LECTURE 8. EXTREMAL SET THEORY

1. Dilworth's theorem

Definition 1. *A* partially ordered set (poset) *is a pair* $P = (X, \leq)$ *where* X *is the* ground set *of* P *and* $\leq$ *is a* partial order *of* P*, i.e., satisfies*

(i) *(Reflexive)* $a \leq a$ *for all* $a \in S$.
(ii) *(Antisymmetry)* $a \leq b$ *and* $b \leq a$ *implies* $a = b$.
(iii) *(Transitivity)* $a \leq b$ *and* $b \leq c$ *implies* $a \leq c$.

Let P be a partially ordered set. A *chain* of P is a set of (distinct) elements $\{a_1, \cdots, a_k\} \subseteq P$ satisfying $a_i \leq a_j$ for all $i < j$. We say that two elements $a, b \in X$ are *incomparable* if neither $a \leq b$ nor $b \leq a$ holds. An *antichain* of P is a set of elements $\{a_1, \cdots, a_k\} \subseteq P$ such that a_i and a_j are incomparable for all $i, j \in [k]$. An element a is *maximal* if for all $b \in P$, either (i) $a \leq b$ or (ii) a and b are incomparable. Similarly define *minimal* elements.

A *chain decomposition* of a poset P is a partition $\mathcal{C}$ of its ground set into disjoint chains.

Proposition 2. *Let* P *be a poset and* $\mathcal{C}$ *be a chain decomposition of* P*. Then for every antichain* A *of* P*, we have* $|A| \leq |\mathcal{C}|$.

Proof. Let A be an antichain of P. Note that $|A \cap C| \leq 1$ for all $C \in \mathcal{C}$. Therefore $|A| \leq |\mathcal{C}|$. □

The following theorem proved by Dilworth in 1950 is a fundamental theorem in the study of posets. It is a min/max type theorem extending Proposition 2.

Theorem 3. *(Dilworth 1950) Let* P *be a poset. Then there exists an antichain* A *and a chain decomposition* $\mathcal{C}$ *satisfying* $|\mathcal{C}| = |A|$.

Proof 1. We prove the statement by induction on the number of elements n of P. The statement trivially holds if $n = 0$.

Let P be a poset with n elements and suppose the theorem has been proven for all smaller values of n. If all pairs of elements in P are incomparable, then the conclusion trivially holds. Otherwise, let m be the maximum size of an antichain in P. Let 0 be a miminal element and 1 be a maximal element of P such that $0 \leq 1$ and $0 \neq 1$. Consider the poset P' obtained by removing 0 and 1. If the maximum size of an antichain in P' is $m - 1$, then we can finish the proof by induction. Hence assume that there exists an antichain A in P' of size m.

Define $P^+ = \{x \in P : \exists a \in P', x \geq a\}$ and $P^- = \{x \in P : \exists a \in P', x \leq a\}$. Since A is a antichain, we have $P^+ \cap P^- = A$, and since it is maximal,

we have $P^+ \cup P^- = P$. Furthermore since 0 is a minimal element, we have $0 \notin P^+$, and this implies $0 \in P^-$. Similarly, $1 \in P^+$. Therefore P^+ and P^- both have size at most $n-1$ and by induction, we can find a partition of P^+ into m chains. Similarly, we can find a partition of P^- into m chains. We can combine these two families to find m chains covering all elements of P. □

Proof 2. We prove the statement by induction on the number of elements n of P. The statement trivially holds if $n = 0$.

Let P be a poset with n elements and suppose the theorem has been proven for all smaller values of n. Let a be a maximal element in P. By induction, there exists a chain decomposition $C_1 \cup \cdots \cup C_k$ of $P' = P \setminus \{a\}$ where a maximum antichain in P' has size k. Since an antichain can intersect C_i in at most one element, each maximum antichain of size k intersects C_i for all $i \in [k]$. For each $i \in [k]$, let x_i be the maximum element in C_i that intersects some maximum antichain of size k.

Claim. $X = \{x_1, \cdots, x_k\}$ is an antichain.

Suppose that the claim does not hold and $x_i < x_j$ for some distinct indices i, j. Take an antichain A of size k containing x_j, and let y_i be the element of this antichain in C_i. By the definition of x_i, we must have $y_i \leq x_i$. However by transitivity, this implies that $y_i < x_j$ contradicting the fact that A is an antichain.

If $X \cup \{a\}$ is an antichain, then we can add the chain $\{a\}$ to $\mathcal{C}$ to find the desired chain decomposition. Otherwise, suppose that $a > x_i$ for some i (recall that a is a maximal element). Consider the chain $C = \{a\} \cup \{y \in C_i : y \leq x_i\}$. By the definition of x_i, each antichain in P' of size k intersects C. Therefore the maximum size of an antichain in the poset $P \setminus C$ is at $k-1$. Hence we can find a chain decomposition of $P \setminus C$ of size $k-1$. This together with C gives a desired decomposition. □

Corollary 4. *Let n and m be natural numbers. If P is a poset with $nm+1$ elements, then it has a chain of size $n+1$ or an antichain of size $m+1$.*

Proof. Otherwise if each chain has size at most n and each antichain has size at most m, then Dilworth's theorem implies that $|P| \leq mn$. □

Dilworth's theorem has many interesting applications. For example, it straightforwardly implies the following theorem.

