Transversals of Additive Latin Squares

Samit Dasgupta
Department of Mathematics, University of California, Berkeley, CA
dasgupta@post.harvard.edu

Gyula Károlyi[*]
Department of Algebra and Number Theory, Eötvös University, Budapest
karolyi@cs.elte.hu

Oriol Serra[†]
Department of Applied Mathematics, Polytechnic University of Catalonia, Barcelona
oserra@mat.upc.es

Balázs Szegedy
Department of Algebra and Number Theory, Eötvös University, Budapest
szegedy@cs.elte.hu

version 9

Abstract

Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be two subsets of an Abelian group G, $k \leq |G|$. Snevily conjectured that, when G is of odd order, there is a permutation $\pi \in S_k$ such that the sums $a_i + b_{\pi(i)}$, $1 \leq i \leq k$, are pairwise different. Alon showed that the conjecture is true for groups of prime order, even when A is a sequence of $k < |G|$ elements, i.e., by allowing repeated elements in A. In this last sense the result does not hold for other Abelian groups. With a new kind of application of the polynomial method in various finite and infinite fields we extend Alon's result to the groups $(\mathbb{Z}_p)^\alpha$ and $\mathbb{Z}_{p^\alpha}$ in the case $k < p$, and verify Snevily's conjecture for every cyclic group of odd order.

1 Introduction

A *transversal* of an $n \times n$ matrix is a collection of n cells, no two of which are in the same row or column. A transversal of a matrix is a *Latin transversal* if no two of its cells contain the same element. A conjecture of Snevily [6, Conjecture 1] asserts that, for any odd n, every $k \times k$ sub-matrix of the Cayley addition table of $\mathbb{Z}_n$ contains a Latin transversal. Putting it differently, for any two subsets A and B with $|A| = |B| = k$ of a cyclic group G of odd order $n \geq k$, there exist numberings $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ of the elements of A and B respectively

[*] Supported by Hungarian research grants OTKA F030822 and T029759.

[†] Supported by the Catalan Research Council under grant 1998SGR00119.

such that the k sums $a_i + b_i$, $1 \le i \le k$, are pairwise different. In fact, this is also conjectured for arbitrary Abelian groups G of odd order [6, Conjecture 3]. The statement does not hold for cyclic groups of even order as shown, for example, by taking $A = B = G$, whereas for this choice it clearly holds when $|G|$ is odd (just take $a_i = b_i, i = 1, \ldots, n$). For arbitrary groups of even order take $A = B = \{0, g\}$, with g an involution, to get a counterexample. Here we first verify Snevily's conjecture for arbitrary cyclic groups of odd order.

Theorem 1 *Let G be a cyclic group of odd order. Let $A = \{a_1, a_2, \ldots, a_k\}$ and B be subsets of G, each of cardinality k. Then there is a numbering $b_1, \ldots, b_k$ of the elements of B such that the sums $a_1 + b_1, \ldots, a_k + b_k$ are pairwise different.*

Alon [2] proved the conjecture in the particular case when $n = p$ is a prime number. Actually he proved a stronger result which can be considered as a special case of the following result when $\alpha = 1$.

Theorem 2 *Let p be a prime number, α a positive integer and $G = \mathbb{Z}_{p^\alpha}$ or $G = (\mathbb{Z}_p)^\alpha$. Let $(a_1, \ldots, a_k)$, $k < p$, be a sequence of not necessarily distinct elements in G. Then, for any subset $B \subset G$ of cardinality k there is a numbering $b_1, \ldots, b_k$ of the elements of B such that the sums $a_1 + b_1, \ldots, a_k + b_k$ are pairwise different.*

Note that the above theorem is not true with $k = p$ (see [2]). Following Alon's approach, our starting point is the following result called 'Combinatorial Nullstellensatz'.

Theorem 3 (Alon [1]) *Let F be an arbitrary field and let $f = f(x_1, \ldots, x_k)$ be a polynomial in $F[x_1, \ldots, x_k]$. Suppose that there is a monomial $\prod_{i=1}^k x_i^{t_i}$ such that $\sum_{i=1}^k t_i$ equals the degree of f and whose coefficient in f is nonzero. Then, if $S_1, \ldots, S_k$ are subsets of F with $|S_i| > t_i$ then there are $s_1 \in S_1, s_2 \in S_2, \ldots s_k \in S_k$ such that $f(s_1, \ldots, s_k) \neq 0$.*

For the case $G = (\mathbb{Z}_p)^\alpha$ the proof of Theorem 2 is almost the same as the one given by Alon in [2] which we sketch here to demonstrate the method.

