A talk given at the Second East Asian Conf. Algebra & Combin. on Nov. 21, 2003.

HOW TO UNIFY COVERING SYSTEMS, RESTRICTED SUMSETS AND ZERO-SUM PROBLEMS?

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

1. Introduction to covering systems

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ we call

$$a(n) = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\}$$

a residue class with modulus n. As any integer can be written uniquely in the form $nq + r$ with $q \in \mathbb{Z}$ and $r \in R(n) = \{0, 1, \cdots, n-1\}$, the finite system $\{r(n)\}_{r=0}^{n-1}$ is a partition of $\mathbb{Z}$ (i.e., a disjoint cover of $\mathbb{Z}$). Can we cover all the integers with finitely many residue classes whose moduli are distinct? Such topics were initiated by the great mathematician Paul Erdős in the early 1930's.

For a finite system

$$A = \{a_s(n_s)\}_{s=1}^{k} \tag{1.1}$$

of residue classes, if $\bigcup_{s=1}^{k} a_s(n_s) = \mathbb{Z}$ then we call (1.1) a covering system of $\mathbb{Z}$, or a *cover* of $\mathbb{Z}$ in short. Clearly (1.1) forms a cover of $\mathbb{Z}$ if and only

if it covers $0, 1, \cdots, N_A - 1$, where N_A is the least common multiple of the moduli $n_1, \cdots, n_k$. If (1.1) covers every integer exactly once, then we call (1.1) an *exact* cover of $\mathbb{Z}$ or a disjoint cover of $\mathbb{Z}$.

Here are two early examples of covers with distinct moduli given by P. Erdős:

$$A_0 = \{0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)\},$$
$$A_1 = \{0(2),\ 0(3),\ 1(4),\ 3(8),\ 7(12),\ 23(24)\}.$$

(Note that $11(12) \subseteq 3(8) \cup 23(24)$.) In 1950 Erdős used A_1 to show that the residue class $2036812(5592405)$ contains *no* integers of the form $2^n + p$ where $n \in \mathbb{N} = \{0, 1, 2, \cdots\}$ and p is a prime. A simple nontrivial example of an exact cover is the system

$$A_3 = \{1(2),\ 2(2^2), \cdots,\ 2^{k-2}(2^{k-1}),\ 0(2^{k-1})\}$$

given by S. K. Stein in 1958.

Covers of $\mathbb{Z}$ have many surprising applications (e.g. $78557 \times 2^n + 1$ can never be a prime). Erdős was very proud of this invention, he said: *"Perhaps my favorite problem of all concerns covering systems."*

Soon after his invention of the concept of covering system, Erdős conjectured that *no cover (other than 0(1)) with distinct moduli can be exact*. This was confirmed by H. Davenport, L. Mirsky, D. Newman and R. Rado who showed independently that if (1.1) forms a disjoint cover of $\mathbb{Z}$ with

$$1 < n_1 \leqslant \cdots \leqslant n_{k-l} < n_{k-l+1} = \cdots = n_k \tag{1.2}$$

then $l \geqslant 2$ (i.e. $n_{k-1} = n_k$). In 1971 M. Newman [Math. Ann.] proved a conjecture of Š. Znám which asserts that l is not less than the smallest prime divisor of n_k for any exact cover (1.1) with (1.2).

For a positive integer m, (1.1) is said to be an *exact m-cover* if it covers each integer exactly m times. This concept was introduced by Š. Porubský [Acta Arith.] in 1976, he used the old term "m times covering systems of congruences". Porubský asked whether every exact m-cover is a union of m disjoint covers. Choi supplied the following exact 2-cover

$$\{1(2); 0(3); 2(6); 0, 4, 6, 8(10); 1, 2, 4, 7, 10, 13(15); 5, 11, 12, 22, 23, 29(30)\},$$

which is not a union of two exact covers. In 1991, using a graph-theoretic argument M. Z. Zhang proved that for each $m = 2, 3, \cdots$ there are infinitely many exact m-covers of $\mathbb{Z}$ which are not unions of an n-cover and an $(m-n)$-cover with $0 < n < m$.

As $a(n)$ is just a coset of the subgroup $n\mathbb{Z}$ of the additive group $\mathbb{Z}$, instead of covers of $\mathbb{Z}$ by residue classes one may study covers of an abstract group G by left cosets of subgroups. A basic result of B. H. Neumann [J. London Math. Soc. 1954] states that if the finite system

$$\mathcal{A} = \{a_i G_i\}_{i=1}^k \tag{1.3}$$

forms an irredundant cover of a group G by left cosets then all the indices $n_i = [G : G_i]$ are finite and $[G : \bigcap_{i=1}^k G_i] \leqslant c_k$ where c_k only depends on k. In 1987 M. J. Tomkinson [Comm. Algebra] showed further that one can take $c_k = k!$ and this is best possible. In 1974 M. Herzog and

J. Schönheim [Canad. Math. Bull.] conjectured that Erdős' conjecture can be extended to covers of groups (i.e., if (1.3) forms an exact cover of a group G then the indices $n_i = [G : G_i]$ cannot be pairwise distinct). Recently I [J. Algebra 273(2004)] made progress on the Herzog-Schönheim conjecture by proving that if (1.3) forms an exact m-cover of a group G with $k > 1$ and all the G_i subnormal in G then there are $1 \leqslant i < j \leqslant k$ such that $[G : G_i] = [G : G_j]$, actually I obtained many further results by a combined use of tools from group theory and number theory.

