§4. THE LITTLEWOOD-OFFORD PROBLEM

The aim of this brief section is to present Kleitman's beautiful solution to a problem of Littlewood and Offord. When studying the number of real zeros of random polynomials, Littlewood and Offord (1943) arrived at the following problem. Let $z_1, z_2, \ldots, z_n$ be complex numbers of modulus at least 1. Form all 2^n sums of the form $z_{i_1} + z_{i_2} + \ldots + z_{i_t}$, $1 \leq i_1 < i_2 < \ldots < i_t \leq n$. (The value of the empty sum is 0). At most how many of these sums can differ from each other by less than 1? Littlewood and Offord gave a bound which was good enough for their purpose (see also Littlewood (1982, vol. 2, pp. 1333–1344)) but a complete solution was found only considerably later.

Erdős (1945) noticed that for real numbers Sperner's theorem implies a best possible bound. Indeed, suppose $x_1, x_2, \ldots, x_n$ are real numbers of modulus at least 1. For $A \subset [n]$ set $x_A = \sum_{i \in A} x_i$ (by convention, $x_\emptyset = 0$). At most how many of the 2^n sums differ by less than 1 from each other. In this problem x_i may be replaced by $-x_i$ (replace A by $A \triangle \{i\}$ and x by $x - x_i$) so we may assume that $x_i \geq 1$ for every i. Let $\mathcal{F} \subset \mathcal{P}(X)$ be such that $|x_A - x_B| < 1$ for $A, B \in \mathcal{F}$. Then $\mathcal{F}$ is a Sperner system since if $A \subset B \subset [n]$ and $A \neq B$ then $|x_A - x| + |x_B - x| \geq x_B - x_A = x_{B \setminus A} \geq 1$ so at most one of A and B can belong to $\mathcal{F}$. Hence, by Theorem 2.1, $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$. This bound is clearly best possible: if $x_1 = x_2 = \ldots = x_n = 1$ then $\binom{n}{\lfloor n/2 \rfloor}$ of the sums x_A are $\lfloor n/2 \rfloor$.

Kleitman (1965) and Katona (1966) proved that the bound $\binom{n}{\lfloor n/2 \rfloor}$ holds for sums of complex numbers as well. In fact, Kleitman (1970) proved that, somewhat surprisingly, instead of complex numbers we may even take vectors in an arbitrary normed space. We shall present this latter proof since it is particularly simple and elegant.

The key idea in solving the Littlewood-Offord problem is to adapt a proof of Sperner's theorem to the setting of sums of vectors, rather than

simply apply Sperner's theorem. First let us have another look at $\mathcal{P}(X)$. In the proof of Theorem 3.1 we showed that $\mathcal{P}(X)$ can be partitioned into $\binom{n}{\lfloor n/2 \rfloor}$ chains. We shall show now that these chains can be chosen to be of a special form.

Call a chain $A_1 \subset A_2 \subset \ldots \subset A_k$ in $\mathcal{P}(X)$ *symmetric* if $|A_{i+1}| = |A_i| + 1$ and $|A_1| = n - |A_k|$. Thus a chain is symmetric if it goes from a level l to the level $k = n - l$, and has a set on every level between. In particular, every symmetric chain has a set at level $\lfloor n/2 \rfloor$. Can $\mathcal{P}(X)$ be partitioned into symmetric chains? If there is such a partition then, as every symmetric chain meets $X^{(\lfloor n/2 \rfloor)}$ in one set, there must be $\binom{n}{\lfloor n/2 \rfloor}$ non-empty chains in the partition.

It is rather tempting to dismiss this question and claim that the answer is a trivial "yes". To justify this claim, one has the following "solution". Say $n = 2m$ and partition the lower half $\bigcup_{k=0}^{m} X^{(k)}$ into chains, as in the proof of Theorem 2.1, each chain ending in an element of $X^{(m)}$, the middle level. The set $\mathcal{P}(X)$ being symmetric about $X^{(m)}$, the partition of the lower half can be flipped over to produce a partition of the upper half $\bigcup_{k=m}^{n} X^{(k)}$. The two partitions mesh together to produce a symmetric partition of $\mathcal{P}(X)$. Where is the hole in this argument? In the use of the symmetry: the upper half of $\mathcal{P}(X)$ does look like the lower half, but there is no symmetry mapping the lower half into the upper half and keeping the elements of $X^{(m)}$ fixed. Though the argument above is incorrect, the answer to the question is still "yes", but with a not entirely trivial proof.