Let p be a prime number and let $\mathbb{F}_q$ be the finite field of order $q = p^\alpha$. Identify the group $G = (\mathbb{Z}_p)^\alpha$ with the additive group of $\mathbb{F}_q$. Consider the polynomial

$$\begin{aligned} f(x_1, \ldots, x_k) &= \prod_{1 \le j < i \le k} ((x_i - x_j)(a_i + x_i - a_j - x_j)) \\ &= \prod_{1 \le j < i \le k} ((x_i - x_j)(x_i - x_j)) + \text{terms of lower degree.} \end{aligned}$$

The degree of f is $k(k-1)$ and the coefficient of $\prod_{i=1}^k x_i^{k-1}$ in f is $c = (-1)^{\binom{k}{2}} k!$ (see Section 2). Since the characteristic of the field is $p > k$, it follows that c is a nonzero element. By applying Theorem 3 with $t_i = k - 1$ and $S_i = B$ for $i = 1, \ldots, k$, we obtain elements $b_1, \ldots b_k \in B$ such that

$$\prod_{1 \le j < i \le k} ((b_i - b_j)(a_i + b_i - a_j - b_j)) \neq 0.$$

Therefore, the elements $b_1, \dots, b_k$ are pairwise distinct and so are the k sums $b_1 + a_1, \dots, b_k + a_k$. This completes the proof for $G = (\mathbb{Z}_p)^\alpha$. □

So far we only have exploited the additive structures of finite fields; and it is clear that $(\mathbb{Z}_p)^\alpha$ are the only groups that can be treated this way. On the other hand, every cyclic group is the subgroup of the multiplicative group of certain fields, and there exists a multiplicative analogue of the above described method, which is worked out in the following section. We apply this method to obtain Theorems 1 and 2 in Section 3. In the remaining part of the paper we study the possibility of further extending these results. In particular, we attempt to attack in Section 5 another conjecture of Snevily [6, Conjecture 2], namely that, if n is even, a $k \times k$ sub-matrix of the Cayley addition table of $\mathbb{Z}_n$ contains a Latin transversal unless k is an even divisor of n and the rows and columns of the sub-matrix are each cosets of the unique subgroup of order k in $\mathbb{Z}_n$.

2 The multiplicative analogue

In this section we study how to modify Alon's method if we wish to identify G with a subgroup of the multiplicative group of a suitable field. This will reduce the original problems to the study of permanents of certain Vandermonde matrices.

Denote by $V(y_1, \dots, y_k)$ the Vandermonde matrix

$$V(y_1, \dots, y_k) = \begin{pmatrix} 1 & y_1 & \dots & y_1^{k-1} \\ 1 & y_2 & \dots & y_2^{k-1} \\ \vdots & \vdots & & \vdots \\ 1 & y_k & \dots & y_k^{k-1} \end{pmatrix}.$$

For a matrix $M = (m_{ij})_{1 \le i,j \le k}$, the permanent of M is $\mathrm{Per}M = \sum_{\pi \in S_k} m_{1\pi(1)} m_{2\pi(2)} \dots m_{k\pi(k)}$.

Lemma 4 *Let F be an arbitrary field and suppose that $\mathrm{Per}V(a_1, \dots, a_k) \neq 0$ for some elements $a_1, a_2, \dots, a_k \in F$. Then, for any subset $B \subset F$ of cardinality k there is a numbering $b_1, \dots, b_k$ of the elements of B such that the products $a_1 b_1, \dots, a_k b_k$ are pairwise different.*

Proof. Consider the following polynomial in $F[x_1, \dots, x_k]$

$$f(x_1, \dots, x_k) = \prod_{1 \le j < i \le k} \left((x_i - x_j)(a_i x_i - a_j x_j) \right).$$

