A talk given at Univ. Rome "Tor Vergata" on June 30, 2004.

TWO LOCAL-GLOBAL THEOREMS AND A POWERFUL FORMULA

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. A conjecture of Paul Erdős states that a system of k residue classes covers all the integers if it covers those integers from 1 to 2^k. Motivated by this conjecture we obtain two local-global results one of which is concerned with sums of periodic arithmetical maps to an arbitrary abelian group. We also present a powerful formula for polynomials over a ring, which implies some deep results on zero-sums (e.g. Olson's theorem on the Davenport constant of an abelian p-group). This talk is essentially self-contained, and we will show how some deep results can be deduced via very simple (but definitely nontrivial) ideas.

1. Two local-global theorems related to periodic arithmetical maps

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

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

a *residue class* or an *arithmetic sequence* with modulus n. Its characteristic function

$$\psi(x) = [x \in a(n)] = \begin{cases} 1 & \text{if } x \in a(n), \\ 0 & \text{otherwise}, \end{cases}$$

is periodic modulo n.

For a finite system

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

of residue classes, the *covering function* $w_A : \mathbb{Z} \to \mathbb{Z}$ given by

$$w_A(x) = |\{1 \leqslant s \leqslant k : \ x \in a_s(n_s)\}| = \sum_{s=1}^{k} [x \in a_s(n_s)]$$

is obviously periodic modulo the least common multiple $N_A = [n_1, \ldots, n_k]$ of all the moduli $n_1, \ldots, n_k$.

For a positive integer m, if $w_A(x) \geqslant m$ for all $x \in \mathbb{Z}$, then system A is called an *m-cover* of $\mathbb{Z}$ as in [Z. W. Sun, Acta Arith. 72(1995)]; if $w_A(x) = m$ for all $x \in \mathbb{Z}$, then A is said to be an *exact m-cover* of $\mathbb{Z}$. We also use the term *cover* instead of 1-cover, and the term *exact cover* or *disjoint cover* instead of exact 1-cover.

The concept of cover of $\mathbb{Z}$ was first introduced by P. Erdős in the early 1930's when he used a particular cover of $\mathbb{Z}$ to show that there is an infinite arithmetic progression of positive odd integers no term of which can be written as a sum of a prime and a power of 2. The first nontrivial cover of $\mathbb{Z}$ with distinct moduli was the following one discovered by P. Erdős.

$$B = \{0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)\}.$$

Note that $N_B = 12$ and B covers $0, 1, \ldots, 11$.

For any positive integer n, the system $\{r(n)\}_{r=0}^{n-1}$ is obviously a disjoint cover of $\mathbb{Z}$. Observe that

$$A_1 = \{1(2), 0(2)\},\ A_2 = \{1(2), 2(4), 0(4)\},\ A_3 = \{1(2), 2(4), 4(8), 0(8)\},$$
$$\cdots\cdots,\ A_k = \{1(2), 2(2^2), \ldots, 2^{k-1}(2^k), 0(2^k)\},\ \cdots\cdots$$

are also disjoint covers of $\mathbb{Z}$.

H. Davenport, L. Mirsky, D. Newman and R. Radó: *If* $A=\{a_s(n_s)\}_{s=1}^k$ *is a disjoint cover of* $\mathbb{Z}$ *with* $1<n_1\leqslant\cdots\leqslant n_{k-1}\leqslant n_k$ *then we must have* $n_{k-1}=n_k$.

In 1958 S. K. Stein [Math. Ann.] conjectured that if A is disjoint (i.e. the k residue classes in A are pairwise disjoint) with $1<n_1<\cdots<n_k$ then there exists an integer $x\notin\bigcup_{s=1}^k a_s(n_s)$ with $1\leqslant x\leqslant 2^k$. In 1965 P. Erdős offered a prize for a proof of his following stronger conjecture.

Erdős' Conjecture. $A=\{a_s(n_s)\}_{s=1}^k$ *forms a cover of* $\mathbb{Z}$ *if it covers those integers from* 1 *to* 2^k.