The *covering function* of system (1.1) is given by

$$w_A(x) = |\{1 \leqslant s \leqslant k\colon x \in a_s(n_s)\}|,$$

it is periodic modulo $N_A = [n_1, \cdots, n_k]$. One can easily verify the following equality:

$$\sum_{s=1}^{k} \frac{1}{n_s} = \frac{1}{N_A} \sum_{x=0}^{N_A-1} w_A(x). \tag{1.4}$$

For any cover (1.1) of $\mathbb{Z}$ we have the well-known inequality $\sum_{s=1}^{k} 1/n_s \geqslant 1$. In 1989, by using Riemann zeta function M. Z. Zhang showed further that if (1.1) is a cover of $\mathbb{Z}$ then $\sum_{s\in I} 1/n_s \in \mathbb{Z}^+$ for some $I \subseteq [1, k] = \{1, \cdots, k\}$. The stating point of Zhang is that (1.1) forms a cover of $\mathbb{Z}$ if any only if

$$\prod_{s=1}^{k} \left(1 - e^{2\pi i(n+a_s)/n_s}\right) = 0 \ \text{ for all } n = 1, 2, 3, \cdots.$$

In 1992 I [Israel J. Math.] proved that for any exact m-cover (1.1) of $\mathbb{Z}$ and $n = 0, 1, \cdots, m$ there are at least $\binom{m}{n}$ subsets I of $[1, k]$ with

$\sum_{s\in I}1/n_s=n$. The initial idea is that (1.1) forms an exact m-cover of $\mathbb{Z}$ if and only if we have the identity

$$\prod_{s=1}^k\left(1-r^{1/n_s}e^{2\pi ia_s/n_s}\right)=(1-r)^m\quad(r\geqslant 0).$$

In 1995 I [Acta Arith.] introduced m-covers of $\mathbb{Z}$ for the first time. (1.1) is called an *m-cover* of $\mathbb{Z}$ if it covers every integer at least m times. I observed that (1.1) covers an integer x at least m times if and only if

$$\prod_{s=1}^k\left(1-r^{1/n_s}e^{2\pi i(a_s-x)/n_s}\right)=o\left((1-r)^{m-1}\right)\ \text{ as } r\to 1,$$

and then used tools from analysis, linear algebra, number theory and combinatorics to obtain the first substantial characterization of m-covers.

Theorem 1.1 (Z. W. Sun, 1995)**.** (1.1) *forms an m-cover of $\mathbb{Z}$ if and only if we have*

$$\sum_{\substack{I\subseteq[1,k]\\ \{\sum_{s\in I}1/n_s\}=\theta}}(-1)^{|I|}\binom{\lfloor\sum_{s\in I}1/n_s\rfloor}{n}e^{2\pi i\sum_{s\in I}a_s/n_s}=0$$

for all $\theta\in[0,1)$ and $n=0,1,\cdots,m-1$.

By the way, the new approach made me obtained the following local-global result: *(1.1) forms an m-cover of $\mathbb{Z}$ if and only if it covers $|S(A)|$ consecutive integers at least m times where*

$$S(A)=\left\{\left\{\sum_{s\in I}\frac{1}{n_s}\right\}:I\subseteq[1,k]\right\}$$

and $\{\alpha\}$ stands for the fractional part of a real number α. This is stronger than a conjecture of P. Erdős which says that (1.1) is a cover of $\mathbb{Z}$ if it covers integers from 1 to 2^k.

Here are some results derived from Theorem 1.1 and its refinement.

Theorem 1.2. *Let* (1.1) *be an* m*-cover of* $\mathbb{Z}$ *and let* $m_1,\cdots,m_k\in\mathbb{Z}^+$.

(i) (Z. W. Sun, Trans. Amer. Math. Soc. 1996) *There are at least* m *positive integers in the form* $\sum_{s\in I}m_s/n_s$ *with* $I\subseteq[1,k]$.

(ii) (Z. W. Sun, Proc. Amer. Math. Soc. 1999) *If the residue class* $a_t(n_t)$ *is essential (i.e., with* $a_t(n_t)$ *omitted (1.1) will fail to be an* m*-cover of* $\mathbb{Z}$*), and* $(m_s,n_s)=1$ *for all* $s\in[1,k]\setminus\{t\}$*, then there is an* $\alpha_t\in[0,1)$ *such that*

$$\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}: I\subseteq[1,k]\setminus\{t\},\ \left\lfloor\sum_{s\in I}\frac{m_s}{n_s}\right\rfloor\geqslant m-1\right\}\supseteq\left\{\frac{\alpha_t+r}{n_t}: r\in R(n_t)\right\}.$$

I [Acta Arith. 1997; Combinatorica, 2003] also published some other results in this aspect.

Besides connections with unit fractions, there are many other directions concerning covers of $\mathbb{Z}$ and their generalizations. For problems and results in this field the reader may consult a recent survey of Š. Porubský and J. Schönheim [*Covering systems of Paul Erdős: Past, present and future*, 2002] reviewed by me for Math. Reviews.

