Abstract. In this survey I list some of my main results on the three topics (covering systems, restricted sumsets and zero-sum problems).

1. ON COVERING SYSTEMS

Let $M$ be an additive abelian group. A triple $(\lambda, a, n)$ with $\lambda \in M$, $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots \}$ and $a \in R(n) = \{0, 1, \ldots, n-1\}$, can be viewed as the residue class
\[ a(n) = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\} \quad (1.1) \]
associated with weight $\lambda$. For systems $\mathcal{A} = \{(\lambda_s, a_s, n_s)\}_{s=1}^k$ and $\mathcal{B} = \{\langle \mu_t, a_t, m_t \rangle\}_{t=1}^l$ of such triples, if
\[ \sum_{1 \leq s \leq k}^{x \in a_s(n_s)} \lambda_s = \sum_{1 \leq t \leq l}^{x \in b_t(m_t)} \mu_t \quad \text{for all } x \in \mathbb{Z}, \]
then we say that $\mathcal{A}$ is (covering) equivalent to $\mathcal{B}$ and write $\mathcal{A} \sim \mathcal{B}$ for this. A map $f : \bigcup_{n \in \mathbb{Z}^+} \mathbb{Z}/n\mathbb{Z} \to M$ is said to be equivalent if
\[ \sum_{j=0}^{n-1} f(a + jd + nd\mathbb{Z}) = f(a + d\mathbb{Z}) \quad \text{for any } a \in \mathbb{Z} \text{ and } d, n \in \mathbb{Z}^+. \quad (1.2) \]
We use $E(M)$ to denote the set of such equivalent maps.

The following fundamental theorem on covering equivalence was first announced in [Z. W. Sun, Adv. in Math. (China) 18(1989)] (with a complete proof submitted for reviews) and then proved in [Z. W. Sun, J. Algebra 240(2001)] with great details.
**Theorem 1.1** (Sun, 1989). For any function \( f : \bigcup_{n \in \mathbb{Z}^+} \mathbb{Z}/n\mathbb{Z} \to \mathbb{C} \), the following statements are equivalent:

(a) Whenever \( A = \{ \{ \lambda_s, a_s, n_s \} \}_{s=1}^k \) and \( B = \{ \{ \mu_t, b_t, m_t \} \}_{t=1}^l \) are equivalent with \( \lambda_s, \mu_t \in \mathbb{C} \), we have the equality

\[
\sum_{s=1}^k \lambda_s f(a_s + n_s \mathbb{Z}) = \sum_{t=1}^l \mu_t f(b_t + m_t \mathbb{Z}).
\] (1.3)

(b) \( f \) is an equivalent function, i.e., \( f \in E(\mathbb{C}) \).

(c) \( f \) has the following form:

\[
f(a + n\mathbb{Z}) = \frac{1}{n} \sum_{m=0}^{n-1} \psi \left( \frac{m}{n} \right) e^{2\pi i \frac{ma}{n}} \ (a \in \mathbb{Z} \text{ and } n \in \mathbb{Z}^+)
\] (1.4)

where \( \psi \) is a function from \( \mathbb{Q} \cap [0, 1) \) to \( \mathbb{C} \).

**Remark 1.1.** Let \( M \) be an additive abelian group. A map \( F \) to \( M \) with \( \text{Dom}(F) \subseteq \mathbb{C} \times \mathbb{C} \) is said to be uniform if for any \( \langle x, y \rangle \in \text{Dom}(F) \) and \( n \in \mathbb{Z}^+ \) we have \( \{ \langle (x + r)/n, ny \rangle : r \in R(n) \} \subseteq \text{Dom}(F) \) and

\[
\sum_{r=0}^{n-1} F \left( \frac{x + r}{n}, ny \right) = F(x, y).
\] (1.5)

If \( F \) is uniform, then for any \( \langle x, y \rangle \in \text{Dom}(F) \) the function \( f(a + n\mathbb{Z}) = F((x + a)/n, ny) \ (a \in R(n)) \) is equivalent. Conversely, if \( f \in E(M) \) then the function \( F(x, y) = f(xy + y\mathbb{Z}) \) (where \( \langle x, y \rangle \in \text{Dom}(F) \) if \( y \in \mathbb{Z}^+ \) and \( xy \in \mathbb{Z} \)) is uniform. In view of this, the equivalence of (a) and (b) was proved in [Z. W. Sun, Nanjing Univ. J. Math. Biquarterly 6(1989)] via uniform functions introduced there. In 1989 Sun also pointed out several examples of uniform functions such as \( \lfloor x \rfloor \) and \( y^{m-1} B_m(x) \) with \( M = \mathbb{C} \), and \( 2\sin \pi x \) and \( \Gamma^*(x, y) = \Gamma(x) y^{x-1/2}/\sqrt{2\pi} \) with \( M = \mathbb{C}^* = \mathbb{C} \setminus \{0\} \).