The 2^k in Erdős' conjecture is best possible because $\{2^{s-1}(2^s)\}_{s=1}^k$ covers $1,\ldots,2^k-1$ but does not cover any multiple of 2^k.

In 1969–1970 R. B. Crittenden and C. L. Vanden Eynden [Bull. Amer. Math. Soc. 1969; Proc. Amer. Math. Soc. 1970] supplied a long and awkward proof of the Erdős conjecture for $k\geqslant 20$, which involves some deep results concerning the distribution of primes.

The following result is stronger than Erdős' conjecture.

The First Local-Global Theorem [Z. W. Sun, Acta Arith. 72(1995), Trans. Amer. Math. Soc. 348(1996)]**.** *Let* $A=\{a_s(n_s)\}_{s=1}^k$ *be a finite system of residue classes, and let* $m_1,\ldots,m_k$ *be integers relatively prime to* $n_1,\ldots,n_k$ *respectively. Then system* A *forms an* m*-cover of* $\mathbb{Z}$ *if it* *covers $|S|$ consecutive integers at least m times, where*

$$S = \left\{ \left\{ \sum_{s\in I} \frac{m_s}{n_s} \right\} :\ I \subseteq \{1,\ldots,k\} \right\}.$$

(*As usual the fractional part of a real number x is denoted by $\{x\}$.*)

Proof. For any integer x, clearly

$$\begin{aligned} & x \text{ is covered by } A \\ \iff & e^{2\pi i(a_s-x)m_s/n_s} = 1 \text{ for some } s = 1,\ldots,k \\ \iff & \prod_{s=1}^{k}\left(1 - e^{2\pi i(a_s-x)m_s/n_s}\right) = 0 \\ \iff & \sum_{I\subseteq\{1,\ldots,k\}} (-1)^{|I|} e^{2\pi i\sum_{s\in I} a_s m_s/n_s} \cdot e^{-2\pi i x\sum_{s\in I} m_s/n_s} = 0 \\ \iff & \sum_{\theta\in S} e^{-2\pi i x\theta} z_\theta = 0, \end{aligned}$$

where

$$z_\theta = \sum_{\substack{I\subseteq\{1,\ldots,k\} \\ \{\sum_{s\in I} m_s/n_s\}=\theta}} (-1)^{|I|} e^{2\pi i\sum_{s\in I} a_s m_s/n_s}.$$

Suppose that A covers $|S|$ consecutive integers $a, a+1, \ldots, a+|S|-1$ where $a \in \mathbb{Z}$. By the above,

$$\sum_{\theta\in S} (e^{-2\pi i\theta})^r (e^{-2\pi i a\theta} z_\theta) = 0$$

for $r = 0, 1, \ldots, |S|-1$. As the determinant $\|(e^{-2\pi i\theta})^r\|_{0\leqslant r<|S|,\,\theta\in S}$ is of Vandermonde's type and hence nonzero, by Cramer's rule we have $z_\theta = 0$ for all $\theta \in S$. Therefore $\sum_{\theta\in S} e^{-2\pi i x\theta} z_\theta = 0$ for all $x \in \mathbb{Z}$, i.e., any $x \in \mathbb{Z}$ is covered by A. This proves the theorem in the case $m = 1$.

Obviously no integer can be covered by A more than k times. Below we let $1 < m \leqslant k$. Observe that $w_A(x) \geqslant m$ if and only if for any $J \subseteq \{1, \dots, k\}$ with $|J| = m - 1$ the system $\{a_s(n_s)\}_{s \notin J}$ covers x. If $w_A(x) \geqslant m$ for

$$\max_{\substack{J \subseteq \{1,\dots,k\} \\ |J|=m-1}} \left| \left\{ \left\{ \sum_{s \in I} \frac{m_s}{n_s} \right\} :\ I \subseteq \{1, \dots, k\} \setminus J \right\} \right| \leqslant \min \left\{ |S|, 2^{k-m+1} \right\}$$

consecutive integers x, then by the above we have $w_A(x) \geqslant m$ for all $x \in \mathbb{Z}$. We are done. $\square$

Now we give an interesting consequence of the theorem.