2. Introduction to restricted sumsets and zero-sum problems

For a finite set $S=\{a_1,\cdots,a_k\}$ contained in the ring $\mathbb{Z}$ or a field, sums in the form $\sum_{s\in I}a_s$ with $I\subseteq[1,k]$ are called subset sums of S. It is interesting to provide a lower bound for the cardinality of the set

$$\{a_1x_1+\cdots+a_kx_k: x_1,\cdots,x_k\in\{0,1\}\}=\left\{\sum_{s\in I}a_s: I\subseteq[1,k]\right\}.$$

The classical Cauchy-Davenport theorem asserts that if X and Y are subsets of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (where p is a prime) then

$$|X+Y| \geqslant \min\{p, |X|+|Y|-1\}$$

where $X+Y = \{x+y: x \in X,\ y \in Y\}$. In 1964 Erdős and Heilbronn [Acta Arith.] conjectured that if p is a prime and $\emptyset \neq X \subseteq \mathbb{Z}_p$ then

$$|\{x+y: x,y \in X \text{ and } x \neq y\}| \geqslant \min\{p, 2|X|-3\}.$$

Until thirty years later this conjecture was first confirmed by Dias da Silva and Hamidoune [Bull. London Math. Soc.] in 1994, who obtained a generalization which implies that if $S \subseteq \mathbb{Z}_p$ and $|S| > \sqrt{4p-7}$ then any element of $\mathbb{Z}_p$ is a subset sum of S. Their main tool is the representation theory of groups. Soon after this, N. Alon, M. B. Nathanson and I. Z. Ruzsa [Amer. Math. Monthly 1995; J. Number Theory 1996] invented the so-called polynomial method to handle similar problems.

For a polynomial $f(x_1, \cdots, x_n)$ over a field, by $[x_1^{i_1} \cdots x_n^{i_n}] f(x_1, \cdots, x_n)$ we mean the coefficient of the monomial $x_1^{i_1} \cdots x_n^{i_n}$ in $f(x_1, \cdots, x_n)$.

ANR Lemma. *Let $X_1, \cdots, X_k$ be finite subsets of a field F with $|X_s| = h_s \in \mathbb{Z}^+$ for $s \in [1,k]$. If $P(x_1, \cdots, x_k) \in F[x_1, \cdots, x_k] \setminus \{0\}$ has degree not exceeding $\sum_{s=1}^k (h_s - 1)$ and*

$$[x_1^{h_1-1} \cdots x_k^{h_k-1}] P(x_1, \cdots, x_k)(x_1 + \cdots + x_k)^{\sum_{s=1}^k (h_s-1) - \deg P} \neq 0,$$

then

$$\left| \left\{ \sum_{s=1}^k x_s : x_s \in X_s \text{ and } P(x_1, \cdots, x_k) \neq 0 \right\} \right| \geqslant \sum_{s=1}^k (h_s - 1) - \deg P + 1.$$

The lemma actually depends on the following remarkable principle rooted in Alon and Tarsi [Combinatorics, 1989] and stated explicitly by Alon [Combin. Probab. Comput. 1999].

Combinatorial Nullstellenstaz. *Let $X_1,\cdots,X_k$ be finite subsets of a field F with $|X_s|>l_s$ for $s\in[1,k]$ where $l_1,\cdots,l_k\in\mathbb{N}=\{0,1,2,\cdots\}$. If $f(x_1,\cdots,x_k)\in F[x_1,\cdots,x_k]$, $[x_1^{l_1}\cdots x_k^{l_k}]f(x_1,\cdots,x_k)\neq 0$ and $\sum_{s=1}^k l_s$ is the total degree of f, then there are $x_1\in X_1,\cdots,x_k\in X_k$ such that $f(x_1,\cdots,x_k)\neq 0$.*

The first application of Combinatorial Nullstellenstaz is the following result concerning a conjecture of Jaeger.

Theorem 2.1 (Alon and Tarsi, 1989)**.** *Let F be a finite field with $|F|$ not a prime, and let M be a nonsingular $k\times k$ matrix over F. Then there exists a vector $\vec{x}\in F^k$ such that neither $\vec{x}$ nor $M\vec{x}$ has zero component.*

Another remarkable application of Combinatorial Nullstellenstaz is the following deep result [J. Combin. Theory Ser. B, 1984] in graph theory.

Theorem 2.2 (Alon, Friedland, Kalai, 1984)**.** *Let p be a prime, and let G be a loopless graph with average degree bigger than $2p-2$ and maximum degree at most $2p-1$. Then G has a p-regular subgraph.*

A recent application of Combinatorial Nullstellenstaz concerns a conjecture of H. S. Snevily.

Theorem 2.3 (Z. W. Sun, J. Combin. Theory Ser. A, 2003)**.** *Let G be an additive abelian group whose finite subgroups are all cyclic. Let $A_1,\cdots,A_n$*

$(n>1)$ be finite subsets of G with cardinality $k>m(n-1)$ where $m\in\mathbb{Z}^+$, and let $b_1,\cdots,b_n$ be pairwise distinct elements of G with odd order. Then there are more than $(k-1)n-(m+1)\binom{n}{2}$ sets $\{a_1,\cdots,a_n\}$ such that $a_1\in A_1,\cdots,a_n\in A_n$, and both $a_i\neq a_j$ and $ma_i+b_i\neq ma_j+b_j$ (or both $ma_i\neq ma_j$ and $a_i+b_i\neq a_j+b_j$) for all $1\leqslant i<j\leqslant n$.

This theorem extends a recent result of Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math. 2000] on Snevily's conjecture. Actually stronger results on sumsets with polynomial restrictions are obtained in my paper. My other results on restricted sumsets can be found in [Acta Arith. 1998, 2001, 2002; J. Number Theory 2002; J. Combin. Theory Ser. A 2002].

