4 Subsequence Sums I: the Davenport Constant

Here we turn our attention to a different type of combinatorial problem, namely subsequence sums. To set the stage, we begin by defining a fundamental parameter, first suggested by Davenport. Let G be a finite multiplicative group. We define the *Davenport Constant* of G, denoted $D(G)$, to be the smallest integer ℓ so that every sequence of $a_1, a_2, \ldots, a_\ell$ from G has a nontrivial subsequence with product equal to 1 (in the given order). We begin with a rather trivial upper bound on $D(G)$, and an easy lower bound on $D(G)$ for abelian groups.

Observation 4.1 *$D(G) \leq |G|$ for every group G.*

Proof: Let $|G| = n$ and let $a_1, a_2, \ldots, a_n$ be a sequence in G. Now for $k = 1 \ldots, n$ let $b_k = \prod_{i=1}^{k} a_i$. If there exists $1 \leq k \leq n$ with $b_k = 1$ then we are finished. Otherwise, there must exist $1 \leq j < k \leq n$ with $b_j = b_k$. Then $\prod_{i=j+1}^{k} a_i = b_j^{-1} b_k = 1$. $\square$

Observation 4.2 *If $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \ldots \mathbb{Z}_{n_r}$, then $D(G) \geq 1 + \sum_{i=1}^{r}(n_i - 1)$.*

Proof: A sequence consisting of $n_i - 1$ copies of the vector with a 1 in the i^{th} position and 0 elsewhere for every $1 \leq i \leq r$ has no nontrivial zero sum subsequence. This establishes the desired bound. $\square$

For $\mathbb{Z}_n$, our upper and lower bounds match, so we get the following.

Observation 4.3 *$D(\mathbb{Z}_n) = n$*

We have now established the Davenport constant for cyclic groups. Shortly, we will see a beautiful theorem of Olson which establishes it for all abelian groups whose order is a power of a prime. Unfortunately, little more is known about this interesting parameter. For the remainder of this section, we fix a prime p, and we shall proceed toward Olson's theorem by first studying the groups $\mathbb{Z}_p$ and $\mathbb{Z}_p^n$, where we will achieve somewhat stronger results. We begin with a nice property of $\mathbb{Z}_p$ which follows easily from the Cauchy-Davenport Theorem.

Corollary 4.4 *If $\alpha = a_1, a_2, \ldots, a_p$ is a sequence of nonzero elements in $\mathbb{Z}_p$, then for every $g \in \mathbb{Z}_p$ there is a nontrivial subsequence of α with sum equal to g.*

Proof: Consider the sumset $A = \{a_1\} + \{0, a_2\} + \{0, a_3\} + \ldots + \{0, a_p\}$. Every member of A is the sum of a subsequence of α, and by repeatedly applying the Cauchy-Davenport theorem, we have $|A| \geq p$. $\square$

Next we shall consider the group $\mathbb{Z}_p^n$. This group may be viewed as a vector space over the field $\mathbb{Z}_p$, and this structure is the inspiration for our next theorem. A familiar fact from linear algebra is that the set of common solutions to a family of linear equations is a (possibly empty) affine subspace whenever there are more variables than equations. In a vector space over a field of characteristic p, this implies that the set of common solutions always has size a multiple of p (again assuming there are more variables then equations). Our next result is a generalization of this fact to polynomials of higher degree. For this, we'll need first one easy fact about finite fields.

Proposition 4.5 *If $\mathbb{F}$ is a field of order q, and $k < q-1$, then $\sum_{x \in \mathbb{F}} x^k = 0$.*

Proof: The multiplicative group of every finite field is cyclic (otherwise this group would have a subgroup of the form $\mathbb{Z}_r \times \mathbb{Z}_r$ and the polynomial $x^r - 1$ would have too many roots). If $z \in \mathbb{F}$ is a generator of the multiplicative group, then we have

$$\sum_{x \in \mathbb{F}} x^k = \sum_{i=0}^{q-2} z^{ki} = \frac{1 - z^{k(q-1)}}{1 - z^k} = 0$$

which completes the proof. $\square$

Theorem 4.6 (Chevalley-Warning) *For $1 \leq i \leq n$ let $P_i(x_1, x_2, \ldots, x_m)$ be a polynomial of degree d_i over the field $\mathbb{F}$ of characteristic p. If $\sum_{i=1}^n d_i < m$, then the number N of common zeros of $P_1, P_2, \ldots, P_n$ is a multiple of p.*