(Thus J. Beebee [Proc. Amer. Math. Soc. 112(1991), 120(1994)] partly repeated Sun’s earlier work.) For more uniform functions see [Z. W. Sun, Acta Arith. 97(2001)] and [Z. W. Sun, On covering equivalence, 2002]. When \( F(x, y) = g(x)h(y) \), the equation (1.5) yields the so-called generalized Kubert identity which has been investigated by many mathematicians.

**Theorem 1.2** (Local-Global Theorem). (i) [Sun, Acta Arith. 72(1995); Trans. Amer. Math. Soc. 348(1996)] Let \( A = \{ a_s(n_s) \}_{s=1}^k \) and let \( m_1, \ldots, m_k \in \mathbb{Z} \) be relatively prime to \( n_1, \ldots, n_k \) respectively. Then \( A \) covers all the integers at least \( m \) times if it cover \( |S| \) consecutive integers at least \( m \) times, where

\[
S = \left\{ \left\lfloor \sum_{s \in I} \frac{m_s}{n_s} \right\rfloor : I \subseteq [1, k] = \{1, \ldots, k\} \right\}
\] (1.6)
and \( \{\alpha\} \) denotes the fractional part of real number \( \alpha \).

(ii) [Z. W. Sun, arXiv:math.NT/0404137; Math. Res. Lett. 11(2004)] Let \( \psi_1, \ldots, \psi_k \) be maps from \( \mathbb{Z} \) to an abelian group with respective periods \( n_1, \ldots, n_k \in \mathbb{Z}^+ \). Then \( \psi = \psi_1 + \cdots + \psi_k \) is constant if \( \psi(x) \) equals a constant for \( |T| \) consecutive integers \( x \) where

\[
T = \bigcup_{s=1}^{k} \left\{ \frac{r}{n_s} : r = 0, \ldots, n_s - 1 \right\}.
\]  

(1.7)

In particular, \( A = \{a_s(n_s)\}_{s=1}^k \) covers all the integers exactly \( m \) times if it covers consecutive \( |T| \) integers exactly \( m \) times.

Remark 1.2. In the 1960’s P. Erdős conjectured that \( A = \{a_s(n_s)\}_{s=1}^k \) forms a cover of \( \mathbb{Z} \) if it covers integers from 1 to \( 2^k \). This was confirmed by R. B. Crittenden and C. L. Vanden Eynden [Proc. Amer. Math. Soc. 24(1970)] in a very complicated way. Theorem 1.2 (i) is better than this because \( |S| \leq 2^k \) depends on the moduli \( n_1, \ldots, n_k \) rather than the number of the moduli.

Theorem 1.3. Let \( A = \{a_s(n_s)\}_{s=1}^k \) and \( w(x) = \sum_{s \in I_s} \lambda_s \), where \( \lambda_s \in \mathbb{C} \) and \( I_s = \{1 \leq s \leq k : x \in a_s(n_s)\} \).

(i) [Z. W. Sun, Chin. Quart. J. Math. 6(1991)] Let \( n_0 \in \mathbb{Z}^+ \) be the smallest period of the function \( w(x) \). If \( d \in \mathbb{Z}^+ \) does not divide \( n_0 \) and \( \sum_{d|n_s} \lambda_s/n_s \neq 0 \), then

\[
|\{a_s \mod d : 1 \leq s \leq k \, \& \, d \mid n_s\}| \geq \min_{0 \leq s \leq k} \frac{d}{(d, n_s)} \geq p(d) \tag{1.8}
\]

where \( p(d) \) is the least prime divisor of \( d \). In particular, if \( n_1 \leq \cdots \leq n_k-1 < n_{k-1+1} = \cdots = n_k \) and \( n_{k} \mid n_{0} \), then

\[
l \geq \min_{0 \leq s \leq k-l} \frac{n_k}{(n_s, n_k)} \geq p(n_k). \tag{1.9}
\]

(ii) [Z. W. Sun, J. Number Theory 111(2005), 190-196] Let \( n_0 \in \mathbb{Z}^+ \) be the smallest positive period of \( w(x) \mod m \in \mathbb{Z} \). Suppose that \( d \in \mathbb{Z}^+ \) does not divide \( n_0 \) but \( I(d) = \{1 \leq s \leq k : d \mid n_s\} \neq \emptyset \). If \( \lambda_1, \ldots, \lambda_k \in \mathbb{Z} \), and \( m \) does not divide \([n_1, \ldots, n_k] \sum_{s \in I(d)} \lambda_s/n_s\), then (1.8) also holds. Consequently, if \( k > 1 \) and \( n_1, \ldots, n_k \) are distinct, then \( |I_x| : x \in \mathbb{Z} \) is not contained in any residue class with modulus greater one.