In 1961 Erdős, Ginzburg and Ziv [Bull. Research Council. Israel] established the following celebrated theorem and thus laid the foundation of the zero-sum theory.

Theorem 2.4 (The EGZ Theorem)**.** *For any $c_1,\cdots,c_{2n-1}\in\mathbb{Z}$, there is an $I\subseteq[1,2n-1]$ with $|I|=n$ such that $\sum_{s\in I}c_s\equiv 0\pmod n$. 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 easily reduced to the case where n is a prime (and hence $\mathbb{Z}_n$ is a field), and then deduced from the well-known Cauchy-Davenport theorem or the Chevalley-Warning theorem.

For a finite abelian group G (written additively), the *Davenport constant* $D(G)$ is defined as the smallest positive integer k such that any sequence $\{c_s\}_{s=1}^k$ (repetition allowed) of elements of G has a subsequence

$c_{i_1},\cdots,c_{i_l}$ $(i_1<\cdots<i_l)$ with zero-sum (i.e. $c_{i_1}+\cdots+c_{i_l}=0$). 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 [J. Number Theory] used the knowledge of group rings to show that the Davenport constant of an abelian p-group $G\cong\mathbb{Z}_{p^{h_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{h_l}}$ is

$$L(G)=1+\sum_{t=1}^{l}(p^{h_t}-1). \tag{2.1}$$

Theorem 2.5 (Olson, 1969)**.** *Let p be a prime and let G be an additive abelian p-group. Given $c,c_1,\cdots,c_{L(G)}\in G$ we have*

$$\sum_{\substack{I\subseteq[1,L(G)]\\ \sum_{s\in I}c_s=c}}(-1)^{|I|}\equiv 0\pmod p, \tag{2.2}$$

and in particular there exists a nonempty $I\subseteq[1,L(G)]$ with $\sum_{s\in I}c_s=0$.

Observe that the additive group of the finite field with p^l elements is isomorphic to $\mathbb{Z}_p^l$, the direct sum of l copies of the ring $\mathbb{Z}_p$.

Let p be a prime and $c,c_1,\cdots,c_{2p-1}\in\mathbb{Z}_p$. Olson's congruence (1.1) in the case $G=\mathbb{Z}_p^2$ yields that

$$\left|\left\{I\subseteq[1,2p-1]\colon |I|=p\text{ and }\sum_{s\in I}c_s=c\right\}\right|\equiv[c=0]\pmod p, \tag{2.3}$$

where for a predicate P we let $[P]$ be 1 or 0 according to whether P holds or not.

In 1994 Alford, Granville and 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.

What is the smallest integer $k = s(\mathbb{Z}_n^2)$ such that every sequence of k elements in $\mathbb{Z}_n^2$ contains a zero-sum subsequence of length n? In 1983 Kemnitz [Ars Combin.] conjectured that $s(\mathbb{Z}_n^2) = 4n-3$. 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 result to deduce that $s(\mathbb{Z}_q^2) \leqslant 4q-2$ for any prime power q.

3. A unified approach to the three topics

It seems that covers of $\mathbb{Z}$ have nothing to do with restricted sumsets in a field and zero-sum problems. Can you imagine that Theorems 2.1-2.2 and the EGZ theorem are related to covers of $\mathbb{Z}$?

Let (1.1) be an m-cover of $\mathbb{Z}$ and $P(x) \in \mathbb{C}[x]$ have degree less than m. As $P(x)$ can be written in the form $\sum_{n=0}^{m-1} c_n \binom{x}{n}$, by Theorem 1.1 for any $\theta \in [0,1)$ we have

$$\sum_{\substack{I\subseteq[1,k]\\ \{\sum_{s\in I} 1/n_s\}=\theta}} (-1)^{|I|} P\bigg(\sum_{s\in I}\frac{1}{n_s}\bigg) e^{2\pi i \sum_{s\in I} a_s/n_s} = 0,$$

that is,

$$\sum_{\substack{I\subseteq[1,k]\\ \{\sum_{s\in I} 1/n_s\}=\theta}} (-1)^{|I|} \bar{P}([1\in I],\cdots,[k\in I]) e^{2\pi i \sum_{s\in I} a_s/n_s} = 0$$

where $\bar{P}(x_1,\cdots,x_k) = P(\sum_{s=1}^k x_s/n_s)$.

Lemma 3.1 (Z. W. Sun, 1998-11-19). *Let $f(x_1,\cdots,x_k) \in \mathbb{C}[x_1,\cdots,x_k]$*

have degree not greater than $w_A(0)$ where A is as in (1.1). *Then*

$$\begin{aligned}&\sum_{I\subseteq[1,k]}(-1)^{|I|}f([1\in I],\cdots,[k\in I])e^{2\pi i\sum_{s\in I}a_s/n_s}\\&=\Big[\prod_{\substack{1\leqslant s\leqslant k\\ n_s\mid a_s}}x_s\Big]f(x_1,\cdots,x_k)(-1)^k\prod_{\substack{1\leqslant s\leqslant k\\ n_s\nmid a_s}}\left(e^{2\pi i a_s/n_s}-1\right).\end{aligned}\tag{3.1}$$

This lemma was first obtained by me dramatically in 1998, on March 7, 1999 I reproved it by a more direct method. As my new proof is somewhat similar to the proof of Combinatorial Nullstellenstaz, from that time I had believed that covers of $\mathbb{Z}$ may have connections with restricted sumsets. I also noted that the EGZ theorem and Zhang's result (which says that for any cover (1.1) there is a nonempty $I\subseteq[1,k]$ with $\sum_{s\in I}1/n_s\equiv 0\ (\mathrm{mod}\ 1)$) have the same flavor! So, covering systems, restricted sumsets and zero-sum problems might be unified by my intuition. This feeling became stronger with the time going on. I mentioned this feeling to my twin brother and Prof. Gao in 1999, and to Prof. Yeh (in Taiwan) in June 2002, and to Prof. Noga Alon during the ICM (Beijing 2002). But I was unable to disclose the mysterious connections.