The degree of f is clearly not greater than $k(k-1)$. In addition,

$$\begin{aligned}
f(x_1,\ldots,x_k) &= \mathrm{Det}V(x_1,\ldots,x_k)\cdot\mathrm{Det}V(a_1x_1,a_2x_2,\ldots,a_kx_k) \\
&= \left(\sum_{\pi\in S_k}(-1)^{I(\pi)}\prod_{i=1}^{k}x_{\pi(i)}^{(i-1)}\right)\left(\sum_{\tau\in S_k}(-1)^{I(\tau)}\prod_{i=1}^{k}(a_{\tau(i)}x_{\tau(i)})^{(i-1)}\right) \\
&= \left(\sum_{\pi\in S_k}(-1)^{I(\pi)}\prod_{i=1}^{k}x_{\pi(i)}^{(i-1)}\right)\left(\sum_{\tau\in S_k}(-1)^{I(\tau)}\prod_{i=1}^{k}(a_{\tau(k+1-i)}x_{\tau(k+1-i)})^{(k-i)}\right) \\
&= \left(\sum_{\pi\in S_k}(-1)^{I(\pi)}\prod_{i=1}^{k}x_{\pi(i)}^{(i-1)}\right)\left(\sum_{\pi\in S_k}(-1)^{\binom{k}{2}-I(\pi)}\prod_{i=1}^{k}(a_{\pi(i)}x_{\pi(i)})^{(k-i)}\right).
\end{aligned}$$

Therefore, the coefficient $c(a_1,\ldots,a_k)$ of the monomial $\prod_{i=1}^{k}x_i^{k-1}$ in f,

$$\begin{aligned}
c(a_1,\ldots,a_k) &= \sum_{\pi\in S_k}(-1)^{\binom{k}{2}}\prod_{i=1}^{k}a_{\pi(i)}^{k-i} \\
&= (-1)^{\binom{k}{2}}\sum_{\pi\in S_k}\prod_{i=1}^{k}a_{\pi(k+1-i)}^{i-1} \\
&= (-1)^{\binom{k}{2}}\sum_{\tau\in S_k}\prod_{i=1}^{k}a_{\tau(i)}^{i-1} \\
&= (-1)^{\binom{k}{2}}\mathrm{Per}V(a_1,\ldots,a_k)
\end{aligned}$$

is different from 0 (in particular, $c(1,\ldots,1)=(-1)^{\binom{k}{2}}k!$). Consequently, f is of degree $k(k-1)$, and we can apply Theorem 3 with $t_i=k-1$ and $S_i=B$ for $i=1,\ldots,k$ to obtain k distinct elements $b_1,\ldots,b_k$ in B such that the products $a_1b_1,\ldots,a_kb_k$ are pairwise distinct. This completes the proof of the lemma. □

Another proof of Lemma 4, independent of Theorem 3, is based on the following identity. Let $1\in R$ be a commutative ring, $u_1,\ldots,u_k,v_1,\ldots,v_k$ indeterminates. For any permutation $\pi\in S_k$, define

$$P_\pi=P_\pi(u_1,\ldots,u_k;v_1,\ldots,v_k)=\prod_{1\le j<i\le k}(u_iv_{\pi(i)}-u_jv_{\pi(j)})\in R[u_1,\ldots,u_k,v_1,\ldots,v_k]\ .$$

An easy algebraic manipulation yields

Lemma 5

$$\sum_{\pi\in S_k}P_\pi=\mathrm{Det}V(u_1,\ldots,u_k)\mathrm{Per}V(v_1,\ldots,v_k)\ .$$

□

2^{nd} proof of Lemma 4. Suppose $B = \{b'_1, \ldots, b'_k\}$. It follows from Lemma 5 that

$$\begin{aligned}\sum_{\pi \in S_k} P_\pi(b'_1, \ldots, b'_k; a_1, \ldots, a_k) &= \mathrm{Det}V(b'_1, \ldots, b'_k)\mathrm{Per}V(a_1, \ldots, a_k) \\ &= \left(\prod_{1 \le j < i \le k} (b'_i - b'_j) \right) \mathrm{Per}V(a_1, \ldots, a_k)\end{aligned}$$

is different from zero. Consequently, there is a permutation $\pi \in S_k$ such that

$$P_\pi(b'_1, \ldots, b'_k; a_1, \ldots, a_k) = \prod_{1 \le j < i \le k} (b'_i a_{\pi(i)} - b'_j a_{\pi(j)}) \neq 0 \ .$$

Writing $\sigma = \pi^{-1}$ and $b_i = b'_{\sigma(i)}$, we can conclude that the $a_i b_i$'s are pairwise different. □

