n$, the multiplicative group of the finite field F with order $2^{\varphi(n)}$ has a cyclic subgroup of order n. This observation of Dasgupta, Károlyi, Serra and Szegedy enabled them to reduce Snevily's conjecture for cyclic groups of odd order to the following statement in view of Combinatorial Nullstellenstaz: *If F is a field of characteristic 2 and $b_1,\cdots,b_n$ are distinct elements of $F^*=F\setminus\{0\}$, then*

$$c:=[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(b_jx_j-b_ix_i)\neq 0.$$

In fact,

$$\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(b_jx_j-b_ix_i)=(-1)^{\binom{n}{2}}\|x_j^{n-i}\|_{1\leqslant i,j\leqslant n}\times\|b_j^{i-1}x_j^{i-1}\|_{1\leqslant i,j\leqslant n}$$
$$=(-1)^{\binom{n}{2}}\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)\prod_{i=1}^n x_{\sigma(i)}^{n-i}\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^n b_{\tau(i)}^{i-1}x_{\tau(i)}^{i-1}.$$

Therefore

$$\begin{aligned}(-1)^{\binom{n}{2}}c&=\sum_{\tau\in S_n}\prod_{i=1}^n b_{\tau(i)}^{i-1}\\&=\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^n b_{\tau(i)}^{i-1}\ \ (\text{because ch}(F)=2)\\&=\|b_j^{i-1}\|_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(b_j-b_i)\neq 0.\end{aligned}$$

This is exactly the way Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math. 126(2001)] proved Snevily's conjecture for cyclic groups with odd order.

By using some knowledge from Algebraic Number Theory (in particular, cyclotomic fields and Dirichlet's unit theorem), I [J. Combin. Theory Ser. A 103(2002)] was able to prove the following theorem.

Theorem 2 [Z. W. Sun, J. Combin. Theory Ser A 103(2002)]**.** *Let G be an additive abelian group whose finite subgroups are all cyclic. Let $b_1, \cdots, b_n$ be pairwise distinct elements of G, and let $A_1, \cdots, A_n$ be finite subsets of G with cardinality $k \geqslant m(n-1)+1$ where m is a positive integer.*

(i) *There are at least $(k-1)n - m\binom{n}{2} + 1$ multisets $\{a_1, \cdots, a_n\}$ such that $a_i \in A_i$ for $i = 1, \cdots, n$ and all the $ma_i + b_i$ are pairwise distinct.*

(ii) *If $b_1, \cdots, b_n$ are of odd order, then the sets*

$$\{\{a_1, \cdots, a_n\}: a_i \in A_i,\ a_i \neq a_j \text{ and } ma_i + b_i \neq ma_j + b_j \text{ if } i \neq j\}$$

and

$$\{\{a_1, \cdots, a_n\}: a_i \in A_i,\ ma_i \neq ma_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j\}$$

have more than $(k-1)n - (m+1)\binom{n}{2} \geqslant (m-1)\binom{n}{2}$ elements.

When G is a cyclic group with $|G|$ odd, our Theorem 2 (ii) in the case $k = n$ and $m = 1$, yields the main results of Dasgupta et al. In our opinion, the condition that all finite subgroups of G are cyclic might be omitted from Theorem 2.

Actually Theorem 2 follows from my stronger results on sumsets with polynomial restrictions.