In the case $n_1=\cdots=n_k=1$ the above lemma yields the identity

$$\sum_{I\subseteq[1,k]}(-1)^{k-|I|}f([1\in I],\cdots,[k\in I])=[x_1\cdots x_k]f(x_1,\cdots,x_k)$$

for any $f(x_1,\cdots,x_k)\in\mathbb{C}[x_1,\cdots,x_k]$ with $\deg f\leqslant k$. In 2001 when I saw Maltby's paper in [Rocky Mountain J. Math. 2000] I immediately realized that the above identity implies the so-called Escott's identity:

$$\sum_{I\subseteq[1,k]}(-1)^{|I|}\Big(\sum_{s\in I}c_s\Big)^n=0\quad\text{ for } n=0,1,\cdots,k-1.$$

But at that time I had no time to work further.

At the beginning of 2003, I wrote a manuscript on covers of $\mathbb{Z}$ containing Lemma 3.1 and its applications.

Theorem 3.1 (Z. W. Sun, 2003-01-15)**.** *Let R be a ring with identity, and let $f(x_1,\cdots,x_k)$ be a polynomial over R. If $J\subseteq[1,k]$ and $|J|\geqslant\deg f$, then we have the formula*

$$\sum_{I\subseteq J}(-1)^{|J|-|I|}f([1\in I],\cdots,[k\in I])=\left[\prod_{j\in J}x_j\right]f(x_1,\cdots,x_k). \tag{3.2}$$

On Jan. 21, 2003 I wrote that Theorem 3.1 should be very powerful and might have many applications despite of its simplicity. On that day I only noted that Theorem 3.1 implies the key lemma of Rónyai in his study of the Kemnitz conjecture.

On Feb. 8, 2003, my colleague Wu asked me the following question: Let p be a prime and F be a field with p elements. Is it true that for any $c_1,\cdots,c_{p-1}\in F\setminus\{0\}$ there is an $I\subseteq[1,p-1]$ with $\sum_{s\in I}c_s=1$? After two minutes' thinking I immediately got the positive answer. Let $X_1=\cdots=X_{p-1}=\{0,1\}$. We want to prove that there are $x_1\in X_1,\cdots,x_{p-1}\in X_{p-1}$ such that $\sum_{s=1}^{p-1}c_sx_s=1$, i.e., $f(x_1,\cdots,x_{p-1})=(\sum_{s=1}^{p-1}c_sx_s-1)^{p-1}-1\neq0$. As $[x_1\cdots x_{p-1}]f(x_1,\cdots,x_{p-1})=(p-1)!a_1\cdots a_{p-1}\neq0$, the desired result follows by applying Combinatorial Nullstellenstaz. Soon I realized that this also follows from Theorem 3.1 which implies Combinatorial Nullstellenstaz in the case $l_1,\cdots,l_k\in\{0,1\}$. The question is not difficult, but my answer taught me how to apply Theorem 3.1 with

a suitable f. This began a unified theory of the three topics, and I was fully absorbed in the unification during the rest of February.

On March 1 I finished the first version of a paper on the unification, but at that time I could only deal with zero-sum problems for elementary abelian p-groups. Olson's theorem for general abelian p-groups needs the tool of group rings, and no other proof had been found since 1969.

On April 16, 2003, I succeeded in deducing Olson's theorem from Theorem 3.1 by a fresh observation. Moreover, I got the following stronger result.

Theorem 3.2 (Z. W. Sun, 2003-04-17)**.** *Let $h_1,\cdots,h_l\in\mathbb{Z}^+$ and $k=\sum_{t=1}^l(p^{h_t}-1)$ where p is a prime. Let $c_{st},c_t\in\mathbb{Z}$ for all $s\in[1,k]$ and $t\in[1,l]$. Then*

$$\begin{aligned}&\sum_{\substack{I\subseteq[1,k]\\ p^{h_t}\mid\sum_{s\in I}c_{st}-c_t\ \text{for}\ t\in[1,l]}}(-1)^{|I|}\\ &\equiv\sum_{\substack{I_1\cup\cdots\cup I_l=[1,k]\\ |I_t|=p^{h_t}-1\ \text{for}\ t\in[1,l]}}\prod_{t=1}^l\prod_{s\in I_t}c_{st}\pmod p.\end{aligned}\tag{3.3}$$

Corollary 3.1. *Let p be a prime and let $h>0$ be an integer.*

(i) *If $c,c_1,\cdots,c_{p^h-1}\in\mathbb{Z}$, then*

$$\sum_{\substack{I\subseteq[1,p^h-1]\\ p^h\mid\sum_{s\in I}c_s-c}}(-1)^{|I|}\equiv c_1\cdots c_{p^h-1}\pmod p.\tag{3.4}$$

(ii) *For $c, c_1, \cdots, c_{2p^h-2} \in \mathbb{Z}$ we have*

$$\begin{aligned}&\left|\left\{I \subseteq [1, 2p^h-2]: |I| = p^h-1,\ p^h \ \Big|\ \sum_{s\in I} c_s - c\right\}\right| \\ &\equiv [x^{p^h-1}] \prod_{s=1}^{2p^h-2} (x - c_s) \pmod p.\end{aligned} \tag{3.5}$$

We can provide an advance on the Kemnitz conjecture by using Theorem 3.1.