Corollary 1.1. *Let $n > 1$ be an integer and $m_1, \dots, m_{n-1}$ be integers relatively prime to n. Then the set $\{\sum_{s \in I} m_s : I \subseteq \{1, \dots, k\}\}$ contains a complete system of residues modulo n.*

Proof. Observe that the system $C = \{r(n)\}_{r=1}^{n-1}$ covers $n-1$ consecutive integers $1, \dots, n-1$. If $W = |\{\{\sum_{s \in I} m_s/n\} : I \subseteq \{1, \dots, n-1\}\}|$ is less than n, then C covers $1, \dots, W$ and hence it covers all the integers. Since C does not cover 0, we must have $W = n$ and hence the desired result follows. $\square$

Z. W. Sun [Trans. Amer. Math. Soc. 348(1996)] asked whether the First Local-Global Theorem still holds if we replace "m-cover" by "exact m-cover", and "at least m times" by "exactly m times". The answer is actually negative, moreover there is no constant $c(k, m) \in \mathbb{Z}^+$ such that $A = \{a_s(n_s)\}_{s=1}^{k}$ forms an exact m-cover of $\mathbb{Z}$ whenever it covers $c(k, m)$ consecutive integers exactly m times. In fact, if A is an exact m-cover of $\mathbb{Z}$, then for any integer $N > 1$ the system $\{a_1(n_1), \ldots, a_k(n_k), 0(N)\}$ covers $1, \ldots, N-1$ exactly m times but it covers 0 exactly $m+1$ times! (This observation is due to the speaker's student H. Pan.)

The characteristic function of a residue class is a periodic arithmatical map. Dirichlet characters are also periodic functions. If an element a in an additive abelian group G has order n, then the map $\psi : \mathbb{Z} \to G$ given by $\psi(x) = xa$ is periodic mod n.

The Second Local-Global Theorem [Z. W. Sun, Math. Res. Lett. 11(2004); arXiv:math.NT/0404137]**.** *Let G be any additive abelian group, and let $\psi_1, \ldots, \psi_k$ be maps from $\mathbb{Z}$ to G with periods $n_1, \ldots, n_k \in \mathbb{Z}^+$ respectively. Then the function $\psi = \psi_1 + \cdots + \psi_k$ is constant if $\psi(x)$ equals a constant for $|T|$ consecutive integers x, where*

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

As a constant can be viewed as a function on $\mathbb{Z}$ with period $n_0 = 1$, it suffices to show that ψ is the zero function if $\psi(x) = 0$ for $|T|$ consecutive integers x.

When G is a subgroup of the additive group of complex numbers (e.g.

$G = \mathbb{Z}$), we have

$$\begin{aligned}\psi(x) &= \sum_{s=1}^{k}\sum_{a=0}^{n_s-1}\psi_s(a)[x\in a(n_s)]\\ &= \sum_{s=1}^{k}\sum_{a=0}^{n_s-1}\frac{\psi_s(a)}{n_s}\sum_{r=0}^{n_s-1}e^{2\pi i(x-a)r/n_s}\\ &= \sum_{s=1}^{k}\sum_{r=0}^{n_s-1}\left(\sum_{a=0}^{n_s-1}\frac{\psi_s(a)}{n_s}e^{-2\pi iar/n_s}\right)\left(e^{2\pi ir/n_s}\right)^x\\ &= \sum_{\alpha\in T}(e^{2\pi i\alpha})^x\left(\sum_{\substack{s=1\\ \alpha n_s\in\mathbb{Z}}}^{k}\sum_{a=0}^{n_s-1}\frac{\psi_s(a)}{n_s}e^{-2\pi i\alpha a}\right),\end{aligned}$$

and hence the desired result follows by the same trick as in the proof of the First Local-Global Theorem.

