9.3 Snevily's conjecture

In [322], Snevily made the following conjecture.

Conjecture 9.15 (Snevily's conjecture) *[322] Let Z be an additive group of odd order and let A, B be two additive sets in Z with $|A| = |B|$. Then there is a bijection $\phi : A \to B$ such that the sums $\{a + \phi(a) : a \in A\}$ are all distinct.*

The general case of this conjecture remains open, but many special cases are known. For instance, using the combinatorial Nullstellensatz, Alon [5] showed that the conjecture holds for cyclic groups of prime order.

Theorem 9.16 *[5] Let $F = F_p$ where $p > 2$ is an odd prime and let A, B be two additive sets in F with $|A| = |B|$. Then there is a bijection $\phi : A \to B$ such that the sums $\{a + \phi(a) : a \in A\}$ are all distinct.*

Proof If $A = B$ then one can simply choose π to be the identity map, taking advantage of the fact that p is odd, so we may assume $A \neq B$. In particular we can take $|A| = |B| < p$. Enumerate $A = \{a_1, \ldots, a_k\}$, and let $P \in F[t_1, \ldots, t_k]$ be the polynomial

$$P(t_1, \ldots, t_k) = \prod_{1 \leq i < j \leq k} (t_j - t_i)(t_j - t_i + a_i - a_j).$$

Then $\deg(P) = k(k-1)$. Also, from Theorem 9.11, the coefficient of $x_1^{k-1} \cdots x_k^{k-1}$ in P is $k! \cdot 1$, which is non-zero in F_p since $k < p$. Applying the combinatorial Nullstellensatz, there is an $s_i \in S_i$ such that $P(s_1, \ldots, s_k) \neq 0$. This means $s_j - s_i \neq 0$ and $s_j - s_i + a_i - a_j \neq 0$ for all $1 \leq i < j \leq k$. If we then define $\phi : A \to B$ by setting $\phi(a_i) := s_i$ we thus see that ϕ is injective (hence surjective), and that the sums $a_i + \phi(a_i) = a_i + s_i$ are all distinct, as desired. □

Let us notice that in the case $k < p$, we never used the assumption that the elements of A are different, and in this case one can in fact generalize to arbitrary fields of characteristic p or 0; see Exercise 9.3.2. Also, observe that the proof only used a very special case of Dyson's conjecture. Using this conjecture in full generality and modifying the rest of the proof accordingly, we have the following more general result.

Theorem 9.17 *Let $F = F_p$ a field of prime order, let $k < p$, and let $R_1, \ldots, R_k$ be additive sets in F_p, such that $\sum_{i=1}^{k} |R_i| < p$. Let $a_1, \ldots, a_k \in F_p$, and let $B_1, \ldots, B_k$ be subsets of F_p with cardinality $|B_i| > (k-1)(r_i + 1)$. Then there are k pairwise distinct elements $\{b_1, \ldots, b_k\}$, where $b_i \in B_i$, such that the sums $a_i + b_i$ are pairwise distinct and for every $i \neq j$, $a_i + b_i - (a_j + b_j) \notin R_i$.*

Proof Let $P \in F[t_1, \ldots, t_k]$ be the polynomial

$$P(t_1, \ldots, t_k) := \left[\prod_{1 \le i < j \le k} (t_i - t_j)(a_i + t_i - a_j - t_j) \right] \times \prod_{i,j \in [1,k]: i \ne j} \prod_{r \in R_i} (a_i + t_i - a_j - t_j - r).$$

Then $\deg(P) = \sum_{i=1}^{k} (k-1)(|R_i| + 1)$. Also, by Theorem 9.11 the coefficient of $\prod_{1 \le i \ne j \le k} \prod_{r \in R_i} x_i^{(k-1)(|R_i|+1)}$ in P is, up to sign,

$$\pm \frac{\left(\sum_{i=1}^{k} (|R_i| + 1)\right)!}{\prod_{i=1}^{k} (|R_i| + 1)!} \cdot 1$$

which is non-zero in F_p, since $\sum_{i=1}^{k} (r_i + 1) < p$ by the assumption of the theorem. The claim now follows from the combinatorial Nullstellensatz. □

DasGupta, Károly, Serra and Szegedy [67] obtained a multiplicative version of Snevily's conjecture. Define the *Vandermonde permanent* $\mathrm{Per}_n(x_1, \ldots, x_n)$ of n variables to be the quantity

$$\mathrm{Per}_n(x_1, \ldots, x_n) = \sum_{\pi \in S_n} \prod_{i=1}^{n} x_i^{\pi(i)-1}$$

(cf. (9.3).)