Theorem 3.3 (Z. W. Sun, 2003)**.** *Let p be a prime and let $h > 0$ be an integer. Let $a_s, b_s \in \mathbb{Z}$ for $s = 1, \cdots, 4p^h - 3$. If*

$$\sum_{\substack{I,J\subseteq[1,4p^h-3]\\ |I|=|J|=p^h-1\\ I\cap J=\emptyset}} \Big(\prod_{i\in I} a_i\Big)\Big(\prod_{j\in J} b_j\Big) \not\equiv 2 \pmod p, \tag{3.6}$$

then there exists an $I \subseteq [1, 4p^h - 3]$ with $|I| = p^h$ such that $\sum_{s\in I} a_s \equiv \sum_{s\in I} b_s \equiv 0 \pmod{p^h}$.

We can also apply Theorem 3.1 to give a simple proof of a theorem of Baker and Schmidt [J. Number Theory 1980].

The following lemma can be viewed as a generalization of Lemma 3.1, it plays a key role in the unified theory.

Lemma 3.2 (Z. W. Sun, Feb. 2003)**.** *Let* (1.1) *be a system of residue classes, and let $m_1, \cdots, m_k$ be any integers. Let F be a field containing an element ζ of (multiplicative) order N_A, and let $f(x_1, \cdots, x_k) \in F[x_1, \cdots, x_k]$ and $\deg f \leqslant m(A) = \min_{z\in\mathbb{Z}} w_A(z)$. Set $I_z = \{1 \leqslant s \leqslant$*

$k\colon z\in a_s(n_s)\}$ *for* $z\in\mathbb{Z}$. *If* $[\prod_{s\in I_z}x_s]f(x_1,\cdots,x_k)=0$ *for all* $z\in\mathbb{Z}$, *then we have* $\psi(\theta)=0$ *for any* $0\leqslant\theta<1$ *where*

$$\psi(\theta)=\sum_{\substack{I\subseteq[1,k]\\ \{\sum_{s\in I}m_s/n_s\}=\theta}}(-1)^{|I|}f([1\in I],\cdots,[k\in I])\zeta^{N_A\sum_{s\in I}a_sm_s/n_s}.$$

The converse holds when $m_1,\cdots,m_k$ *are relatively prime to* $n_1,\cdots,n_k$ *respectively.*

On March 20 I submitted a research announcement of 10 pages to the managing editor of the **Electronic Research Announcements of Amer. Math. Soc.** which only accepts papers with *significant advance*. The paper was then sent to the editor R. L. Graham for further process.

On May 1, I sent e-mails to several famous number theorists or combinatorists to announce my discovery. Soon Prof. D. Zeilberger, A.S. Fraenkel, I.Z. Ruzsa, A. Granville and N. Alon replied my e-mail and showed their interests to my work. On May 4, 2003 a new web created by me with the title "*Covering Systems, Restricted Sumsets, Zero-sum Problems and Their Unification*" (or simply "**Covers, sumsets and zero-sums**") appeared via internat with the website `http://pweb.nju.edu.cn/zwsun/csz.htm`. On May 5, this was added to the Number Theory Web among the new listings. Up to now the unified theory web has been linked by 115 different websites including `Open Directory Project` and `Google Directory: Number Theory` with the sentence "**A unified approach to covering systems, restricted sumsets and zero-sum problems by Zhi-Wei Sun**".

On May 26 my full paper "*A unified theory of zero-sum problems, subset sums and covers of* $\mathbb{Z}$" was made public on the preprint server `arXiv:math.NT`.

On July 10, 2003 my paper "*Unification of zero-sum problems, subset sums and covers of* $\mathbb{Z}$" (Research announcement) was published by Electron. Res. Announc. Amer. Math. Soc. This is the first publication on the unification!

The general form of the main theorem of the unified theory is somewhat complicated. For the sake of clarity, here I state several consequences of the Main Theorem.

Theorem 3.4. *Let G be an additive abelian p-group where p is a prime. Suppose that (1.1) is an $L(G)+p^h-1$-cover of $\mathbb{Z}$ where $h\in\mathbb{N}$. Let $m_1,\cdots,m_k\in\mathbb{Z}$ and $c_1,\cdots,c_k\in G$. Then for any $c\in G$ and $\alpha\in\mathbb{Q}$ we have the congruence (within the ring of algebraic integers)*

$$\sum_{\substack{I\subseteq[1,k]\\ \sum_{s\in I}c_s=c\\ \sum_{s\in I}m_s/n_s\in\alpha+p^h\mathbb{Z}}}(-1)^{|I|}e^{2\pi i\sum_{s\in I}a_sm_s/n_s}\equiv 0\pmod p. \tag{3.7}$$

In particular, there is a nonempty $I\subseteq[1,k]$ such that $\sum_{s\in I}c_s=0$ and $\sum_{s\in I}m_s/n_s\in p^h\mathbb{Z}$.

Since a system of k copies of $0(1)$ forms a k-cover of $\mathbb{Z}$, Olson's theorem follows from Theorem 3.4 in the case $h=0$ and $n_1=\cdots=n_k=1$.