Theorem 1. *$\mathcal{P}(X)$ can be partitioned into disjoint symmetric chains.*

Proof. Let us apply induction on $n = |X|$. For $n = 1$ there is nothing to prove so assume that $n > 1$ and the assertion holds for smaller values of n. Set $X = [n]$, $Y = [n-1]$ and let $\mathcal{P}(Y) = C_1 \cup C_2 \cup \ldots \cup C_s$ be a partition into non-empty symmetric chains. Note that each chain C_i contains precisely one set of size $\lfloor (n-1)/2 \rfloor$ so $s = \binom{n-1}{\lfloor (n-1)/2 \rfloor}$. Suppose $C_i = \{A_1, A_2, \ldots, A_k\}$, where $A_1 \subset A_2 \subset \ldots \subset A_k$. Set $C_i' = \{A_1, A_2, \ldots, A_k, A_k \cup \{n\}\}$ and $C_i'' = \{A_1 \cup \{n\}, A_2 \cup \{n\}, \ldots, A_{k-1} \cup \{n\}\}$. (For $k = 1$ we have $C_i'' = \emptyset$.) Then C_i' and C_i'' are symmetric chains and clearly

$$\mathcal{P}(X) = \bigcup_{i=1}^{s} C_i' \cup \bigcup_{i=1}^{s} C_i''. \tag{1}$$

Is this a partition? It is indeed. If $A \subset Y$ then only C_i' contains A where C_i is the chain in $\mathcal{P}(Y)$ containing A. If $A = B \cup \{n\}$ where $B \subset Y$

then $B \in C_i$ for some i. If B is the maximal element of C_i then C_i' is the only chain containing A, otherwise A is contained only in C_i''. ∎

A quick reading of the proof above seems to reveal a contradiction. How many chains are there in the partition (1) we constructed? Twice as many as in the partition of $\mathcal{P}(Y)$ we started out with, i.e. $2\binom{n-1}{\lfloor (n-1)/2 \rfloor}$. How many chains do we expect in a symmetric partition of $\mathcal{P}(X)$? Exactly $\binom{n}{\lfloor n/2 \rfloor}$. But $\binom{n}{\lfloor n/2 \rfloor} \neq 2\binom{n-1}{\lfloor (n-1)/2 \rfloor}$ if n is odd! What has gone wrong? Nothing at all, for we have $\binom{n}{\lfloor n/2 \rfloor}$ chains in a partition of $\mathcal{P}(X)$ into non-empty symmetric chains, while in (1) many of our chains may be empty. To be precise, if C_i consists of just one set, which then must be of size $(n-1)/2$, then $C_i'' = \emptyset$, so C_i'' is not included into the partition into non-empty chains. Thus, if $n = 2m$ then we do create $2\binom{2m-1}{m-1} = \binom{2m}{m}$ non-empty chains, but if $n = 2m+1$ then we create only

$$2\binom{2m}{m} - \left\{\binom{2m}{m} - \binom{2m-1}{m-1}\right\} = \binom{2m}{m} + \binom{2m-1}{m-1} = \binom{2m+1}{m}$$

chains, just the right number!

We formulate the main result, Kleitman's (1970) theorem, in terms of normed spaces, though the result does not become less surprising and beautiful if the reader substitutes a Euclidean space $\mathbb{R}^n$ for B.

Theorem 2. *Let B be a normed space and let $x_1, x_2, \ldots \in B$, $\|x_i\| \geq 1$, $i = 1, 2, \ldots$. Then there are at most $\binom{n}{\lfloor n/2 \rfloor}$ vectors of the form $x_{i_1} + x_{i_2} + \ldots + x_{i_t}$, $1 \leq i_1 < i_2 < \ldots < i_t \leq n$, $t = 0, 1, \ldots, n$, such that the difference of any two of these vectors has norm less than 1.*

