5 Subsequence Sums II: length = $|G|$

In this section, we shall concern ourselves with a restricted subsequence sum problem, and except where explicitly noted, we will consider only finite abelian groups. For every (additive) abelian group G, we define the *order length Davenport constant* $D^{ord}(G)$ to be the smallest integer ℓ so that every sequence of elements from G of length $\geq \ell$ has a subsequence of length $|G|$ with sum equal to 0. Our main theorem from this section is a result of Gao which proves that $D^{ord}(G) = D(G) + |G| - 1$ for every abelian group G. The following observation establishes the easy inequality between these quantities.

Observation 5.1 $D^{ord}(G) \geq D(G) + |G| - 1$

Proof: If $\alpha = a_1, a_2, \ldots a_{D(G)-1}$ is a sequence of elements of G without a nontrivial subsequence which sums to zero, then the sequence α' consisting of $|G| - 1$ zeros followed by α has length $D(G) + |G| - 2$ and does not have a subsequence of length $|G|$ which has sum zero. $\square$

For instructional purposes, we begin with an investigation of groups of prime order. Fixing a prime p, we will give two proofs of $D^{ord}(\mathbb{Z}_p) = 2p - 1$. This fact has numerous interesting proofs (see Alon-Dubiner for several more).

Proposition 5.2 $D^{ord}(\mathbb{Z}_p) = 2p - 1$

Proof: Let $a_1, a_2, \ldots, a_{2p-1}$ be a sequence in $\mathbb{Z}_p$, and consider the following two polynomials in the variables $x_1, x_2, \ldots, x_{2p-1}$ over the field $\mathbb{Z}_p$.

$$\sum_{i=1}^{2p-1} x_i^{p-1} \qquad\qquad \sum_{i=1}^{2p-1} a_i x_i^{p-1}$$

Since $(x_1, \ldots, x_{2p-1}) = (0, 0, \ldots, 0)$ is a common zero of these two polynomials, it follows from the Chevalley-Warning theorem, that there is another, say $(z_1, z_2, \ldots, z_{2p-1})$. Setting $I = \{1 \leq i \leq 2p - 1 : z_i \neq 0\}$ we find that $|I| = p$ and that $\sum_{i \in I} a_i = 0$, completing the proof. $\square$

Our next proof of $D^{ord}(\mathbb{Z}_p) = 2p - 1$ achieves a much stronger result. To state it we will need a little further terminology. If $\alpha = a_1, \ldots, a_\ell$ is a sequence in the group G, we let $\rho(\alpha)$

denote the maximum over all $g \in G$ of the number of occurrences of g in α. If k is a positive integer, we define the following two sets.

$$\begin{aligned} \Sigma_k(\alpha) &= \{a_{i_1} + a_{i_2} + \ldots + a_{i_k} : 1 \leq i_1 < i_2 \ldots < i_k \leq \ell\} \\ \Sigma_{\leq k}(\alpha) &= \cup_{i=1}^{k} \Sigma_i(\alpha) \end{aligned}$$

So $\Sigma_k(\alpha)$ ($\Sigma_{\leq k}(\alpha)$) is the set of all possible sums of nontrivial subsequences of α of length k (length $\leq k$).

Proposition 5.3 *If $\alpha = a_1, \ldots, a_{2p-1}$ is a sequence in $\mathbb{Z}_p$, then one of the following holds*

- $\rho(\alpha) \geq p$
- $\Sigma_p(\alpha) = \mathbb{Z}_p$

Proof: Identify the elements of $\mathbb{Z}_p$ with the representatives $0, 1, \ldots, p-1$ as usual. By possibly reordering our sequence, we may assume that $a_1 \leq a_2 \ldots \leq a_{2p-1}$. If there exists $1 \leq i \leq p-1$ so that $a_i = a_{p-1+i}$ then $\rho(\alpha) \geq p$ and we are finished. Otherwise the set $\{a_i, a_{p-1+i}\}$ has size 2 for every $1 \leq i \leq p-1$ so by repeatedly applying the Cauchy-Davenport Theorem we find that the sumset

$$A = \{a_1, a_p\} + \{a_2, a_{p+1}\} \ldots + \{a_{p-1}, a_{2p-2}\} + \{a_{2p-1}\}$$

has size p. Since $A \subseteq \Sigma_p(\alpha)$, this yields the desired result. $\square$

We will now proceed with the proof of Gao's theorem. Our proof will require the following key lemma.

Lemma 5.4 *Let $\alpha = a_1, \ldots, a_\ell$ be a sequence in G and let $\rho = \rho(\alpha)$. If $0 \notin \Sigma_{\leq\rho}(\alpha)$, then $|\Sigma_{\leq\rho}(\alpha)| \geq \ell$.*

Proof: Partition the elements of our sequence into ρ sets $A_1, A_2, \ldots, A_\rho$ (so the multiplicity of any element g in the sequence is equal to the number of sets A_i which contain it). For $1 \leq i \leq \rho$ let $A'_i = A_i \cup \{0\}$. Now consider the sumset $\sum_{i=1}^{\rho} A'_i$. It follows from our assumptions that $\{(a_1, a_2, \ldots, a_\rho) \in A'_1 \times \ldots A'_\rho : \sum_{i=1}^{\rho} a_i = 0\} = \{(0, 0, \ldots, 0)\}$. Thus, by repeatedly applying Theorem 3.1 we have

$$|\sum_{i=1}^{\rho} A'_i| \geq (\sum_{i=1}^{\rho} |A'_i|) - (\rho - 1) = (\sum_{i=1}^{\rho} |A_i|) + 1 = \ell + 1.$$

