# Lecture 2

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Arkaprava Choudhury and Andrew Feng

## Agenda

In the previous lecture, we defined what a matching in a graph means, and in particular, we focused on matchings in bipartite graphs. We saw how to find perfect matchings quickly, if they exist, by using augmenting paths, and also how to determine when no perfect matching exists. In (the first half of) this lecture, we will look at another way to find out when a bipartite graph permits a perfect matching.

We will also define chains and antichains in a partially ordered set and prove Dilworth's theorem in (the second half of) this lecture.

But first, a quick note that the grading scheme of this course will consist of the following: 50% of the grade will be from the homework sets, the final exam will constitute 35% of the final grade, and the remaining 15% will be from scribing lectures.

## 1 Monte-Carlo matchings in bipartite graphs

Let $G = (V, E)$ be a (finite) bipartite graph with $V = L \sqcup R$, where $|L| = |R| = n$. We would like to determine, given $G$, an expression for the total number of perfect matchings possible in $G$.

First, identify $L$ and $R$ with $[n] = \{1, \ldots, n\}$, and let $A \in \{0, 1\}^{n\times n}$ be a $n \times n$ matrix where, for every $x \in L$ and $y \in R$, we have $A_{xy} \in \{0, 1\}$ given by

$$A_{xy} = \begin{cases} 0, & \text{no edge between } x \text{ and } y \\ 1, & \text{otherwise} \end{cases}$$

Then, note that $G$ is a subgraph of the complete bipartite graph $K_{n,n}$. Thus, a perfect matching in $G$ is also a matching in $K_{n,n}$. By generalization, all perfect matchings in $G$ are perfect matchings in $K_{n,n}$, but not necessarily vice versa. This allows us to note that the number of perfect matchings in $G$ can be expressed as shown in the following equation, by using the characteristic variable $\mathbf{1}$ which is 1 if its condition is true and 0 otherwise, where the summation involves all $M$ which are perfect matchings of $K_{n,n}$.

$$\sum_M \mathbf{1}_{M\subseteq E}$$

Now, note that $\mathbf{1}_{M \subseteq E}$ evaluates to 1 if and only if for all $xy \in M$, we have $A_{xy} = 1$, i.e. if and only if $\prod_{xy \in M} A_{xy} = 1$, and otherwise evaluates to 0. Next, observe that the set of all perfect matchings $M$ of $K_{n,n}$ is isomorphic to the permutation group $S_n$. Indeed, when defining a matching $M$, to each vertex $x \in L \cong [n]$, we are simply assigning one unique neighbour $y = \pi_M(i) \in R \cong [n]$. Thus, we can simplify the above expression as follows

$$\sum_{M} \mathbf{1}_{M \subseteq E} = \sum_{M} \prod_{xy \in M} A_{xy} = \sum_{\pi \in S_n} \prod_{i \in [n]} A_{i,\pi(i)} = \operatorname{perm}(A). \qquad \text{(called the permanent of } A\text{)}$$

While computing the permanent of a matrix is known to be #$\mathsf{P}$-hard, we know how to compute the determinant efficiently. This makes the determinant a much easier concept to use in our expressions, and we try to make use of this fact.

**Theorem 1.** *For a $n \times n$ matrix $T$, its determinant is* $\det(T) = \sum_{\pi \in S_n} (-1)^{\operatorname{sgn}(\pi)} \prod_{i \in [n]} T_{i,\pi(i)}$.

**Fact 2.** *Using the triangle inequality, it is easy to see that if* $\det(A) \neq 0$, *then* $\operatorname{perm}(A) \neq 0$ *which would then imply the existence of some perfect matching for $G$.*

Indeed, to see this, note that

$$|\det(A)| = \left| \sum_{\pi \in S_n} (-1)^{\operatorname{sgn}(\pi)} \prod_{i \in [n]} A_{i,\pi(i)} \right| < \sum_{\pi \in S_n} \left| (-1)^{\operatorname{sgn}(\pi)} \prod_{i \in [n]} A_{i,\pi(i)} \right| = \sum_{\pi \in S_n} \prod_{i \in [n]} A_{i,\pi(i)} = \operatorname{perm}(A)$$

(all terms in $A$ positive)

Now, since we showed that the permanent of $A$ evaluates to the number of perfect matchings in $G$, then $0 < |\det(A)|$ would imply that there must exist at least $|\det(A)|$ many perfect matchings in $G$. In particular, there is at least one matching.