Remark 1.3. (i) Let \( A = \{a_s(n_s)\}_{s=1}^k \) be an exact \( m \)-cover (i.e. \( A \) covers every integer exactly \( m \) times) with \( n_1 \leq \cdots \leq n_{k-l} < n_{k-l+1} = \cdots = n_k \).
Then \( l \geq \min_{1 \leq s \leq k-l} n_k/(n_s, n_k) \) by Theorem 1.3. This lower bound for \( l \) is essentially the best one. In the case \( m = 1, l > 1 \) was proved by H. Davenport, L. Mirsky, D. Newman and R. Radó, and the inequality \( l \geq p(n_k) \) was first conjectured by Š. Znám (1969) and then confirmed by M. Newman [Math. Ann. 191(1971)]. A \( n \)-dimensional version of Theorem 1.3(i) was given by Z. W. Sun [Math. Res. Lett. 11(2004)]

(ii) Let \( A = \{a_s(n_s)\}_{s=1}^k \) be a cover of \( \mathbb{Z} \) with \( 1 < n_1 < \cdots < n_k \). By Theorem 1.3(ii), \( A \) cannot cover every integer an odd number of times. It is interesting to compare this with a famous conjecture of P. Erdős and J. L. Selfridge which asserts that \( n_1, \ldots, n_k \) cannot be all odd.

**Theorem 1.4** [Z. W. Sun, arXiv:math.NT/0403271]. Let \( \{a_s(n_s)\}_{s=0}^k \) cover every integer more than \( m = \lfloor \sum_{s=1}^k 1/n_s \rfloor \) times, where \( \lfloor \alpha \rfloor \) denotes the greatest integer not exceeding real number \( \alpha \).

(i) For any \( a = 0, 1, 2, \cdots \) we have

\[
\left| \left\{ I \subseteq [1, k] : \sum_{s \in I} \frac{1}{n_s} = \frac{a}{n_0} \right\} \right| \geq \binom{m}{\lfloor a/n_0 \rfloor}.
\]  

(ii) Assume that \( J \subseteq [1, k] \) and

\[
\left\{ \sum_{s=0}^k \frac{1}{n_s} \right\} < \left\{ \sum_{s \in J} \frac{1}{n_s} \right\} < \frac{1}{n_0}.
\]

Then there is an \( I \subseteq [1, k] \) with \( I \neq J \) such that \( \sum_{s \in I} 1/n_s = \sum_{s \in J} 1/n_s \).

**Remark 1.4.** If \( \{a_s(n_s)\}_{s=0}^k \) is an exact \( m \)-cover of \( \mathbb{Z} \), then \( \sum_{s=0}^k 1/n_s = m \) and so \( \lfloor \sum_{s=1}^k 1/n_s \rfloor = m - 1 \). In this case Theorem 1.4(i) gives Result I in Section 1 of [Z. W. Sun, Acta Arith. 81(1997)]. Theorem 1.4 has the following consequence (which was proved in [Z. W. Sun, Israel J. Math. 77(1992); Acta Arith. 72(1995)] for exact \( m \)-covers): Suppose that \( A = \{a_s(n_s)\}_{s=1}^k \) covers every integer at least \( m = \lfloor \sum_{s=1}^k 1/n_s \rfloor \) times. Then for any \( n = 0, 1, \ldots, m \) we have

\[
\left| \left\{ I \subseteq [1, k] : \sum_{s \in I} \frac{1}{n_s} = n \right\} \right| \geq \binom{m}{n}.
\]

Also, for any \( J \subseteq [1, k] \) with \( \{\sum_{s \in J} 1/n_s\} + \{\sum_{s \notin J} 1/n_s\} \geq 1 \) there exists an \( I \subseteq [1, k] \) with \( I \neq J \) such that \( \sum_{s \in I} 1/n_s = \sum_{s \in J} 1/n_s \).

**Theorem 1.5.** Let \( A = \{a_s(n_s)\}_{s=1}^k \) be an \( m \)-cover of \( \mathbb{Z} \) (i.e. it covers every integer at least \( m \) times), and let \( m_1, \ldots, m_k \) be any positive integers.

(i) [Z. W. Sun, Trans. Amer. Math. Soc. 348(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. 127(1999)] For any $J \subseteq [1,k]$ we have
\[
\left|\left\{I \subseteq [1,k] : I \neq J \& \sum_{s \in I} \frac{m_s}{n_s} - \sum_{s \in J} \frac{m_s}{n_s} \in \mathbb{Z}\right\}\right| \geq m. \quad (1.13)
\]

(iii) [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)] If $m$ is a prime power, then for any $J \subseteq [1,k]$ there is an $I \subseteq [1,k]$ with $I \neq J$ such that $\sum_{s \in I} m_s/n_s - \sum_{s \in J} m_s/n_s \in m\mathbb{Z}$.