3 Proof of the Theorems

Proof of Theorem 1. Write $|G| = m$ and let $\alpha = \phi(m)$, where ϕ is Euler's totient function; then $2^\alpha \equiv 1 \pmod m$. Consider $F = \mathbb{F}_{2^\alpha}$, its multiplicative group $F^\times$ is a cyclic group of order $2^\alpha - 1$. Thus, G can be identified with a subgroup of $F^\times$, the operation on G being the restriction of the multiplication in F. Since F is of characteristic 2, we have

$$\mathrm{Per}V(a_1, \ldots, a_k) = \mathrm{Det}V(a_1, \ldots, a_k) = \prod_{1 \le j < i \le k} (a_i - a_j) \neq 0 \ .$$

The result follows immediately from Lemma 4. Alternatively, we can use Lemma 5 to prove that there is a permutation $\pi \in S_k$ such that $P_\pi(a_1, \ldots, a_k; b_1, \ldots, b_k) \neq 0$. □

Proof of Theorem 2 for $G = \mathbb{Z}_{p^\alpha}$. Consider the cyclotomic field $F = \mathbb{Q}(\xi)$, where ξ is a primitive q^{th} root of unity and $q = p^\alpha$. The degree of this extension is $[\mathbb{Q}(\xi) : \mathbb{Q}] = p^\alpha - p^{\alpha-1}$. Identify G with the multiplicative subgroup $\{1, \xi, \xi^2, \ldots, \xi^{q-1}\}$ of $\mathbb{Q}(\xi)$. As before, the result would be an immediate consequence of the fact $\mathrm{Per}V(a_1, \ldots, a_k) \neq 0$. To verify this fact, note that each term $\prod_{i=1}^k a_{\tau(i)}^{i-1}$ of this permanent is a q^{th} root of unity. Thus, $\mathrm{Per}V(a_1, \ldots, a_k)$ is the sum of q^{th} roots of unity, where the number of summands, $k!$, is not divisible by p. Therefore, it is enough to prove the following lemma.

Lemma 6 *If $\epsilon_1, \ldots, \epsilon_t$ are q^{th} roots of unity such that $\sum_{i=1}^t \epsilon_i = 0$, then t is divisible by p.*

Lemma 6 follows from the more precise statement in Lemma 7 below. Let $\omega_p = e^{2\pi i/p}$. For each $\eta \in F$ such that $\eta^q = 1$ we have $\sum_{i=1}^p \eta\omega_p^i = \eta \sum_{i=1}^p \omega_p^i = 0$. We say that a set $X = \{\epsilon_1, \ldots, \epsilon_p\}$ of q^{th} roots of unity is *simple* if there is $\eta \in F$ with $\eta^q = 1$ such that $X = \{\eta\omega_p, \eta\omega_p^2, \ldots, \eta\omega_p^p\}$.

Lemma 7 *Let $\epsilon_i, i \in I$ be q^{th} roots of unity such that $\sum_{i \in I} \epsilon_i = 0$. Then there is a partition $I = \cup J_r$ such that $\{\epsilon_j \mid j \in J_r\}$ is a simple set for each r.*

Proof. Consider $V = \mathbb{Q}(\xi)$ as a vector space over $\mathbb{Q}$. The dimension of V is $\phi(q) = p^\alpha - p^{\alpha-1}$. Let, for $0 \le s \le q-1$, $K_s = \{i \mid \epsilon_i = \xi^s\}$, and write $c_s = |K_s|$. Let $s \equiv \bar{s} \bmod p^{\alpha-1}$, $0 \le \bar{s} < p^{\alpha-1}$. Note that $\{\xi^s, \xi^{s+p^{\alpha-1}}, \ldots, \xi^{s+(p-1)p^{\alpha-1}}\}$ is a simple set for every $0 \le s < p^{\alpha-1}$. Thus,

$$0 = \sum_{i \in I} \epsilon_i = \sum_{s=0}^{q-1} c_s \xi^s = \sum_{s=0}^{q-1} c_s \xi^s - \sum_{s=0}^{p^{\alpha-1}-1} c_s(\xi^s + \xi^{s+p^{\alpha-1}} + \ldots + \xi^{s+(p-1)p^{\alpha-1}})$$

$$= \sum_{s=0}^{q-1} (c_s - c_{\bar{s}})\xi^s = \sum_{s=p^{\alpha-1}}^{q-1} (c_s - c_{\bar{s}})\xi^s \ .$$