Proof: If $q = |\mathbb{F}|$, then we have

$$N \cong \sum_{x_1, \ldots, x_m \in \mathbb{F}} \prod_{j=1}^{n} (1 - P_j(x_1, \ldots, x_m)^{q-1}) \pmod p.$$

Expanding the right hand side gives us a linear combination of monomomials of the form

$$\prod_{i=1}^{m} x_i^{k_i} \quad \text{with} \quad \sum_{i=1}^{m} k_i < (q-1) \sum_{j=1}^{n} d_j < (q-1)m$$

so in each such monomial there exists an i with $k_i < q-1$. It now follows from the previous proposition that each such monomial contributes 0 (mod p) to the sum in the above equation. This completes the proof. $\square$

An easy corollary of this result gives us the Davenport constant for any group of the form $\mathbb{Z}_p^n$ as follows.

Corollary 4.7 $D(\mathbb{Z}_p^n) = n(p-1)+1$

Proof: Let $m = n(p-1)+1$ and let $\alpha = a_1, a_2, \ldots, a_m$ be a sequence in $\mathbb{Z}_p^n$. For every $1 \leq i \leq m$ let $a_i = (a_{i1}, a_{i2}, \ldots, a_{in})$ and for every $1 \leq j \leq n$ let $P_j = P_j(x_1, \ldots, x_m)$ be the polynomial over $\mathbb{Z}_p$ given by the following rule

$$P_j(x_1, \ldots, x_m) = \sum_{i=1}^{m} a_{ji} x_i^{p-1}$$

Here each x_i acts as a kind of indicator variable since $x_i^{p-1} = 1$ if $x_i \neq 0$. Since $(x_1, \ldots, x_m) = (0, 0, \ldots, 0)$ is a solution to this family of equations, it follows from the previous theorem that there is another solution $(z_1, \ldots, z_m)$. Let $I = \{1 \leq i \leq m : z_i \neq 0\}$. Then I is nonempty and by construction, $\sum_{i \in I} a_i = 0$. Thus, we have a nontrivial subsequence of α with zero sum as required. $\square$

Theorem 4.8 (Olson) *If* $G = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \ldots \times \mathbb{Z}_{p^{n_r}}$, *then* $D(G) = 1 + \sum_{i=1}^{r} (p^{n_i} - 1)$.

Proof: Breaking our usual convention, we will use multiplicative notation for G, and we let R denote the group ring of G over $\mathbb{Z}_p$ (so the elements of R are formal sums of elements in G with coefficients in $\mathbb{Z}_p$). Let $m = 1 + \sum_{i=1}^{r}(p^{n_i} - 1)$ and let $g_1, g_2, \ldots, g_m$ be a sequence in G. Now consider the following expression (computed in R)

$$h = (1 - g_1) \cdot (1 - g_2) \cdots (1 - g_m)$$

We claim that $h = 0$. To see this, define z_i to be the element in G with a 1 in coordinate i and a 0 in every other coordinate (so the order of z_i is p^{n_i}. Since each g_j can be written as a product of the elements z_i, by repeatedly applying the identity $1 - uv = (1-u) + u(1-v)$ we may expand each expression of the form $(1 - g_j)$ into a linear combination (with coefficients in R) of the elements $(1 - z_i)$. Substituting this into the above equation and applying commutativity, we conclude that the right-side is a linear combination of terms of the form

$$\prod_{i=1}^{r}(1 - z_i)^{k_i} \quad \text{where} \quad \sum_{i=1}^{r} k_i > m$$

Thus, for each such term there is an i with $k_i > n_i$ and in R, $(1 - z_i)^{p^{n_i}} = 0$. It follows that $h = 0$. But now observe that h cannot be 0 without there existing a nontrivial subsequence of $g_1, \ldots, g_m$ with product 1. This completes the proof. $\square$