On the other hand, the converse need not be true. If $\det(A) = 0$, it could be the case that there were just as many perfect matchings arising from even permutations as those arising from odd permutations, and the test is inconclusive. This, however, is a very delicate scenario, so we aim to throw it off by randomly changing the matrix we use, by constructing an algorithm as follows. Here, let $N$ be some constant which we will set appropriately at the end. Note that, in the algorithm

**Algorithm 1**
INPUTS: Bipartite graph $G = (L \sqcup R, E)$ with $|L| = |R| = n$

1. Identify $L$ and $R$ with $[N]$. Create a $n \times n$ matrix $B \in [N]^{n \times n}$ as follows.

$$B_{ij} = \begin{cases} 0, & \text{no edge from } i \in L \text{ to } j \in R \\ \text{uniformly random element of } [N], & \text{otherwise.} \end{cases}$$

2. Compute $\det(B)$.

3. If $\det(B)$ is non-zero, then declare "$G$ has a perfect matching"; else, declare "$G$ *probably* has no perfect matching".

described above, the probability is not with respect to $G$, which is fixed, but it is instead with respect to the randomness of the algorithm. Now we look at how the algorithm responds to the two cases where $G$ either has or doesn't have a perfect matching, and if it responds correctly with good probability.

**Theorem 3.** *If $G$ has no perfect matching, then Algorithm 1 declares "G probably has no perfect matching" with probability 1.*

*Proof.* Suppose $G$ has no perfect matching. Then, for all $\pi \in S_n$, we will have $\prod_{i\in[n]} B_{i,\pi(i)} = 0$. Indeed, for any such $\pi$, there must be one term $B_{i,\pi(i)}$ which is zero, or else, we would have a perfect matching at hand. This readily implies

$$\det(B) = \sum_{\pi\in S_n} (-1)^{\mathrm{sgn}(\pi)} \prod_{i\in[n]} B_{i,\pi(i)} = \sum_{\pi\in S_n} 0 = 0$$

This proves the lemma. □

Before considering the other case, when $G$ has a perfect matching, first note the Schwartz-Zippel lemma given as follows.

**Lemma 4** (Schwartz-Zippel)**.** *Consider a non-zero polynomial $P(Z_1,\ldots,Z_m) \in \mathbb{R}[Z_1,\ldots,Z_m]$ of degree $d$ and some finite $S \subseteq \mathbb{R}$ with $|S| = b$. If $z_1,\ldots,z_m$ are independently chosen uniformly at random from $S$, then we have*

$$\Pr[P(z_1,\ldots,z_m) = 0] \le \frac{d}{b}.$$

*Proof.* We prove this by induction on the number of variables. For $m = 1$, note that a nonzero univariate polynomial of degree $d$ has at most $d$ zeroes.

Next, suppose that the lemma holds for all polynomials with at most $m-1$ variables. Then, consider $P$ as a polynomial in $Z_m$ given as follows, where $t \le d$,

$$P(Z_1,\ldots,Z_m) = \sum_{i=0}^{t} Z_m^t P_i(Z_1,\ldots,Z_{m-1}).$$

Since $P$ was nonzero, there must exist some nonzero $P_i$. Since there are only finitely many $P_i$s, define $t$ to be the largest $i$ such that $P_i$ is nonzero. It then follows that $\deg(P_i) \le d - i$, and in particular, $\deg(P_t) \le d - t$.

Choose $z_1,\ldots,z_{m-1}$ uniformly at random, independently, from $S$. Using the induction hypothesis, we have

$$\Pr_{z_1,\ldots,z_{m-1}}[P_i(z_1,\ldots,z_{m-1}) = 0] \le \frac{d-i}{b}.$$

Thus, if we consider the probability that $P(z_1,\ldots,z_{m-1},Z_m)$ is the zero polynomial in $\mathbb{R}[Z_m]$, we get

$$\begin{aligned}\Pr_{z_1,\ldots,z_{m-1}}[P(z_1,\ldots,z_{m-1},Z_m) \equiv 0] &= \prod_{i=1}^{t} \Pr_{z_1,\ldots,z_{m-1}}[P_i(z_1,\ldots,z_{m-1}) = 0] \\ &\le \Pr_{z_1,\ldots,z_{m-1}}[P_t(z_1,\ldots,z_{m-1}) = 0] \le \frac{d-t}{b}\end{aligned}$$