Proof. For $A \subset [n]$ set $x_A = \sum_{i \in A} x_i$, just as in the argument about real numbers. Call a set $\mathcal{D} \subset \mathcal{P}([n])$ *sparse* if $A, B \in \mathcal{D}$ and $A \neq B$ imply $\|x_A - x_B\| \geq 1$. Call a partition $\mathcal{P}([n]) = \bigcup_{j=1}^{s} \mathcal{D}_j$ *symmetric* if $|\mathcal{D}_j| \in \{n+1, n-1, n-3, \ldots\} \setminus \{0\}$ and there are precisely $\binom{n}{i} - \binom{n}{i-1}$ sets $\mathcal{D}_j$ of order $n+1-2i$, $i = 0, 1, \ldots, \lfloor n/2 \rfloor$, where $\binom{n}{-1}$ is taken to be 0. Note that we must have $s = \binom{n}{\lfloor n/2 \rfloor}$. Note also that a partition of $\mathcal{P}([n])$ into non-empty symmetric chains is a symmetric partition — in fact, symmetric partitions have been defined by copying the numerical chracteristics of a partition into non-empty symmetric chains.

We shall prove somewhat more than claimed by Theorem 2, namely we shall show that $\mathcal{P}([n])$ has a symmetric partition into sparse sets. The proof of this is very similar to the proof of Theorem 1. We apply

induction on n. The case $n = 1$ being trivial, we assume that $n > 1$ and the assertion holds for smaller values of n. Let $\mathcal{P}([n-1]) = \bigcup_{j=1}^{s} \mathcal{D}_j$ be an appropriate symmetric partition. Let f be a support functional at x_n, i.e. let $f \in B^*$, $\|f\| = 1$ and $f(x_n) = \|x_n\| \geq 1$. (If B is the Euclidean space $\mathfrak{R}^n$ then we may assume that $x_n = (\xi, 0, 0, \ldots, 0)$, $\xi \geq 1$, and so f is the first coordinate functional: if $y = (\eta_1, \eta_2, \ldots, \eta_n)$ then $f(y) = \eta_1$.)

Let $\mathcal{D}_j = \{A_1, A_2, \ldots, A_k\}$ and let l be such that

$$f(x_{A_l}) \geq f(x_{A_i})$$

for $1 \leq i \leq k$.

Set $\mathcal{D}_j' = \{A_1, A_2, \ldots, A_k, A_l \cup \{n\}\}$ and $\mathcal{D}_j'' = \{A_1 \cup \{n\}, \ldots, A_{l-1} \cup \{n\}, A_{l+1} \cup \{n\}, \ldots, A_k \cup \{n\}\}$. Then, taking only the non-empty sets $\mathcal{D}_j'$, $\mathcal{D}_j''$, we obtain a symmetric partition of $\mathcal{P}([n])$.

It is clear that $\mathcal{D}_j''$ is sparse. But why is $\mathcal{D}_j'$ sparse? Because for $A_m \in \mathcal{D}_j'$ we have

$$\|x_{A_l \cup \{n\}} - x_{A_m}\| \geq f(x_{A_l \cup \{n\}} - x_{A_m})$$

$$= f(x_n) + f(x_{A_l}) - f(x_{A_m}) \geq f(x_n) \geq 1. \qquad \blacksquare$$

Corollary 3. *For $x \in B$ there are at most $\binom{n}{\lfloor n/2 \rfloor}$ sums of the form $x_{i_1} + x_{i_2} + \ldots + x_{i_t}$, $1 \leq i_1 < i_2 < \ldots < i_t \leq n$, $t = 0, 1, \ldots, n$ at distance less than $\frac{1}{2}$ from x.* $\blacksquare$

Exercises

1. Let $x, x_1, x_2, \ldots, x_n \in \mathfrak{R}^n$, with each x_i having length at least 1, and consider all 2^n sums $\sum_{i=1}^{n} \epsilon_i x_i$ where $\epsilon_i = 1$ or -1. Show that at most $\binom{n}{\lfloor n/2 \rfloor}$ of these sums are at a distance less than 1 from x. (This is the extension of the original form of the Littlewood-Offord lemma — it is equivalent to Theorem 2.)

2. Prove the following extension of Sperner's theorem (Theorem 3.1), due to Katona (1966). Let $X = X_1 \cup X_2$ be a partition of X and let $\mathcal{F} \subset \mathcal{P}(X)$ be a set system such that if $A, B \in \mathcal{F}$, $A \subset B$ and $A \neq B$ then $A \cap X_1 \neq B \cap X_1$ and $A \cap X_2 \neq B \cap X_2$. Then

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}.$$