Lemma 9.18 *[67] Let F be an arbitrary field and $a_1, \ldots, a_k$ be elements of F. Assume that the Vandermonde permanent $\mathrm{Per}_k(a_1, \ldots, a_k)$ is non-zero. The for any subset $B = \{b_1, \ldots, b_k\}$ of F there is a permutation $\pi \in S_k$ such that the products $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are all distinct.*

Proof Let $f \in F[t_1, \ldots, t_k]$ be the polynomial

$$f(t_1, \ldots, t_k) := \Delta_k(t_1, \ldots, t_k) \Delta_k(a_1 t_1, \ldots, a_k t_k).$$

Then $\deg(f) \le k(k-1)$. Set $S_1 = B, \ldots, S_k = B$. By the combinatorial Nullstellensatz, it suffices to show that the coefficient of $t_1^{k-1} \ldots t_k^{k-1}$ is not zero. Notice that

$$\begin{aligned} f(t_1, \ldots t_k) &= \left(\sum_{\pi \in S_k} (-1)^{\sigma(\pi)} \prod_{i=1}^{k} t_{\pi(i)}^{i-1} \right) \left(\sum_{\tau \in S_k} (-1)^{\sigma(\tau)} \prod_{i=1}^{k} (a_{\tau(i)} t_{\tau(i)}^{i-1} \right) \\ &= \left(\sum_{\pi \in S_k} (-1)^{\sigma(\pi)} \prod_{i=1}^{k} t_{\pi(i)}^{i-1} \right) \left(\sum_{\pi \in S_k} (-1)^{\binom{k}{2} - \sigma(\pi)} \prod_{i=1}^{k} (a_{\pi(i)} t_{\pi(i)})^{k-i} \right). \end{aligned}$$

Thus the coefficient in concern is exactly

$$\sum_{\pi\in S_k}(-1)^{\binom{k}{2}}\prod_{i=1}^{k}a_{\pi(i)}^{i-1}=(-1)^{\binom{k}{2}}\mathrm{Per}_k(a_1,\ldots,a_k)\cdot 1,$$

which is not zero due to the assumption of the lemma. The proof is thus complete. (For an alternative proof, see Exercise 9.3.3.) □

One can convert this multiplicative statement to an additive statement by embedding additive group as a multiplicative subgroup of a suitable field. For instance, one can now show that Snevily's conjecture holds for cyclic groups of odd order:

Corollary 9.19 *[67] Let $n \geq 1$ be an odd number, and let A, B be two additive sets in $\mathbf{Z}_n$ such that $|A| = |B|$. Then there exists a bijection $\phi : A \to B$ such that the sums $\{a + \phi(a) : a \in A\}$ are all distinct.*

Proof We shall use the theory of finite fields, which we shall review in Section 9.4. Let $\mathbf{Z}_n^\times$ be the multiplicatively invertible elements of n, and let $\phi(n) := |\mathbf{Z}_n^\times|$ be the Euler totient function of n. By Cauchy's theorem (Exercise 3.1.2), we have $2^{\phi(n)} = 1 \pmod{n}$. Let F be a finite field of order $2^{\phi(n)}$ and characteristic 2 (the existence of such a field follows from Exercise 9.4.4). From Lemma 9.22, the multiplicative group $F^\times$ of F contains an element of order n, and hence contains a subgroup G isomorphic to the additive group $\mathbf{Z}_n$. It now suffices to verify the multiplicative form of Snevily's conjecture for G. But if $A = \{a_1, \ldots, a_k\}$ is a subset of G, then since F has characteristic 2 one can replace permanents with determinants and compute

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

The claim now follows from Lemma 9.18. □

A variant of this argument gives a strengthened version of the above result when the cyclic group has order p^k.

Theorem 9.20 *[67] Let $p > 2$ be an odd prime, let $q = p^\alpha$ be power of p for some $\alpha > 1$, let $1 \leq k < p$, and let $a_1, \ldots, a_k$ be elements of $\mathbf{Z}_q$. Then for any set $B = \{b_1, \ldots, b_k\} \subseteq \mathbf{Z}_q$ of cardinality k, there exists a permutation $\pi \in S_k$ such that the sums $a_i + b_{\pi(i)}$, $1 \leq i \leq k$ are all distinct.*

Proof We will need the machinery of cyclotomic fields, which we shall review in Section 9.8. Let ω be a primitive qth root of unity, and let $\mathbf{Q}(\omega)$ be the associated cyclotomic field. Observe that $\mathbf{Q}(\omega)$ contains the multiplicative subgroup $G := \{\xi^n : n \in \mathbf{Z}\} \subset \mathbf{Q}(\omega)$ which is group isomorphic to the additive group $\mathbf{Z}_q$. Thus it suffices to show that for any $a_1, \ldots, a_k \in G$ and any $B = \{b_1, \ldots, b_k\} \subseteq G$