Theorem 5. *(Erdős-Szekeres 1935) Every sequence of $nm+1$ distinct integers contains an increasing subsequence of length at least $n+1$ or a decreasing subsequence of length at least $m+1$.*

Proof. Let $N = nm + 1$. Denote the given sequence as $a_1, a_2, \cdots, a_N$. Construct a poset with ground set $[N]$ where $i \preceq j$ if and only if $i \leq j$ and $a_i \leq a_j$. One can easily verify that $\preceq$ is a partial order.

Furthermore, a chain is an increasing subsequence and an antichain is a decreasing subsequence of the original sequence. Therefore the theorem follows from the above corollary of Dilworth's theorem. □

The dual to Dilworth's theorem is easier to prove.

Theorem 6. *Let P be a poset. Then there exists a chain C and a partition of P into a family $\mathcal{A}$ of antichains where $|\mathcal{A}| = |C|$.*

Proof. Let C be a chain of maximum size. For each $\ell = 1, 2, \cdots, |C|$, define L_ℓ to be the set of elements x of P for which there exists a chain of size ℓ whose maximum element is x but not for $\ell + 1$. We claim that each set L_ℓ is an antichain. Suppose that $x, y \in L_\ell$ are comparable, w.l.o.g., $x \leq y$. Consider the chain C_x of size size ℓ whose maximum element is x. Note that $y \notin C_x$ since $x \leq y$ and x is the maximum element in C_x. Therefore $C_x \cup \{y\}$ is a chain of size $\ell + 1$ whose maximum element is y. However this contradicts our definition of L_ℓ. Therefore L_ℓ is an antichain. □

2. Sperner's lemma

For a finite set X of size n, define 2^X as the power set of X. For a natural number $k \leq n$, define $\binom{X}{k}$ as the set of all k-subsets of X.

Theorem 7. *(Sperner 1928) Let X be a set of size n and $\mathcal{F} \subseteq 2^X$ be family of sets such that $F_1 \not\subseteq F_2$ for all distinct $F_1, F_2 \in \mathcal{F}$. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

Proof. Fix an integer $0 \leq k \leq n$. Consider a bipartite graph Γ_k with two parts $A_k = \binom{X}{k}$ and $B_k = \binom{X}{k-1}$ where $a \in A_k$ and $b \in B_k$ are adjacent if and only if $a \supseteq b$. Note that in Γ_k, each vertex in A_k has degree exactly k and each vertex in B_k has degree exactly $n - k + 1$. Hence for a fixed subset $Z \subseteq B_k$, note that

$$|Z| \cdot (n - k + 1) \leq e(Z, N(Z)) \leq |N(Z)| \cdot k.$$

If $k \leq \frac{n+1}{2}$, then it follows that $|N(Z)| \geq |Z|$. Hence Γ_k has a matching of size $|B_k| = \binom{X}{k-1}$ for all $k = 1, \cdots, \lfloor n/2 \rfloor$. A similar argument shows that for $k > \frac{n+1}{2}$, there exists a matching of size $\binom{X}{k}$ in Γ_k. Fix one such matching for each Γ_k.

Construct a poset with ground set 2^X where $F_1 \leq F_2$ if and only if $F_1 \subseteq F_2$. By using the matchings that we created above, we can find a chain decomposition $\mathcal{C}$ of 2^X where two sets $F_k \in \binom{X}{k}$ and $F_{k+1} \in \binom{X}{k+1}$ are in the same chain $C \in \mathcal{C}$ if and only if $\{F_k, F_{k+1}\}$ is an edge in the matching in Γ_k. Note that $|\mathcal{C}| \leq \binom{n}{\lfloor (n+1)/2 \rfloor} = \binom{n}{\lfloor n/2 \rfloor}$. This proves the theorem by Proposition 2. □

In 1938, Littlewood and Offord, in considering the distribution of zeros of random polynomials, raised the following question. Let $a_1, \cdots, a_n$ be given fixed real numbers of absolute value at least one. How many sums of the form $\sum_{i=1}^n \varepsilon_i a_i$ having $\varepsilon_i \in \{0, 1\}$ for all i can lie within an open unit

interval? They proved that the number is at most $\frac{c \log n}{\sqrt{n}} 2^n$ for some positive constant c. Erdős improved the bound using Sperner's lemma.