Now, if $P_t(z_1, \ldots, z_{m-1}) \neq 0$, then $P(z_1, \ldots, z_{m-1}, Z_m)$ was a nonzero univariate polynomial with degree at most $t$. So, by choosing $z_m$ uniformly at random from $S$, we get

$$\Pr_{z_m}[P(z_1, \ldots, z_{m-1}, z) = 0 | P_t(z_1, \ldots, z_{m-1}) = 0] \leq \frac{t}{b}$$

Thus, by combining the first probability expression and the above conditional probability, we get

$$\Pr_{z_1,\ldots,z_m}[P(z_1, \ldots, z_{m-1}, z) = 0] \leq \frac{d-t}{b} + \frac{t}{b} = \frac{d}{b}$$

This completes the induction. □

**Theorem 5.** *If $G$ has a perfect matching, then Algorithm 1 declares "$G$ has a perfect matching" with probability at least $1 - \frac{n}{N}$.*

Before proving this claim, note that $1 - \frac{n}{N} \to 1$ as $N$ grows larger.

*Proof.* Suppose $G$ has a perfect matching. Using the same indexing for $L$ and $R$ from Algorithm 1, consider the formal $n \times n$ variable matrix $C$ given by

$$C_{ij} = \begin{cases} 0, & \text{no edge from } i \in L \text{ to } j \in R \\ X_{ij}, & \text{otherwise.} \end{cases} \tag{1}$$

Then, $\det(C)$ is a polynomial of the form $\det(C) = P(X_{ij} : ij \in E)$. Let $|E| = m$; then, we can rewrite $\det(C) = P(Z_i : i \in [m])$ by identifying each $X_{ij}$ with some $Z_k$. We now have a formal polynomial in $m$ variables, i.e. $P(Z_1, \ldots, A_m) \in \mathbb{R}[Z_1, \ldots, Z_m]$. Note in particular that, by definition of $\det(C)$, we get $\deg(P) \leq n$, as in any of the products of the form $C_{i,\pi(i)}$, we can have at most $n$ random variables $X_{i,\pi(i)}$.

Since $G$ has a perfect matching, say $M$, there exists some $\pi \in S_n$ corresponding to the perfect matching such that $\prod_{i\in[n]} C_{i,\pi(i)} \neq 0$. Further note that this implies that $P$ is not the zero polynomial. Indeed, this is because for any distinct $\pi' \in S_n$, the monomial resulting from $\pi'$ is different from that of $\pi$, and thus, cannot cancel each other as formal polynomials.

We can then apply Lemma 4 to conclude that $\Pr_{z_1,\ldots,z_m}[P(z_1, \ldots, z_m) = 0] \leq \frac{n}{N}$. Hence, the probability that the determinant is nonzero is simply the complement of this value, and is thus, at least $1 - \frac{n}{N}$. □

By choosing $N$ sufficiently large (taking $N = 10n$ for example) we can get this success probability closer to 1. More importantly, with even something as small as $N > 2n$, we can get a success probability greater than $\frac{1}{2}$, which we can then use to repeat the algorithm sufficiently many times to amplify the success probability arbitrarily close to 1.

As a remark, it is useful to consider why we even constructed such an algorithm for the matching problem in bipartite graphs when we already had an algorithm from last week. For one, last week's algorithm was deterministic while Algorithm 1 is a randomized Monte Carlo algorithm which is not guaranteed to succeed. The reason for this is that Algorithm 1 has some useful applications to other problems. One such problem is the extension of the matching problem known as the $k$ blue-red matching problem, given as follows.

**Problem 1.**

Input: A bipartite graph $G = (L \sqcup R, E)$ with $|L| = |R| = n$ where every edge $e \in E$ is either coloured blue or red.

Output: Determine whether there exists a perfect matching of $G$ with exactly $k$ blue edges.