(iv) [Z. W. Sun, Trans. Amer. Math. Soc. 348(1996)] If $n_1 \leq \cdots \leq n_{k-l} < n_{k-l+1} = \cdots = n_k$, then either $\sum_{s=1}^{k-l} 1/n_s \geq m$ or $l \geq n_k/n_{k-l}$.

Remark 1.5. Parts (i)-(iii) are different extensions of the following result of M. Z. Zhang (1989): If $A = \{a_s(n_s)\}_{s=1}^{k}$ is a cover of $\mathbb{Z}$ then $\sum_{s \in I} 1/n_s \in \mathbb{Z}^+$ for some $I \subseteq [1,k]$. We conjecture that the condition in part (iii) of Theorem 1.5 is unnecessary. Part (iv) in the case $l = 1$ is stronger than the Davenport-Mirsky-Newman-Radó result.

**Theorem 1.6.** Let $A = \{a_s(n_s)\}_{s=1}^{k}$ be an $m$-cover of $\mathbb{Z}$ with $a_k(n_k)$ irredundant.

(i) [Z. W. Sun, Proc. AMS 127(1999); arXiv:math.NT/0305369] Let $m_1, \ldots, m_{k-1}$ be positive integers relatively prime to $n_1, \ldots, n_{k-1}$ respectively. Then there is an $\alpha \in [0,1)$ such that for any $r = 0,1,\ldots,n_k-1$ we have
\[
\left|\left\{\left[\sum_{s \in I} m_s/n_s\right] : I \subseteq [1,k-1] \text{ and } \left\{\sum_{s \in I} m_s\right\} = \frac{\alpha + r}{n_k}\right\}\right| \geq m. \quad (1.14)
\]

(ii) [Z. W. Sun, arXiv:math.NT/0411305] If $n_k$ is a period of the covering function $w(x) = |\{1 \leq s \leq k : x \equiv a_s (\text{mod } n_s)\}|$, then for any $r = 0,1,\ldots,n_k-1$ we have
\[
\left|\left\{\left[\sum_{s \in I} 1/n_s\right] : I \subseteq [1,k-1] \text{ and } \left\{\sum_{s \in I} 1\right\} = \frac{r}{n_k}\right\}\right| \geq m. \quad (1.15)
\]

Remark 1.6. We don’t think that the condition in part (ii) can be cancelled.

**Theorem 1.7** [Z. W. Sun, J. Number Theory 111(2005)]. If systems $A = \{a_s(n_s)\}_{s=1}^{k}$ and $B = \{b_t(n_t)\}_{t=1}^{l}$ both have distinct moduli, and
\[
|\{1 \leq s \leq k : x \equiv a_s(n_s) \pmod m\}| \equiv |\{1 \leq t \leq l : x \equiv b_t(n_t) \pmod m\}| \pmod m
\]
for all $x \in \mathbb{Z}$ where $m$ is an integer not dividing $[n_1, \ldots, n_k, m_1, \ldots, m_l]$, then systems $A$ and $B$ are identical.
Remark 1.7. In the case $m = 0$, this uniqueness theorem was proved by Stein [Math. Ann. 1958] under the condition that both $A$ and $B$ are disjoint, later Žnám [Acta Arith. 26(1975)] cancelled the disjoint condition given by Stein.

Let $H$ be a subnormal subgroup of a group $G$ with finite index, and

$$H_0 = H < H_1 < \cdots < H_n = G$$

be a composition series from $H$ to $G$ (i.e. $H_i$ is maximal normal in $H_{i+1}$ for each $0 \leq i < n$). If the length $n$ is zero (i.e. $H = G$), then we set $d(G, H) = 0$, otherwise we put

$$d(G, H) = \sum_{i=0}^{n-1} ([H_{i+1} : H_i] - 1). \quad (1.16)$$

By the Jordan–Hölder theorem, $d(G, H)$ does not depend on the choice of the composition series from $H$ to $G$. It is known that $d(G, H) \geq \sum_{t=1}^r \alpha_t(p_t - 1)$ if $[G : H]$ has the standard factorization $\prod_{t=1}^r p_t^{\alpha_t}$.