Since $A \setminus 0 \subseteq \Sigma_{\leq\rho}(\alpha)$, this completes the proof. $\square$

Theorem 5.5 (Gao) *$D^{ord}(G) = D(G) + |G| - 1$ for every abelian group G.*

Proof: By Observation 5.1 it suffices to prove $D^{ord}(G) \leq D(G) + |G| - 1$. Set $m = D(G) + |G| - 1$ and let $\alpha = a_1, a_2, \ldots, a_m$ be a sequence in G. Adding a fixed element to every a_i does not change $\Sigma_{|G|}(\alpha)$. By such a shift, we may now assume that 0 appears $\rho = \rho(\alpha)$ times in α. Let $R = \{1 \leq i \leq m : a_i = 0\}$. Next, choose a maximal collection of pairwise disjoint subsets $\{S_1, S_2, \ldots, S_k\}$ of $\{1, 2, \ldots, m\} \setminus R$ so that $|S_j| \leq \rho$ and $\sum_{i \in S_j} a_i = 0$ for every j. Set $S = \cup_{j=1}^{k} S_j$ and note that by the previous corollary $|R| + |S| \geq D(G)$. Finally, choose a maximal collection of pairwise disjoint subsets $\{T_1, T_2, \ldots, T_\ell\}$ of $\{1, 2, \ldots, m\} \setminus (R \cup S)$ so that $|T_j| \leq D(G)$ and $\sum_{i \in T_j} a_i = 0$ for every j. Set $T = \cup_{j=1}^{\ell} T_j$ and note that by the definition of $D(G)$ we must have $|R| + |S| + |T| \geq |G|$. Since every T_j has size $\leq D(G) \leq |R| + |S|$ and every S_j has size $\leq |R|$ there is a subset $I \subseteq R \cup S \cup T$ with size $|G|$ (respecting the partitions of S and T) so that $\sum_{i \in I} a_i = 0$ as desired. □

A corollary of this theorem is the following classic result.

Corollary 5.6 (Erdös, Ginzburg, and Ziv) $D^{ord}(G) \leq 2|G| - 1$

Proof: This follows immediately from Observation 4.1 and the previous theorem. □

In fact, the Erdös, Ginzburg, Ziv theorem reduces easily to the special case when $|G|$ is prime. This observation combined with a proof of $G^{ord}(\mathbb{Z}_p) = 2p - 1$ is the structure of the original argument. To see the reduction, let $H \leq G$, let $s = |H|$ and $t = |G/H|$ and assume that $D^{ord}(H) \leq 2s - 1$ and $D^{ord}(G/H) \leq 2t - 1$. If $\alpha = a_1, a_2, \ldots, a_{2st-1}$ is a sequence in G, then by repeatedly applying $D^{ord}(G/H) \leq 2t - 1$ we may find a collection of $2s - 1$ disjoint subsequences of α each with length t and sum in H. It now follows from $D^{ord}(H) \leq 2s - 1$ that we may choose s of these subsequences with total sum 0, giving us a zero sum subsequence of the desired length.

We finish the proofs from this section with a result which gives another generalization of the Erdös-Ginzburg-Ziv theorem. Our proof of this result is due to Hong Bing Yu.

Theorem 5.7 (Bollobas, Leader) *Let $|G| = n$ and let $\alpha = a_1, a_2, \ldots, a_{n+\ell}$ be a sequence in G. Then one of the following holds.*

- $0 \in \Sigma_n(\alpha)$

- $|\Sigma_n(\alpha)| \geq \ell + 1$

Proof: By adding a fixed element to every a_i we may assume that 0 occurs $\rho = \rho(\alpha)$ times in α. Let $R = \{1 \leq i \leq n + \ell : a_i = 0\}$, and choose a maximal set $S \subseteq \{1, 2, \ldots, n + \ell\} \setminus R$ so that $|S| \leq n$ and $\sum_{i \in S} a_i = 0$. If $|S| \geq n - \rho$, then $0 \in \Sigma_n(\alpha)$ and we are finished. Otherwise, choose a set J with $S \subseteq J \subseteq \{1, 2, \ldots, n + \ell\} \setminus R$ with size $n - \rho$, set $a = \sum_{i \in J} a_i$, and set $Q = \{1, 2, \ldots, n + \ell\} \setminus (R \cup J)$. It follows from the maximality of S and the observation that $|S| \leq n - \rho$ that there does not exist a zero sum subsequence of length $\leq \rho$ with indices in Q. It now follows from Lemma 5.4 that $|\Sigma_{\leq \rho}(\alpha|_Q)| \geq \ell$. Every length $\leq \rho$ subsequence (even the trivial one) of $\alpha|_Q$ with sum b may be extended to a subsequence of α of length n and sum $a + b$ by extending this subsequence to include all those elements with index in J together with an appropriate number with index in R. Thus $|\Sigma_n(\alpha)| \geq \ell + 1$ □

For finite nonabelian groups, Olson proved that the Erdös-Ginzburg-Ziv theorem still holds if reordering is permitted. More precisely, if G is any multiplicative group of order n and $a_1, \ldots, a_{2n-1}$ is a sequence of elements in G, then there is a subsequence which has product equal to 1 in some order. The following interesting conjecture asserts that this reordering is not needed.

Conjecture 5.8 (Olson) *If $\alpha = a_1, a_2, \ldots, a_{2n-1}$ is a sequence of elements from a (multiplicative) group of order n, then there is an n element subsequence of α which has product equal to one in the given order.*