Since $\{1, \xi, \xi^2, \ldots, \xi^{\phi(q)-1}\}$ is a basis of V, $\{\xi^s \mid p^{\alpha-1} \le s \le p^\alpha - 1\}$ is also an independent set. Thus, $c_s = c_{\bar{s}}$ for every $0 \le s \le q-1$. Each set J_r of the desired partition of I can then be obtained by choosing one element in each one of the sets $K_s, K_{s+p^{\alpha-1}}, \ldots, K_{s+(p-1)p^{\alpha-1}}$, for every choice of s, $0 \le s < p^{\alpha-1}$ such that $K_s \neq \emptyset$. □

Since every simple set has exactly p elements, Lemma 6 follows and the proof is complete. □

A more direct proof of Lemma 6 is due to Imre Z. Ruzsa and goes as follows. There is an r^{th} root of unity ϵ ($r = p^\beta, \beta \le \alpha$) such that there exist positive integers α_i with $\epsilon_i = \epsilon^{\alpha_i}$. Consider the polynomial $P(x) = \sum_{i=1}^t x^{\alpha_i}$, then $P(\epsilon) = 0$. It follows that the r^{th} cyclotomic polynomial Φ_r is a divisor of P in the ring $\mathbb{Z}[x]$. Consequently, $p = \Phi_r(1)$ divides $P(1) = t$. □

4 Bad sequences

For a *fixed* integer k, the statements of Theorems 1 and 2 can be expressed in the first order language of Abelian groups. It is immediate that these assertions hold in $\mathbb{Z}$ and in any ordered Abelian group in general. Consequently, it follows from a standard compactness argument (see [4]) that the assertions hold in any finite Abelian group whose order is not divisible by small prime numbers. A quantitative estimate, exponential in k, can be obtained with the so-called rectification principle [3, 4]. Thus, Snevily's conjecture asserts that the statement of Theorem 1 holds whenever $|G|$ is not divisible by 2. We believe that the statement of Theorem 2 is always true if the smallest prime divisor of $|G|$ exceeds k. We also believe that the structure of the counterexamples in other cases cannot be arbitrary, see Problem 1 below.

Let G be any Abelian group and $A = (a_1, a_2, \ldots, a_k)$, $k \le |G|$, be any sequence of group elements. A is said to be a *bad* sequence if there is a subset $B \subset G$ of cardinality k such that, for any numbering $b_1, \ldots, b_k$ of the elements of B, there are $1 \le i < j \le k$ such that $a_i + b_i = a_j + b_j$. Assume that G is a subgroup of the multiplicative group of some field F. It follows from Lemma 4 that A cannot be bad if $\mathrm{Per}V(a_1, \ldots, a_k) \neq 0$ in F. It is possible that a better understanding of permanents of Vandermonde matrices may even help in the characterization of bad sets. We will illustrate this point with the study of the cases $k = 2, 3$. There must be, however, certain limitations to this approach, as shown by the following example.

Example 1 *Suppose that $G \cong \mathbb{Z}_8$ is the subgroup of the multiplicative group of some field, and $A = \{a_1 = 1, a_2 = g^2, a_3 = g^3\}$ where g is a generator for G. Then* $\mathrm{Per}V(a_1, a_2, a_3) = 0$ *although A is not a bad sequence.*

Proof. Writing additively $A = \{0, 2, 3\}$, a short case analysis based on the number of even/odd elements of $B \subset G$, $|B| = 3$ shows that a required numbering b_1, b_2, b_3 of the elements of B always exists. On the other hand,

$$\mathrm{Per}V(a_1, a_2, a_3) = \mathrm{Per}\begin{pmatrix} 1 & 1 & 1 \\ 1 & g^2 & g^4 \\ 1 & g^3 & g^6 \end{pmatrix} = g^2(1 + g + g^2)(1 + g^4) = 0 \ ,$$

given that $g^4 = -1$. □

Next we give a complete description of the bad sequences of length ≤ 3 in cyclic groups.

Example 2 *Characterization of the bad sequences in the case* $k = 2$.