**Theorem 1.8** [Z. W. Sun, Fund. Math. 134(1990); European J. Combin. 22(2001)]. Let $G$ be a group, and let $\{a_iG_i\}_{i=1}^k$ be an exact $m$-cover of $G$ (by left cosets) with all the $G_i$ subnormal in $G$. Then $[G : \bigcap_{i=1}^k G_i] < \infty$ and

$$k \geq m + d\left(G, \bigcap_{i=1}^k G_i\right) \quad (1.17)$$

where the lower bound can be attained. Moreover, for any subgroup $K$ of $G$ not contained in all the $G_i$ we have

$$|\{1 \leq i \leq k : K \not\subseteq G_i\}| \geq 1 + d\left(K, K \cap \bigcap_{i=1}^k G_i\right). \quad (1.18)$$

Remark 1.8. In the case $m = 1$, the first part was first conjectured by Š. Žnám (1968) for the cyclic group $\mathbb{Z}$. I. Korec [Fund. Math. 85(1974)] proved the first part of Theorem 1.8 in the case where $m = 1$ and all the $G_i$ are normal in $G$.

**Theorem 1.9** [G. Lettl & Z. W. Sun, 2004, arXiv:math.GR/0411144]. Let $G$ be an abelian group and $\{a_iG_i\}_{i=1}^k$ be an $m$-cover of $G$ with $a_kG_k$ irredundant. Then we have $k \geq m + f([G : G_k])$, where

$$f(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = \sum_{t=1}^r \alpha_t(p_t - 1)$$
if $p_1, \ldots, p_r$ are distinct primes and $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$.

Remark 1.9. Theorem 1.9 for disjoint covers was first conjectured by J. Mycielski (cf. [Fund. Math. 58(1966)]), it was confirmed by Znám [Colloq. Math. 15(1966)] in the case $G = \mathbb{Z}$ and by Korec [Fund. Math. 85(1974)] for general abelian groups. In the case $m = 1$ and $G_k = \{e\}$, Theorem 1.9 was ever conjectured by W. D. Gao and A. Geroldinger in 2003.

Theorem 1.10 [Z. W. Sun and M. H. Le, Acta Arith. 99(2001)]. The only solutions of the diophantine equation
\[ 2^{2n} - 1 = 2^a + 2^b + p^\alpha \tag{1.19} \]
with $n, a, b, \alpha \in \mathbb{N}$, $a > b$ and $p$ being a prime, are as follows:
\[ 2^{22} - 1 = 2^2 + 2 + 3^2 = 2^3 + 2^2 + 3 = 2^3 + 2 + 5, \]
\[ 2^{23} - 1 = 2^3 + 2^2 + 3^5 = 2^7 + 2 + 5^3. \]

Remark 1.10. In the 1960s A. Schinzel and R. Crocker proved that for each $n = 3, 4, \ldots$ the number $2^{2n} - 1$ cannot be written as the sum of a prime and two distinct powers of 2. Crocker [Pacific J. Math. 36(1971)] also showed that there are infinitely many positive odd integers not in the form $p + 2^a + 2^b$ where $a, b \in \mathbb{N}$ and $p$ is a prime.

\[ 47867742232066880047611079, \]
and let
\[ P = \{2, 3, 5, 7, 11, 13, 17, 19, 31, 37, 41, 61, 73, 97, 109, 151, 241, 257, 331\}. \]
Then any integer $x$ in the residue class $M(\prod_{p \in P} p)$ cannot be written in the form $\pm p^a \pm q^b$ where $p, q$ are primes, $a, b \in \mathbb{N}$ and any choice of signs may be made.

Remark 1.11. F. Cohen and J. L. Selfridge [Math. Comput. 29(1975)] observed that the 26-digit prime $M$ plus or minus a power of 2 can never be a prime. $M$ might be the smallest positive integer which cannot be the sum or difference of two prime powers. The exact value of $\prod_{p \in P} p$ is
\[ 66483084961588510124010691590 \]
(which was replaced by a wrong value in the paper of Sun.)

Theorem 1.12 [Z. W. Sun, Combinatorica 23(2003)]. Let $\{a_s(n_s)\}_{s=1}^k$ be a finite system of residue classes. Then $\max_{x \in \mathbb{Z}} w(x) = \sum_{s=1}^k m_s/n_s$ for some $m_1, \ldots, m_k \in \mathbb{Z}^+$, where $w(x) = |\{1 \leq s \leq k: x \in a_s(n_s)\}|$. If $n_0 \in \mathbb{Z}^+$ is a period of the periodic function $w(x)$, then for any $r = 0, 1, \ldots, n_k/(n_0, n_k) - 1$ there is an $I \subseteq \{1, \ldots, k - 1\}$ with $\sum_{s \in I} 1/n_s = r/n_k$.