When G is the additive group of a field of characteristic p (e.g. $\mathbb{Z}/p\mathbb{Z}$), in order to guarantee that the algebraic closure of the field contains a primitive n_sth roots of unity we must impose a condition that p does not divide n_s. So, as proved in [Z. W. Sun, Math. Res. Lett. 11(2004)] the required result holds if G is the additive group of a field whose characteristic does not divide any of the periods $n_1, \ldots, n_k$.

How can we handle the case $G = \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ (where m is a positive integer)? Now the use of Vandermonde determinants does not work perfectly. **We need a new idea!**

Suppose that $\psi_s(x) \in \mathbb{Z}$ for all $1 \leqslant s \leqslant k$ and $x \in \mathbb{Z}$. Let N be the least common multiple of $n_1, \ldots, n_k$. As the above,

$$u_x := N\psi(x) = \sum_{\alpha\in T}(e^{2\pi i\alpha})^x c_\alpha$$

where

$$c_\alpha = \sum_{\substack{s=1 \\ \alpha n_s \in \mathbb{Z}}}^{k} \frac{N}{n_s} \sum_{a=0}^{n_s-1} \psi_s(a) e^{-2\pi i \alpha a}$$

lies in the ring Ω of all algebraic integers. Note that the sequence $\{u_n\}_{n\in\mathbb{Z}}$ is a linear recurrence of order $|T|$ with the characteristic polynomial

$$\prod_{\alpha \in T} (x - e^{2\pi i \alpha}) \in \Omega[x].$$

Assume that $\psi(a+j) \equiv 0 \pmod{m}$ for $j = 0, 1, \ldots, |T|-1$ where $a \in \mathbb{Z}$. We want to show that $\psi(x) \equiv 0 \pmod{m}$ for all $x \in \mathbb{Z}$, i.e., $u_n \equiv 0 \pmod{mN}$ for all $n \in \mathbb{Z}$. Now that $u_n \equiv 0 \pmod{mN}$ for $n = a, a+1, \ldots, a+|T|-1$, by the recursion of $\{u_n\}_{n\in\mathbb{Z}}$ we also have $u_n \equiv 0 \pmod{mN}$ for $n = a+|T|, a+|T|+1, \ldots$. Since u_n is a periodic function of n, for any $n \in \mathbb{Z}$ we have the congruence $u_n \equiv 0 \pmod{mN}$ over Ω and hence the congruence over $\mathbb{Z}$ is also valid. This proves the theorem in the case $G = \mathbb{Z}_m$.

Now we handle the general case. Without any loss of generality, we may simply let G coincide with its subgroup generated by the finite set

$$\{\psi_s(x) : \ x = 0, \ldots, n_s - 1; \ s = 1, \ldots, k\}.$$

Now G is finitely generated, so there are $m_1, \ldots, m_l \in \mathbb{Z}^+$ and $n \in \mathbb{N}$ such that G is isomorphic to the additive group $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l} \oplus \mathbb{Z}^n$. It is easy to see that the family of abelian groups possessing the property described in the theorem is closed under direct sum, so by previous results the group G also has the described property.

Corollary 1.2 [Z. W. Sun, Math. Res. Lett. 11(2004)]. *$A = \{a_s(n_s)\}_{s=1}^k$ forms an exact m-cover of $\mathbb{Z}$ if it covers*

$$\left|\left\{\frac{r}{n_s} : r = 0, 1, \ldots, n_s - 1;\ s = 1, \ldots, k\right\}\right| \leqslant n_1 + \cdots + n_k - k + 1$$

consecutive integers exactly m times.

Proof. This is because $w_A(x) = \sum_{s=1}^k \psi_s(x)$ where $\psi_s(x) = [x \in a_s(n_s)]$ is periodic mod n_s.