**Exercise 6.** *Use a similar algorithm to Algorithm 1 to solve Problem 1.*

## 2 Posets and Dilworth's Theorem

A *poset* (a partially ordered set) is a set $S$ with a relation $\leq$ satisfying

1. reflexivity: $\forall a : \quad a \leq a$
2. transitivity: $\forall a, b, c : \quad a \leq b \wedge b \leq c \rightarrow a \leq c$
3. anti-symmetry: $\forall a, b : \quad a \leq b \wedge b \leq a \rightarrow a = b.$

If $S$ also satisfies $\forall a, b : \quad a \leq b \vee b \leq a$, then it is *totally ordered.*

Some examples include $(\mathbb{R}, \leq)$, $(\mathcal{P}(X), \subseteq)$, and $(\mathbb{N} \setminus \{0\}, |)$.

A subset $C \subseteq S$ of a poset is called a *chain* if it is totally ordered. A subset $A \subseteq S$ is called an *antichain* if for any distinct elements $a, b \in A$, $a \not\leq b$ and $b \not\leq a$. In this case, $a$ and $b$ are said to be *incomparable.*

A simple fact is the following.

**Fact 7.** *Let $S$ be a poset. For any chain $C \subseteq S$ and antichain $A \subseteq S$, $|C \cap A| \leq 1$.*

This is because any two elements of $A$ must be incomparable whereas any two element of $C$ must be comparable.

This fact, together with the pigeonhole principle, gives the following observation.

**Observation 8** (Dilworth's Observation)**.** *If $S = C_1 \cup \ldots \cup C_t$, then, for any antichain $A \subseteq S$, $|A| \leq t$.*

*Proof.* If there exists some antichain $A$ with $|A| > t$, then by the pigeonhole principle, there exists some chain $C_i$ with $|C_i \cap A| > 1$, which would contradict Fact 7. □

This should look familiar to the max-flow min-cut theorem from last week! Both are instances of linear programming duality.

Given this observation, it makes sense to wonder if it is tight. It turns out that the minimum number of chains required to cover a poset is exactly the size of the largest antichain.

**Theorem 9** (Dilworth's Theorem)**.** *Let $S$ be a poset and $A \subseteq S$ be a maximal antichain. Then, there are chains $C_1, \ldots, C_{|A|}$ that union to $S$.*

*Proof.* We prove this by induction on $|S|$. This is clearly true for $|S| \leq 1$. Let $|S| > 1$.

Let $M$ be the size of the largest antichain in $S$. Let $C$ be a maximum chain in $S$ (i.e cannot add more elements to $C$ to keep it a chain). Note that $|C| > 0$.

If every antichain in $S \setminus C$ has size $\leq M - 1$, then the induction hypothesis says $P \setminus C$ is the union of $M - 1$ chains. Together with $C$, this gives $S$ as a union of $M$ chains.

Otherwise, there exists an antichain $A \subseteq S \setminus C$ of size $M$. Say $A = \{a_1, \ldots, a_M\}$. Define

$$S_{\leq} = \{s \in S : s \leq a_i \text{ for some } i\},$$

and

$$S_{\geq} = \{s \in S : s \geq a_i \text{ for some } i\}.$$

Before we can apply the induction hypothesis to $S_{\leq}$ and $S_{\geq}$, we need to check a few things. First, $S_{\leq} \cup S_{\geq} = S$: if not, we can extend $A$ to be a larger antichain, contradicting that the largest antichain in $S$ has size $M$. Also, $|S_{\leq}| < |S|$: the largest element in $C$ is not in $S_{\leq}$ because $C$ is maximal. Similarly, $|S_{\geq}| < |S|$. The intersection $S_{\leq} \cap S_{\geq}$ is just $A$: if $x \notin A$ and for some $a, a' \in A$, $a \leq x \leq a'$, then $a \leq a'$, which is impossible as $A$ is an antichain. Finally, $A$ is an antichain of largest cardinality in $S_{\leq}$ and $S_{\geq}$.