Remark 1.12. In the case $n_0 = 1$, the latter part was first proved in [Z. W. Sun, Acta Arith. 81(1997)].
Theorem 1.13 [Z. W. Sun, J. Algebra 273(2004)]. Let $G$ be any group and $G_1, \ldots, G_k$ be subnormal subgroups of $G$ not all equal to $G$. If $A = \{a_iG_i\}_{i=1}^k$ (where $a_i \in G$) covers all the elements of $G$ with the same multiplicity, then $M = \max_{1 \leq i \leq k} |\{1 \leq i \leq k : n_i = n_j\}|$ is not less than the smallest prime divisor of $n_1 \cdots n_k$ where $n_i$ is the finite index $[G : G_i]$, moreover

$$\min_{1 \leq i \leq k} \log n_i \leq \frac{e^n}{\log 2} M \log^2 M + O(M \log M \log \log M)$$

where $\gamma = 0.577\cdots$ is the Euler constant and the $O$-constant is absolute.

Remark 1.13. In 1974 Herzog and Schönheim [Canad. Math. Bull.] conjectured that if $\{a_iG_i\}_{i=1}^k$ ($1 < k < \infty$) is a partition of a group $G$ into left cosets then the (finite) indices $n_1 = [G : G_1], \ldots, n_k = [G : G_k]$ cannot be pairwise distinct. In the case $G = \mathbb{Z}$ this reduces to a conjecture of P. Erdős confirmed by Davenport, Mirsky, Newman and Rado.

2. On Restricted Sumsets

The additive order of the identity of a field $F$ is either infinite or a prime, we call it the characteristic of $F$.

Let $F$ be a field of characteristic $p$, and let $A_1, \ldots, A_n$ be finite subsets of $F$ with $0 < k_1 = |A_1| \leq \cdots \leq k_n = |A_n|$. Concerning various restricted sumsets of $A_1, \ldots, A_n$, there are following known results:

(i) (The Cauchy-Davenport theorem)

$$|\{a_1 + \cdots + a_n : a_i \in A_i, a_i \in A_n\}| \geq \min\{p, k_1 + \cdots + k_n - n + 1\}.$$

(ii) (Dias da Silva and Hamidoune [Bull. London Math. Soc. 26(1994)]) If $A_1 = \cdots = A_n = A$, then

$$|\{a_1 + \cdots + a_n : a_i \in A, a_1, \ldots, a_n \text{ are distinct}\}| \geq \min\{p, n|A| - n^2 + 1\}.$$

(iii) (Alon, Nathanson and Ruzsa [J. Number Theory 56(1996)]) If $k_1 < \cdots < k_n$, then

$$|\{a_1 + \cdots + a_n : a_i \in A_i, a_i \neq a_j \text{ if } i \neq j\} \geq \min\left\{p, \sum_{i=1}^n k_i - \frac{n(n+1)}{2} + 1\right\}.$$

(iv) (Hou and Sun [Acta Arith. 102(2002)]) Let $S_{ij}$ ($1 \leq i, j \leq n, i \neq j$) be finite subsets of $F$ with cardinality $m$. If $k_1 = \cdots = k_n = k$ and $p > \max\{ln, mn\}$ where $l = k - 1 - m(n - 1)$, then

$$|\{a_1 + \cdots + a_n : a_i \in A_i, a_i - a_j \notin S_{ij} \text{ if } i \neq j\}| \geq ln + 1.$$
(v) (Liu and Sun [J. Number Theory 97(2002)]) Let \( P_1(x), \ldots, P_n(x) \in F[x] \) be monic and of degree \( m > 0 \). If \( k_n > m(n - 1) \), \( k_{i+1} - k_i \in \{0, 1\} \) for all \( i = 1, \ldots, n-1 \), and \( p > K = (k_n - 1)n - (m + 1)\binom{n}{2} \), then we have

\[ |\{a_1 + \cdots + a_n: a_i \in A_i, \ P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geq K + 1. \]

(vi) (Z.-W. Sun [J. Combin. Theory Ser. A, 103(2003), 291-304]) Let \( P_1(x), \ldots, P_n(x) \in F[x] \) have degree \( m > 0 \) with the permanent of the matrix \((b_j^{i-1})_{1 \leq i,j \leq n}\) nonzero, where \( b_j \) is the leading coefficient of \( P_j(x) \). If \( k_1 = \cdots = k_n = k > m(n-1) \) and \( K = (k-1)n - (m + 1)\binom{n}{2} < p \), then

\[ |\{a_1 + \cdots + a_n: a_i \in A_i, \ a_i \neq a_j, \ P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geq K + 1. \]

H. S. Snevily [Amer. Math. Monthly 106(1999)] posed the following 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 \( a_1 + b_1, \ldots, a_n + b_n \) are pairwise distinct.


**Theorem 2.1** [Z. W. Sun, J. Combin. Theory Ser. A, 103(2003)]. Let \( G \) be an additive abelian group whose finite subgroups are all cyclic. Let \( A_1, \ldots, A_n \) \((n > 1)\) be finite subsets of \( G \) with cardinality \( k \geq n \), and let \( b_1, \ldots, b_n \) be elements of \( G \). Let \( m \) be any positive integer not exceeding \((k-1)/(n-1)\).