Corollary 1.3 [N. J. Fine and H. S. Wilf, Proc. Amer. Math. Soc. 1965]. *Let $\{f_n\}_{n\geqslant 0}$ and $\{g_n\}_{n\geqslant 0}$ be real sequences with respective periods h and k respectively. If $f_n = g_n$ for $0 \leqslant n < h+k-\gcd(h,k)$, then $f_n = g_n$ for every $n = 0, 1, 2, \ldots$.*

Proof. Observe that

$$\left|\left\{\frac{r}{h} : r = 0, 1, \ldots, h-1\right\} \cup \left\{\frac{s}{k} : s = 0, 1, \ldots, k-1\right\}\right| = h+k-\gcd(h,k).$$

So the desired result follows from the Second Local-Global Theorem.

Corollary 1.3 has applications in combinatorics of finite words.

2. A powerful polynomial formula and its applications

Let G be a finite abelian group G (written additively). If $c_1, \ldots, c_{|G|} \in G$, then the partial sums

$$s_0 = 0,\ s_1 = c_1,\ s_2 = c_1 + c_2, \ldots, s_{|G|} = c_1 + \cdots + c_{|G|}$$

cannot be distinct by the pigeon-hole principle, thus there are $0 \leqslant i < j \leqslant |G|$ such that $s_i = s_j$, i.e., $c_{i+1} + \cdots + c_j = 0$. The *Davenport constant* $D(G)$

of 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 nonempty subsequence $c_{i_1},\cdots,c_{i_l}$ $(i_1<\cdots<i_l)$ with zero-sum (i.e. $c_{i_1}+\cdots+c_{i_l}=0$). Clearly $D(G)\leqslant|G|$, and $D(\mathbb{Z}_n)=n$ where n is a positive integer and $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$. 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 J. E. 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

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

Olson's Theorem. *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*

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

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

Olson obtained this theorem by showing that if $c_1,\ldots,c_k\in G$ where $k\geqslant L(G)$ then we have $\prod_{s=1}^k(1-c_s)=0$ in the group-ring $\mathbb{Z}_p[G]$. Although this classical theorem has been cited hundreds of times, many authors on zero-sums just follow Olson's approach by using the group-ring method, and no new proof of Olson's theorem had been found until the speaker's work in 2003.

Here is a useful polynomial formula due to Zhi-Wei Sun.

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 $f(x_1,\cdots,x_k)$ be a polynomial over R. If $J\subseteq[1,k]$ and $|J|\geqslant\deg f$, then we have the formula*

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

where $[x_1^{i_1}\cdots x_k^{i_k}]f(x_1,\cdots,x_k)$ denotes the coefficient of the monomial $x_1^{i_1}\cdots x_k^{i_k}$ in the polynomial $f(x_1,\cdots,x_k)$, and for an assertion P we let $[P]$ be 1 or 0 according to whether P holds or not.

The proof of this polynomial formula is not difficult, so we omit it here.

Let p be a prime and a be any integer. Fermat's little theorem tells us that we can characterize whether p divides a or not by a polynomial with integer coefficients. Namely,

$$[p\mid a]\equiv 1-a^{p-1}\pmod p.$$

Let h be a positive integer. Can we characterize whether p^h divides a in a similar way? Zhi-Wei Sun observed in 2003 that

$$[p^h\mid a]\equiv\binom{a-1}{p^h-1}\pmod p$$

which can be deduced from Lucas' theorem or proved directly. This observation made Sun find that Olson's theorem is just a consequence of the polynomial formula.

Let p be a prime, and let $h_1,\dots,h_l\in\mathbb{N}=\{0,1,2,\dots\}$. Let $k\geqslant 1+\sum_{t=1}^{l}(p^{\alpha_t}-1)$. Let $c_{st}\in\mathbb{Z}$ for all $0\leqslant s\leqslant k$ and $1\leqslant t\leqslant l$. Then