Theorem 8. *(Erdős 1945) Let $a_1, \cdots, a_n$ be given fixed real numbers of absolute value at least one. For all open unit intervals I, there are at most $\binom{n}{\lfloor n/2 \rfloor}$ vectors $(\varepsilon_1, \cdots, \varepsilon_n) \in \{0,1\}^n$ such that $\sum_{i=1}^n \varepsilon_i a_i \in I$.*

Proof. Define $\vec{a} = (a_1, \cdots, a_n)$. It suffices to prove the statement when all a_i are positive. To see this, suppose that a_1 is negative. Then

$$\varepsilon_1 a_1 + \varepsilon_2 a_2 + \cdots + \varepsilon_n a_n \in I$$

if and only if

$$(1 - \varepsilon_1) \cdot (-a_1) + \varepsilon_2 a_2 + \cdots + \varepsilon_n a_n \in -a_1 + I.$$

Thus we can switch the coordinates without affecting the conclusion.

For a set $X \subseteq [n]$ define $s(X) = \sum_{i \in X} a_i$. It suffices to count the number of sets X such that $s(X) \in I$. Suppose that X_1 and X_2 are two sets such that $X_1 \supseteq X_2$. Then

$$|s(X_1) - s(X_2)| = \sum_{i \in X_1 \setminus X_2} a_i \geq 1.$$

Since I is an open unit interval, only at most one of the values $s(X_1)$ and $s(X_2)$ can be in I. This shows that the family $\mathcal{F} = \{X : s(X) \in I\}$ is an antichain in the poset defined by inclusion. Therefore by Sperner's lemma, we have $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$. □

The tightness of this result can be seen by considering case $a_i = 1$ for all i and $I = \{\lfloor \frac{n}{2} \rfloor\}$. Note that asymptotically, Erdős's bound is $O(\frac{2^n}{\sqrt{n}})$.

Suppose that instead of finding values in an interval, we are interested in exact values. The same upper and lower bound transfers to this case. Furthermore in this case, it is known that one can significantly improve the bound if we assume that all the values a_i are distinct. More precisely, improving on results of Erdős and Moser, and Sárközy and Szemerédi, Stanley proved the following theorem.

Theorem 9. *(Stanley 1980) If $a_1, \cdots, a_n$ are distinct then for all x, there are at most $O(\frac{2^n}{n^{3/2}})$ vectors $(\varepsilon_1, \cdots, \varepsilon_n) \in \{0,1\}^n$ such that $\sum_{i \in [n]} \varepsilon_i a_i = x$. In fact when n is odd, then maximum is achieved when $\{a_1, \cdots, a_n\} = \{-\frac{n-1}{2}, \cdots, \frac{n-1}{2}\}$. (similar holds when n is even)*

Define $p(\vec{a}) := \max_{x \in \mathbb{R}} s(X)$. A *general arithmetic progression (GAP)* of rank k is a set of the form $\{c_0 + b_i d_i : \forall i \in [k], d_i \in [-D_i, D_i]\}$ for given $c_0, b_1, \cdots, b_k$ and $D_1, \cdots, D_k$. In general if $\{a_1, \cdots, a_n\}$ is a subset of a GAP, then $p(\vec{a})$ can be large. In 2009, Tao and Vu showed that the inverse to this statement is true.

Theorem 10. *(Tao-Vu 2009, inverse Littlewood-Offord theorem) For all positive constants A and α, there exists A' such that the following holds.*

Let μ be a positive constants at most one and assume that $\vec{a} = (a_1, \cdots, a_n)$ satisfies $p(\vec{a}) \geq n^{-A}$. Then there exists a GAP Q of rank at most A' and volume at most $n^{A'}$ which contains all but at most n^{α} elements in $\{a_1, \cdots, a_n\}$ (counting multiplicity).

Littlewood-Offord problem is closely related to the study of random ± 1 matrices. Consider a random $n \times n$ matrix $\mathbf{M}_n$ whose entries are ± 1 chosen independently and uniformly at random (this is known as the *random Bernoulli matrix*).

What is the probability that $\mathbf{M}_n$ is singular?

Clearly the matrix is singular if there are two identical rows. Therefore the singular probability is at least $2 \cdot \binom{n}{2} \cdot \frac{1}{2^n} \approx \frac{n^2}{2^n}$.

Conjecture 11. *The probability that $\mathbf{M}_n$ is singular is $(\frac{1}{2} + o(1))^n$.*

The relation between this problem and the Littlewood-Offord problem can be seen by considering the null space of the matrix. Note that a vector $\vec{v} = (v_1, \cdots, v_n)$ is in the null space of $\mathbf{M}_n$ if and only if $\vec{v} \cdot \vec{m}_i$ for each row vector $\vec{m}_i$ of $\mathbf{M}_n$. The inverse Littlewood-Offord problem tells us the structure of those vectors $\vec{v}$ which have high probability of being in the null space.

This conjecture is still open. The current best known result gives a $(\frac{1}{\sqrt{2}} + o(1))^n$ bound and was proved by Bourgain, Vu, and Wood.