Identify $G \cong \mathbb{Z}_n$ with a subgroup of $\mathbb{C}^\times$, as in the proof of Theorem 2. Let ϵ, η be n^{th} roots of unity. Then $\mathrm{Per}V(\epsilon, \eta) = \epsilon + \eta = 0$ if and only if $\eta = -\epsilon = \omega_n^{n/2}\epsilon$. Consequently, $A = (a_1, a_2)$ can be a bad sequence in $\mathbb{Z}_n$ only if n is even and $a_2 = a_1 + n/2$, in which case it is indeed a bad sequence.

Example 3 *Characterization of the bad sequences in the case* $k = 3$.

Again we identify $G \cong \mathbb{Z}_n$ with a subgroup of $\mathbb{C}^\times$. Let ϵ, η, ζ be n^{th} roots of unity, $n \geq 3$. In this case $\mathrm{Per}V(\epsilon, \eta, \zeta) = 0$ if and only if

$$(\epsilon + \eta)(\eta + \zeta)(\zeta + \epsilon) = 2\epsilon\eta\zeta \ ,$$

that is,

$$(1 + x)(1 + y)(1 + z) = 2 \tag{1}$$

where $x = \eta/\epsilon, y = \zeta/\eta, z = \epsilon/\zeta$ are all n^{th} roots of unity and $xyz = 1$.

Recall (see e.g. [5]) that for ω a primitive n^{th} root of unity ($n > 1$), the norm of $1 - \omega$ in the n^{th} cyclotomic field $\mathbb{Q}_n = \mathbb{Q}(\omega)$ is

$$N_{\mathbb{Q}_n/\mathbb{Q}}(1 - \omega) = \prod_{\substack{1 \leq j < n \\ (j,n)=1}} (1 - \omega^j) = \begin{cases} 1 & \text{if } n \text{ is not a prime power,} \\ p & \text{if } n \text{ is a power of the prime } p. \end{cases}$$

Moreover, $-\omega$ is also a primitive n^{th} root of unity if n is even and a primitive $(2n)^{th}$ root of unity otherwise. Consequently,

$$N_{\mathbb{Q}_{2n}/\mathbb{Q}}(1 + \omega) = \begin{cases} 2^{\phi(2n)} & \text{if } \omega = 1, \\ 0 & \text{if } \omega = -1, \\ 2^{\phi(2n)/2^{\alpha-1}} & \text{if } \omega \text{ is a primitive } (2^\alpha)^{th} \text{ root of unity, } \alpha \geq 2, \\ 1 & \text{otherwise.} \end{cases}$$

By the multiplicative property of the norm, equality (1) can hold only if

- (i) one of x, y, z (say x) is 1, or

- (ii) one of x, y, z (say x) is a primitive 4^{th} root of unity, while y and z are primitive 8^{th} roots of unity.

In the first case we have $\epsilon = \eta$, and with $u = \zeta/\epsilon$, $\mathrm{Per}V(\epsilon, \eta, \zeta) = \epsilon^3 \mathrm{Per}V(1, 1, u) = 2\epsilon^3(1+u+u^2)$ is 0 if and only if u is a primitive 3^{rd} root of unity, in which case (ϵ, η, ζ) is indeed a bad sequence.

In the second case $\mathrm{Per}V(\epsilon, \eta, \zeta) = \epsilon^3 \mathrm{Per}V(1, x, xy)) = \epsilon^3((x-1) - y^2(1+x))$ is 0 if and only if $y^2 = x = \pm i$. This, however, yields no bad sequences, see Example 1.

Consequently, $A = (a_1, a_2, a_3)$ is a bad sequence in $\mathbb{Z}_n$ if and only if n is divisible by 3, and for some permutation (i, j, k) of the indices $(1, 2, 3)$, $a_i = a_j = a_k \pm n/3$.

These results could have certainly been obtained without any algebraic consideration. We only worked them out to indicate that there may be further applications of our method. The above calculations also yield to an alternative proof of Theorem 1, and suggest that being bad is a local property.