Theorem 3.4 in the case $|G|=1$, yields the following new extension of Zhang's result on covers of $\mathbb{Z}$.

Corollary 3.2. *Let* (1.1) *be an* m*-cover of* $\mathbb{Z}$*, and let* $m_1,\cdots,m_k\in\mathbb{Z}$*. If* $q\leqslant m$ *is a prime power (including* 1*), then for any* $J\subseteq[1,k]$ *there is an* $I\subseteq[1,k]$ *with* $I\neq J$ *such that* $\sum_{s\in I}m_s/n_s-\sum_{s\in J}m_s/n_s\in q\mathbb{Z}$*, in particular* $\sum_{s\in I}m_s/n_s\in q\mathbb{Z}$ *for some* $\emptyset\neq I\subseteq[1,k]$*.*

Corollary 3.2 suggests the following important extension of the basic fact $D(\mathbb{Z}_m)=m$.

Conjecture 3.1. *Let* (1.1) *be an* m*-cover of* $\mathbb{Z}$*. Then* $\sum_{s\in I}1/n_s\in m\mathbb{Z}^+$ *for some* $I\subseteq[1,k]$*. Moreover, for any* $m_1,\cdots,m_k\in\mathbb{Z}$ *and* $J\subseteq[1,k]$ *there is an* $I\subseteq[1,k]$ *with* $I\neq J$ *such that* $\sum_{s\in I}m_s/n_s-\sum_{s\in J}m_s/n_s\in m\mathbb{Z}$*.*

Part (i) of the following corollary gives a nice generalization of the EGZ theorem.

Corollary 3.3. *Let* (1.1) *be a system of residue classes, and let* q *be a prime power.*

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

(ii) *If* (1.1) *forms an exact* $3q$*-cover of* $\mathbb{Z}$*, then for any* $c_1,\cdots,c_k\in\mathbb{Z}_q^2$ *with* $c_1+\cdots+c_k=0$*, there exists an* $I\subseteq[1,k]$ *such that* $\sum_{s\in I}1/n_s=q$ *and* $\sum_{s\in I}c_s=0$*.*

Corollary 3.3 in the case $n_1=\cdots=n_k=1$ yields the EGZ theorem and a lemma of Alon and Dubiner. Corollary 3.3 (i) can be extended as follows: Let p be a prime and let $h\geqslant n\geqslant 0$ be integers. If $[p^n+p^h-1,2p^h]\supseteq\{w_A(x)\colon x\in\mathbb{Z}\}\neq\{2p^h\}$, then for any $c_1,\cdots,c_k\in\mathbb{Z}_{p^n}$ there exists an $I\subseteq[1,k]$ such that $\sum_{s\in I}1/n_s=p^h$ and $\sum_{s\in I}c_s=0$.

Conjecture 3.2. *The prime power q in Corollary 3.3 can be replaced by any positive integer.*

Now we apply Theorem 3.4 to strengthen the Alon-Friedland-Kalai result.

Corollary 3.4. *Let G be a loopless graph of l vertices with the edge set $\{1,\cdots,k\}$. Suppose that all the vertices of G have degree not more than $2p^n-1$ and that (1.1) forms an $l(p^n-1)+p^h$-cover of $\mathbb{Z}$, where p is a prime and $n,h\in\mathbb{N}$. Then for any $m_1,\cdots,m_k\in\mathbb{Z}$ we have*

$$\mathcal{H}=\left\{p^n\text{-regular subgraph } H \text{ of } G\colon \sum_{s\in E(H)}\frac{m_s}{n_s}\in p^h\mathbb{Z}\right\}\neq\emptyset \tag{3.8}$$

where $E(H)$ denotes the edge set of the subgraph H, furthermore

$$\sum_{H\in\mathcal{H}}(-1)^{|E(H)|}e^{2\pi i\sum_{s\in E(H)}a_sm_s/n_s}\equiv -1 \pmod p. \tag{3.9}$$

Corollary 3.4 in the case $h=0$ and $n_1=\cdots=n_k=1$ implies the the Alon-Friedland-Kalai result.

Theorem 3.5. *Let A be as in (1.1). Suppose that $m(A)=\min_{z\in\mathbb{Z}}w_A(z)<m(A')$ where $A'=\{a_1(n_1),\cdots,a_k(n_k),a(n)\}$, $a\in\mathbb{Z}$, $n\in\mathbb{Z}^+$ and $w_A(a)=m(A)$. Let $m_1,\cdots,m_k\in\mathbb{Z}$ be relatively prime to $n_1,\cdots,n_k$ respectively. Let $J\subseteq\{1\leqslant s\leqslant k\colon a\in a_s(n_s)\}$ and $P(x_1,\cdots,x_k)\in F[x_1,\cdots,x_k]$ where F is a field with characteristic not dividing N_A. Assume that $0\leqslant\deg P\leqslant|J|$ and*

$$\left[\prod_{j\in J}x_j\right]P(x_1,\cdots,x_k)(x_1+\cdots+x_k)^{|J|-\deg P}\neq 0.$$

Let $X_1=\{b_1,c_1\},\cdots,X_k=\{b_k,c_k\}$ be subsets of F such that $b_s=c_s$ only if $a\in a_s(n_s)$ and $s\notin J$. Then for some $0\leqslant\alpha<1$ we have

$$|S_r|\geqslant|J|-\deg P+1>0\quad\text{for all } r=0,1,\cdots,n-1 \tag{3.10}$$

where

$$S_r=\left\{\sum_{s=1}^k x_s\colon x_s\in X_s,\ P(x_1,\cdots,x_k)\neq 0,\ \left\{\sum_{\substack{s=1\\x_s\neq b_s}}^k\frac{m_s}{n_s}\right\}=\frac{\alpha+r}{n}\right\}. \tag{3.11}$$

When $n=n_1=\cdots=n_k=1$, Theorem 3.5 yields the ANR lemma in the case $h_1,\cdots,h_k\in\{1,2\}$.