(i) If \( b_1, \ldots, b_n \) are pairwise distinct, then there are at least \((k-1)n - m\binom{n}{2} + 1\) multisets \( \{a_1, \ldots, a_n\} \) such that \( a_i \in A_i \) for \( i = 1, \ldots, n \) and all the \( ma_i + b_i \) are pairwise distinct.

(ii) The sets

\[ \{a_1, \ldots, a_n\}: a_i \in A_i, \ a_i \neq a_j \text{ and } ma_i + b_i \neq ma_j + b_j \text{ if } i \neq j \] (2.1)

and

\[ \{a_1, \ldots, a_n\}: a_i \in A_i, \ ma_i \neq ma_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j \] (2.2)

have more than \((k-1)n - (m + 1)\binom{n}{2} \geq (m - 1)\binom{n}{2} \) elements, provided that \( b_1, \ldots, b_n \) are pairwise distinct and of odd order, or they have finite order and \( n! \) cannot be written in the form \( \sum_{p \in P} px_p \) where all the \( x_p \) are
nonnegative integers and $P$ is the set of primes dividing one of the orders of $b_1, \ldots, b_n$.

Remark 2.1. When $G$ is a cyclic group with $|G|$ being odd or a prime power, Theorem 2.1 (ii) in the case $k = n$ and $m = 1$, yields Theorems 1 and 2 of Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math. 126(2001)] respectively. In our opinion, the condition that all finite subgroups of $G$ are cyclic might be omitted from Theorem 2.1.

The polynomial method of Alon-Nathanson-Ruzsa was rooted in [Alon and Tarsi, Combinatorica 9(1989)] where the following elegant theorem was proved.

**Theorem 2.2** [Alon and Tarsi, 1989]. Let $F$ be a finite field with $|F|$ not being a prime, and let $M$ be a nonsingular $k$ by $k$ matrix over $F$. Then there exists a vector $\vec{x} \in F^k$ such that both $\vec{x}$ and $M\vec{x}$ have no zero component.

We extend this result as follows.

**Theorem 2.3** [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)]. Assume that $A = \{a_s(n_s)\}_{s=1}^k$ doesn’t form an $m + 1$-cover of $\mathbb{Z}$ but $A' = \{a_1(n_1), \ldots, a_k(n_k), a(n)\}$ does where $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Let $m_1, \ldots, m_k$ be integers relatively prime to $n_1, \ldots, n_k$ 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

$$X = \left\{ \sum_{j=1}^k x_j : x_j \in [0, p-1] \text{ and } \sum_{j=1}^k x_j a_{ij} \neq b_i \text{ for all } i \in [1, m] \right\}. \quad (2.3)$$

If $p$ does not divide $n_1, \ldots, n_k$ and the matrix $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq k}$ has rank $m$, then the set

$$\left\{ \left\{ \sum_{s \in I} \frac{m_s}{n_s} \right\} : I \subseteq [1, k] \text{ and } |I| \in X \right\} \quad (2.4)$$

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

3. On Zero-sum Problems

**Theorem 3.1.** Let $n$ be any positive integer.

(i) [Erdős, Ginzburg and Ziv, Bull. Research Council Israel 10(1961)] For any $c_1, \ldots, c_{2n-1} \in \mathbb{Z}$, there is an $I \subseteq [1, 2n - 1]$ with $|I| = n$ such that $\sum_{s \in I} c_s \equiv 0 \pmod{n}$.

(ii) [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)] Let $A = \{a_s(n_s)\}_{s=1}^k$ and $\{w_A(x) : x \in \mathbb{Z}\} \subseteq \{2n - 1, 2n\}$ where $w_A(x) = \ldots$
\{1 \leq s \leq k: x \in a_s(n_s)\}. If \(n\) is a prime power, then for any \(c_1, \ldots, c_k \in \mathbb{Z}\) there is an \(I \subseteq [1,k]\) such that \(\sum_{s \in I} 1/n_s = n\) and \(\sum_{s \in I} c_s \equiv 0 \pmod{n}\).

Remark 3.1. Part (ii) is an extension of part (i) in the case where \(n\) is a prime power, for, a system of \(2n-1\) copies of \(0(1)\) covers every integer exactly \(2n-1\) times.

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 \(c_{i_1}, \ldots, c_{i_l}\) \((i_1 < \cdots < i_l)\) 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 \(K\).