2^{nd} proof of Theorem 1. Identify $G \cong \mathbb{Z}_n$ with a subgroup of $\mathbb{C}^\times$ and suppose $a_1, a_2, \dots, a_k$ are all n^{th} roots of unity, n odd. Note that $\mathrm{Per}V(a_1, \dots, a_k) = \mathrm{Det}V(a_1, \dots, a_k) + 2A = \prod_{1 \le j < i \le k}(a_i - a_j) + 2A$, where $A \in \mathbb{Q}_n$ is an algebraic integer. Were $\mathrm{Per}V(a_1, \dots, a_k) = 0$ we would have $\prod_{1 \le j < i \le k}(1 - a_j/a_i) = 2B$ with an algebraic integer $B \in \mathbb{Q}_n$. The norm of the right hand side in $\mathbb{Q}_n$ is divisible by $N(2) = 2^{\phi(n)}$. On the other hand, if a_j/a_i is a primitive m^{th} root of unity for some divisor m of n, then $N_{\mathbb{Q}_n/\mathbb{Q}}(1 - a_j/a_i) = (N_{\mathbb{Q}_m/\mathbb{Q}}(1 - a_j/a_i))^{\phi(n)/\phi(m)}$ is an odd integer, unless $m = 1$. Consequently, $(a_1, a_2, \dots, a_k)$ cannot be a bad sequence, unless there are indices $1 \le j < i \le k$ with $a_i = a_j$. □

Problem 1 *Is it true that, if $A = (a_1, a_2, \dots, a_k)$ is a bad sequence in an Abelian group G, then there exists a subgroup $H \le G$ with $|H| = k$, a bad sequence $A' = (a'_1, a'_2, \dots, a'_k)$ in H, and an element $c \in G$ such that $a_i = a'_i + c$ for every $1 \le i \le k$?*

If true, it would settle down Snevily's other conjectures mentioned in the introduction. Indeed, assume that the answer is yes. Let first G be any Abelian group of odd order which contains a bad set $A = \{a_1, \dots a_k\}$. It follows that $\{a'_1, \dots, a'_k\}$ is a bad set in a k-element subgroup H of G. That is, H itself is a bad set in H, a contradiction, since k is odd. Thus, Snevily's conjecture [6, Conjecture 3] follows. Next, let $A = \{a_1, \dots a_k\}$ be a bad set in $\mathbb{Z}_n$, n even. Then again, $A' = H$ is a bad set in $H \cong \mathbb{Z}_k$, which can only happen if k is even. Moreover, A is a translate of $A' = H$, implying [6, Conjecture 2] as well.

5 Beyond permanents

The proof of Theorem 2 which uses Lemma 5 can be modified to attack this second conjecture. Unfortunately, we cannot replace permanents with determinants by using a field of characteristic 2 as before, since such a field will not contain a primitive nth root of unity. However, we may work again within the complex numbers. Let $\{w_1, \cdots, w_k\}$ and $\{x_1, \dots, x_k\}$ be nth roots of unity in $\mathbb{C}^\times$ representing the rows and columns of a $k \times k$ sub-matrix of the multiplication table of the unique n-element cyclic subgroup of $\mathbb{C}^\times$. Snevily's conjecture will then follow from the following conjecture.

Conjecture 2 *Suppose that $w_1, \dots, w_k$ are pairwise distinct nonzero complex numbers, as are $x_1, \dots, x_k$. If for each permutation $\pi \in S_k$ we have*

$$P_\pi = \prod_{1 \le j < i \le k} (w_i x_{\pi(i)} - w_j x_{\pi(j)}) = 0,$$

then

$$w_1^k = w_2^k = \cdots = w_k^k$$

and

$$x_1^k = x_2^k = \cdots = x_k^k.$$

Given that the w_i are distinct, $w_1^k = w_2^k = \cdots = w_k^k$ implies that $w_1 w_2 \cdots w_k = (-1)^{k-1} w_1^k$. Therefore, the equations $w_1^k = w_2^k = \cdots = w_k^k$ are equivalent to the $k-1$ elementary symmetric equations

$$\begin{aligned} E_1(w) = w_1 + w_2 + \cdots + w_k &= 0 \\ E_2(w) = w_1 w_2 + w_1 w_3 + \cdots + w_{k-1} w_k &= 0 \\ &\vdots \\ E_{k-1}(w) = w_1 w_2 \cdots w_{k-1} + \cdots + w_2 w_3 \cdots w_k &= 0 \end{aligned}$$

since the polynomial of degree k satisfied by the w_i is then

$$(x - w_1)(x - w_2) \cdots (x - w_k) = x^k + (-1)^k w_1 w_2 \cdots w_k.$$

To attempt to show that these symmetric equations indeed hold when the P_π are zero (as in Conjecture 2), we algebraically manipulate the P_π. For example, we find that

$$\sum_{\pi \in S_k} P_\pi \cdot w_{\pi^{-1}(i)} = \mathrm{Det} V(w) E_1(w) \left(\sum_{\substack{\sigma \in S_k \\ \sigma(1) = i}} x_{\sigma(1)}^{k-1} x_{\sigma(2)}^{k-2} \cdots x_{\sigma(k)}^0 \right). \tag{2}$$