Corollary 3.5. *Suppose that $\mathcal{A}=\{a_s(n_s)\}_{s=0}^k$ is an m-cover of $\mathbb{Z}$ with $a_0(n_0)$ essential. Let $m_1,\cdots,m_k\in\mathbb{Z}$ be relatively prime to $n_1,\cdots,n_k$ respectively. Let F be a field with characteristic p not dividing $N_{\mathcal{A}}$, and let $X_1=\{b_1,c_1\},\cdots,X_{k-1}=\{b_k,c_k\}$ be any subsets of F with cardinality 2. Then for some $0\leqslant\alpha<1$ we have*

$$\left|\left\{\sum_{s=1}^k x_s\colon x_s\in X_s,\ \left\{\sum_{\substack{1\leqslant s\leqslant k\\x_s=c_s}}\frac{m_s}{n_s}\right\}=\frac{\alpha+r}{n_0}\right\}\right|\geqslant\min\{p',m\} \tag{3.12}$$

for all $r\in[0,n_0-1]$, where $p'=p$ if p is a prime, and $p'=+\infty$ if $p=0$.

In the case $X_s=\{0,m_s/n_s\}$ $(1\leqslant s\leqslant k)$, Corollary 3.5 implies Theorem 1.2(ii).

Corollary 3.6. *Suppose that $\mathcal{A}=\{a_s(n_s)\}_{s=0}^k$ is a p-cover of $\mathbb{Z}$ with $a_0(n_0)$ essential, where p is a prime not dividing $N_{\mathcal{A}}$. Let $m_1,\cdots,m_k\in\mathbb{Z}$*

be relatively prime to $n_1,\cdots,n_k$ *respectively. Then, for any* $c,c_1,\cdots,c_k\in\mathbb{Z}_p$ *with* $c_1\cdots c_k\neq 0$ *the set*

$$\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}: I\subseteq[1,k-1]\ \textit{and}\ \sum_{s\in I}c_s=c\right\} \tag{3.13}$$

contains an arithmetic progression of length n_0 *with common difference* $1/n_0$.

This follows from Corollary 3.5 in the case $F=\mathbb{Z}_p$ and $X_s=\{0,c_s\}$.

Corollary 3.7. *Assume that* (1.1) *doesn't form an* $m+1$*-cover of* $\mathbb{Z}$ *but* $A'=\{a_1(n_1),\cdots,a_k(n_k),a(n)\}$ *does where* $a\in\mathbb{Z}$ *and* $n\in\mathbb{Z}^+$. *Let* $m_1,\cdots,m_k$ *be integers relatively prime to* $n_1,\cdots,n_k$ *respectively. Let* F *be a field of prime characteristic* p, *and let* $a_{ij},b_i\in F$ *for all* $i\in[1,m]$ *and* $j\in[1,k]$. *Set*

$$X=\left\{\sum_{j=1}^k x_j: x_j\in[0,p-1]\ \textit{and}\ \sum_{j=1}^k x_ja_{ij}\neq b_i\ \textit{for all}\ i\in[1,m]\right\}. \tag{3.14}$$

If p *does not divide* N_A *and the matrix* $(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant k}$ *has rank* m, *then the set*

$$S=\left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}: I\subseteq[1,k]\ \textit{and}\ |I|\in X\right\} \tag{3.15}$$

contains an arithmetic progression of length n *with common difference* $1/n$, *in particular when* $n=N_A$ *we have* $S=\{r/N_A: r\in[0,N_A-1]\}$.

The Alon-Tarsi result follows from Corollary 3.7 in the case $n_1=\cdots=n_k=n=1$.

Theorem 3.5 also implies the following result.

Theorem 3.6. *Let* (1.1) *be an* m*-cover of* $\mathbb{Z}$ *with* $a_k(n_k)$ *essential and* $n_k = N_A$*. Let* $m_1,\cdots,m_{k-1}\in\mathbb{Z}$ *be relatively prime to* $n_1,\cdots,n_{k-1}$ *respectively. Then for any* $r\in[0,N_A-1]$ *we have the inequality*

$$\left|\left\{I\subseteq[1,k-1]\colon\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\}=\frac{r}{N_A}\right\}\right|\geqslant 2^{m-1}. \tag{3.16}$$

Applying Theorem 3.6 to the trivial exact cover $\{r(n)\}_{r=0}^{n-1}$, we obtain

Corollary 3.8. *Let* $m_1,\cdots,m_{n-1}$ *be integers relatively prime to* n*. Then for any* $r=0,1,\cdots,n-1$ *there is an* $I\subseteq[1,n-1]$ *such that* $\sum_{s\in I}m_s\equiv r\pmod n$.

This result tells us that if $c_1,\cdots,c_{n-1}$ are generators of the additive cyclic group of order n then every element of the group can be written in the form $\sum_{s\in I}c_s$ with $I\subseteq[1,n-1]$.

My unified approach has pushed each of the three topics and led several new discoveries. To end this talk I should say that recently we have some further ideas which will be made public soon.