$$\begin{aligned}&\sum_{\substack{I\subseteq\{1,\dots,k\}\\ \sum_{s\in I}c_{st}\equiv c_{0t}\ (\mathrm{mod}\ p^{h_t})\\ \text{for all } t=1,\dots,l}}(-1)^{|I|}\\ \equiv&\sum_{I\subseteq\{1,\dots,k\}}(-1)^{|I|}\prod_{t=1}^{l}\left[p^{h_t}\mid\sum_{s\in I}c_{st}-c_{0t}\right]\ (\mathrm{mod}\ p)\\ \equiv&\sum_{I\subseteq\{1,\dots,k\}}(-1)^{|I|}\prod_{t=1}^{l}\binom{\sum_{s\in I}c_{st}-c_{0t}-1}{p^{h_t}-1}\ (\mathrm{mod}\ p).\\ \equiv&\sum_{I\subseteq\{1,\dots,k\}}(-1)^{|I|}f([1\in I],\dots,[k\in I])\ \ (\mathrm{mod}\ p),\end{aligned}$$

where

$$f(x_1,\dots,x_k)=\prod_{t=1}^{l}\binom{\sum_{s=1}^{k}c_{st}x_s-c_{0t}-1}{p^{h_t}-1}$$

is a polynomial taking integer values at integral inputs. As $\deg f\leqslant\sum_{t=1}^{l}(p^{h_t}-1)<k$, we have $[x_1\cdots x_k]f(x_1,\dots,x_k)=0$. Applying the polynomial formula we get that

$$\sum_{\substack{I\subseteq\{1,\dots,k\}\\ \sum_{s\in I}c_{st}\equiv c_{0t}\ (\mathrm{mod}\ p^{h_t})\\ \text{for all } t=1,\dots,l}}(-1)^{|I|}\equiv 0\ \ (\mathrm{mod}\ p).$$

In other words, if $c,c_1,\dots,c_k\in G=\mathbb{Z}_{p^{h_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{h_l}}$ then we have the congruence

$$\sum_{\substack{I\subseteq\{1,\dots,k\}\\ \sum_{s\in I}c_s=c}}(-1)^{|I|}\equiv 0\ (\mathrm{mod}\ p).$$

This proves Olson's theorem in an elementary way.

Corollary 2.1 [Z. W. Sun, Electron. Res. Amer. Math. Soc. 9(2003); `arXiv:math.NT/0305369`]. *Let p be a prime and h be a positive integer. Let $c, c_1, \ldots, c_{p^h-1} \in \mathbb{Z}$. Then we have the congruence*

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

Proof. Just apply the polynomial formula with

$$f(x_1,\ldots,x_{p^h-1})=\binom{\sum_{s=1}^{p^h-1}c_sx_s-c}{p^h-1}.$$

This corollary tells more detailed information than Corollary 1.1 in the case where n is a prime power.

The following result was first obtained by Baker and Schmidt [J. Number Theory 12(1980)] via a very deep and complicated method.

Corollary 2.2 (Baker & Schmidt, 1980). *Let $h_t \in \mathbb{N}$ and $f_t(x_1,\cdots,x_k) \in \mathbb{Z}[x_1,\cdots,x_k]$ for $t = 1,\cdots,l$. If p is a prime and $k > \sum_{t=1}^{l}(p^{h_t}-1)\deg f_t$, then*

$$\sum_{\substack{I\subseteq[1,k]\\ p^{h_t}\mid f_t([1\in I],\cdots,[k\in I])\\ \text{for all }t\in[1,l]}}(-1)^{|I|}\equiv 0\pmod p.$$

Proof. For the polynomial

$$f(x_1,\cdots,x_k)=\prod_{t=1}^{l}\binom{f_t(x_1,\cdots,x_k)-1}{p^{h_t}-1},$$

clearly $\deg f \leqslant \sum_{t=1}^{l}(p^{h_t}-1)\deg f_t < k$ and so $[x_1\cdots x_k]f(x_1,\cdots,x_k) = 0$. Now it suffices to apply the polynomial formula.

Finally we remark that the polynomial formula is also the starting point of Z. W. Sun's unification of the following three topics of P. Erdős: *Covers of* $\mathbb{Z}$ *by residue classes, zero-sum problems on abelian groups, and subset sums in fields.*