For a prime \(p\) and an abelian \(p\)-group \(G\), if \(G \cong \mathbb{Z}_{p^{h_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{h_l}}\) where \(h_1, \ldots, h_l \in \mathbb{Z}^+\), then we define \(L(G) = 1 + \sum_{t=1}^l (p^{h_t} - 1)\). When \(|G| = p^0 = 1\), we simply let \(L(G) = 1\).

Theorem 3.2 [Olson, J. Number Theory 1(1969)]. Let \(p\) be a prime and let \(G\) be an additive abelian \(p\)-group. Then \(D(G) = L(G)\). Moreover, given \(c, c_1, \ldots, c_{L(G)} \in G\) we have

\[
\sum_{I \subseteq [1,L(G)]} (-1)^{|I|} \equiv 0 \pmod{p}.
\]  

(3.1)

Remark 3.2. Let \(p\) be a prime. Clearly 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 \(\mathbb{Z}_p\). In 1996 Gao [J. Number Theory 56(1996)] proved that if \(c, c_1, \ldots, c_{2p-1} \in \mathbb{Z}_p\) then

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

where for a predicate \(P\) we let \([P]\) be 1 or 0 according to whether \(P\) holds or not. Note that Gao’s result can be written as

\[
\sum_{I \subseteq [1,L(\mathbb{Z}_p^2)] \atop p || |I|} (-1)^{|I|} \equiv 0 \pmod{p},
\]

which clearly follows from Olson’s congruence (3.1) in the case \(G = \mathbb{Z}_p^2\).

Olson obtained the above result by the knowledge of group rings. Without using group-rings, Z. W. Sun proved the following stronger result.
Theorem 3.3 [Z. W. Sun, 2003, arXiv:math.NT/0305369]. Let $p$ be a prime, $h_1, \ldots, h_l \in \mathbb{Z}^+$ and $k = \sum_{t=1}^l (p^{h_t} - 1)$. Let $c_{st}, c_t \in \mathbb{Z}$ for all $s \in [1, k]$ and $t \in [1, l]$. Then

$$
\sum_{I \subseteq [1,k]} (-1)^{|I|} p^{h_I} \prod_{s \in I} c_{st} - c_t \quad \text{for all } t \in [1,l]
$$

$$
\equiv \sum_{|I| \equiv 1 \mod 1} \prod_{t=1}^l \prod_{s \in I_t} c_{st} \pmod{p}. \tag{3.2}
$$

Remark 3.3. Theorem 3.3 implies Theorem 3.2, for, under the condition of Theorem 3.3 we have

$$
\sum_{I \subseteq [1,k]} (-1)^{|I|} \equiv \sum_{I \subseteq [1,k]} (-1)^{|I|} \pmod{p}
$$

where $c_1, \ldots, c_0$ are any integers. By Theorem 3.3 in the case $l = 1$, if $c, c_1, \ldots, c_{p^h - 1} \in \mathbb{Z}$, then

$$
\sum_{I \subseteq [1,p^h - 1]} (-1)^{|I|} \equiv c_1 \cdots c_{p^h - 1} \pmod{p}. \tag{3.3}
$$

Theorem 3.4. Let $q$ be a prime power.

(i) [Alon and Dubiner, 1993] If $c_1, \ldots, c_{3q} \in \mathbb{Z}_q^2$ and $c_1 + \cdots + c_{3q} = 0$, then there is an $I \subseteq [1, k]$ with $|I| = q$ and $\sum_{s \in I} c_s = 0$.

(ii) [Z. W. Sun, 2003, arXiv:math.NT/0305369] If $A = \{a_s(n_s)\}_{s=1}^k$ covers every integer exactly $3q$ times, then for any $c_1, \ldots, c_k \in \mathbb{Z}_q$ 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 $\sum_{s \in I} c_s = 0$.

Remark 3.4. Part (i) of Theorem 3.4 follows from the second part in the case $n_1 = \cdots = n_k = 1$.

Theorem 3.5 [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)]. Let $G$ be an additive abelian $p$-group where $p$ is a prime. Suppose that $A = \{a_s(n_s)\}_{s=1}^k$ covers every integer at least $L(G) + p^h - 1$ times where $h \in \mathbb{N}$. Let $m_1, \ldots, m_k \in \mathbb{Z}$ and $c_1, \ldots, c_k \in G$. Then for any $c \in G$ and $\alpha \in \mathbb{Q}$ we have

$$
\sum_{I \subseteq [1,k]} (-1)^{|I|} e^{2\pi i \sum_{s \in I} a_s m_s / n_s} \equiv 0 \pmod{p}. \tag{3.4}
$$

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

Remark 3.5. Since a system of \( k \) copies of \( 0(1) \) forms a \( k \)-cover of \( \mathbb{Z} \), Olson’s Theorem 3.2 follows from Theorem 3.4 in the case \( h = 0 \) and \( n_1 = \cdots = n_k = 1 \).