Thus, if each $P_\pi = 0$, then since the w_i are distinct, we have either $E_1(w) = 0$ or else

$$\sum_{\substack{\sigma \in S_k \\ \sigma(1) = i}} x_{\sigma(1)}^{k-1} x_{\sigma(2)}^{k-2} \cdots x_{\sigma(k)}^0 = 0$$

for each $i = 1, \dots, k$. Perhaps it is true that the last equation cannot hold for all i when the x_i are distinct. If this is the case, we will indeed have $E_1(w) = 0$.

Problem 3 *Let $x_1, \dots, x_k$ be nonzero complex numbers such that for each $i = 1, \dots, k$,*

$$\sum_{\substack{\sigma \in S_k \\ \sigma(1) = i}} x_{\sigma(1)}^{k-1} x_{\sigma(2)}^{k-2} \cdots x_{\sigma(k)}^0 = 0.$$

Then is it true that some pair of the x_i's must be equal?

For the other equations $E_j(w)=0$, we use a similar formula. For pairwise distinct $i_1, i_2, \ldots, i_j$ in $\{1,\ldots,k\}$, we have

$$\sum_{\pi\in S_k} P_\pi \cdot w_{\pi^{-1}(i_1)}\cdots w_{\pi^{-1}(i_j)} = \mathrm{Det}V(w)E_j(w)\left(\sum_{\substack{\sigma\in S_k\\ \sigma(\{1,2,\ldots j\})=\{i_1,\ldots,i_j\}}} x_{\sigma(1)}^{k-1}x_{\sigma(2)}^{k-2}\cdots x_{\sigma(k)}^{0}\right). \qquad (3)$$

An affirmative answer to the following question (which generalizes the previous question) would then prove Snevily's conjecture for even n:

Problem 4 *Let $x_1,\ldots,x_k$ be nonzero complex numbers, and let j be a fixed integer between* 1 *and $k-1$. Suppose that for each set $T\subset\{1,\ldots,k\}$ of size j, we have*

$$\sum_{\substack{\sigma\in S_k\\ \sigma(\{1,2,\ldots j\})=T}} x_{\sigma(1)}^{k-1}x_{\sigma(2)}^{k-2}\cdots x_{\sigma(k)}^{0} = 0.$$

Is it then true that some pair of the x_i's must be equal?

Even if we cannot verify these conjectures, equalities (2), (3) can be useful in proving that certain sequences are not bad. For example, let, as in Example 1, $G\cong\mathbb{Z}_8$ be the subgroup of the multiplicative group of some field, and $A=\{x_1=1, x_2=g^2, x_3=g^3\}$ where g is a generator for G. Since the minimal polynomial of g is x^4+1, no three elements of G can add up to 0. Thus, if w_1, w_2, w_3 are distinct elements of G, then $\mathrm{Det}V(w)\neq 0$ and $E_1(w)\neq 0$. Moreover, $x_1^2x_2+x_1^2x_3=x_1^2(x_2+x_3)\neq 0$, and it follows from equality (2) that $\sum_{\pi\in S_3}P_\pi\cdot w_{\pi^{-1}(1)}\neq 0$. Consequently, there is a $P_\pi\neq 0$, and A is not a bad sequence.

References

[1] N. Alon, Combinatorial Nullstellensatz, Combinatorics, Probability and Computing **8** (1999) 7–29.

[2] N. Alon, Additive Latin transversals, Israel J. Math. **117** (2000) 125–130.

[3] Y.F. Bilu, V.F. Lev, and I.Z. Ruzsa, Rectification principles in additive number theory, Discrete Comput. Geom. **19** (1998) 343–353.

[4] Gy. Károlyi, A compactness argument in the additive theory, in preparation.

[5] S. Lang, Algebraic Number Theory (2nd Edition), GTM **110**, Springer, 1994.

[6] H. Snevily, The Cayley addition table of Z_n, Amer. Math. Monthly **106** (1999) 584–585.