By induction, $S_{\leq} = C_1 \cup \ldots \cup C_M$ and $S_{\geq} = C'_1 \cup \ldots \cup C'_M$ where $C_i$ and $C'_i$ are chains. For each $a \in A$, there is exactly one $C_i$ such that $a \in C_i$. This is because $A \subseteq S_{\leq}$ and each $C_i$ can only cover one of $a \in A$. Same can be said about $C'_i$. Without loss of generality, assume $a_i \in C_i \cap C'_i$ for all $i$. Then, we can line up $C_i$ and $C'_i$ to obtain a chain $C''_i$. This shows $S$ is a union $C''_1 \cup \ldots \cup C''_M$ of $M$ chains. This completes the proof. □

In some sources, the chains in Dilworth's theorem are disjoint, but this is in fact equivalent: a poset can be written as a union of $k$ chains if and only if it is the union of $k$ disjoint chains. To see why, if a poset can be written as $C_1 \cup \ldots \cup C_k$, then for each $1 < i \leq k$, just remove the elements in $C_i$ that already appears in some $C_j$, $j < i$. This gives a decomposition into disjoint chains.

An application of Dilworth's theorem is the following.

Consider the poset $(\mathcal{P}([n]), \subseteq)$. The set of all subsets of size $\lfloor n/2 \rfloor$ is an antichain of size $\binom{n}{\lfloor n/2 \rfloor}$. We claim this is an antichain of maximal size.

**Exercise 10.** *Find $\binom{n}{\lfloor n/2 \rfloor}$ chains that union to $\mathcal{P}([n])$. Hint: begin building each chain from a subset of size $\binom{n}{\lfloor n/2 \rfloor}$.*

Alternatively, we have the following proof using the probabilistic method.

**Theorem 11.** *Let $\mathcal{A}$ be an antichain in $(\mathcal{P}([n]), \subseteq)$. Then, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

*Proof.* Let $\pi \in S_n$ be a permutation and let $E_{A,\pi}$ be the event that $\{\pi(1), \ldots, \pi(|A|)\} = A$ for each $A \in \mathcal{A}$. It is clear that for a uniformly random permutation $\pi$, the first $k$ elements $\{\pi(1), \ldots, \pi(k)\}$ is a uniformly random $k$-element subset of $[n]$. Thus, $\Pr_{\pi \in S_n \text{ uniform}}[E_{A,\pi}] = \begin{pmatrix} n \\ |A| \end{pmatrix}^{-1}$. Moreover, because $\mathcal{A}$ is an antichain, $E_{A,\pi}$ and $E_{A',\pi}$ are disjoint for any distinct $A, A' \in \mathcal{A}$.

Applying the union bound and the fact that probabilities are at most 1, we get

$$\sum_{A \in \mathcal{A}} \Pr_{\pi \in S_n} [E_{A,\pi}] \leq 1. \tag{2}$$

We know that $\binom{n}{\lfloor n/2 \rfloor} \geq \binom{n}{k}$ for any $k$, so

$$\sum_{A \in \mathcal{A}} \Pr_{\pi \in S_n} [E_{A,\pi}] \geq \frac{|\mathcal{A}|}{\binom{n}{\lfloor n/2 \rfloor}}.$$

So $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$. □

In the proof above, the inequality 2 is also known as the LYM inequality. More specifically,

**Theorem 12.** *Let $U$ be a set of size $n$ and $A \subseteq \mathcal{P}(U)$ an antichain. Let $A_k$ be the set of sets in $A$ of size $k$. Then,*

$$\sum_{k=0}^{n} \frac{|A_k|}{\binom{n}{k}} \leq 1.$$

**Exercise 13.** *Prove the above theorem.*

Finally, consider the following example of a poset in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of order $q$.

**Example 14.** *Define the poset of linear subspaces of $\mathbb{F}_q^n$ with a partial order given by the inclusion relation.*

As a related question, what is the number of linear subspaces in $\mathbb{F}_q^n$ of dimension $d$? To answer this, first consider the natural many-to-one map from the set of all $d$-dimensional subspaces with a basis to the set of all $d-$ dim subspaces.

The number of ways to pick a $d$-dimensional subspace with a basis is the same as the number of ways to pick $d$ linearly independent vectors, i.e. $\prod_{i \in [d]} (q^n - q^{i-1})$.

Next, the number of bases for any $d$-dimensional subspace is the same as the number of ways to pick $d$ linearly independent vectors in the $d$-dimensional space, i.e. $\prod_{i \in [d]} (q^d - q^{i-1})$.

Thus, the number of ways to pick a $d$-dimensional linear subspace in $\mathbb{F}_q^n$ is

$$\prod_{i \in [d]} \frac{q^n - q^{i-1}}{q^d - q^{i-1}}.$$