Combinatorics Notes

Instructor: Clinton Conley
Notes by: Lichen Zhang
Carnegie Mellon University
21-301 Combinatorics

Spring 2019

Contents

1 Graphs **3**
1.1 Basic definitions . . . 3
1.2 Walks, trails and paths . . . 5
1.3 Spanning trees . . . 6

2 Coloring **9**
2.1 Vertex and edge colorings . . . 9
2.2 Ramsey's theorem . . . 11

3 Extremal Graph Theory **15**

4 Matching Theory **19**
4.1 Hall's Theorem and Systems of Distinct Representatives . . . 19
4.2 Applications of Hall's matching . . . 22

5 Posets & Extremal Set Theory **24**

6 Flows & Networks **28**
6.1 Max-flow and Min-cut . . . 28
6.2 More flows and applications . . . 31

7 Principle of Inclusion & Exclusion **34**
7.1 Inclusion & Exclusion . . . 34
7.2 Description, Involution, Exception . . . 37

8 Elementary Counting & Stirling Numbers **40**

9 Generating Functions & Formal Power Series **43**
9.1 Generating functions: prelude . . . 43
9.2 Formal power series . . . 45
9.3 Finite calculus . . . 47
9.4 Solving recurrences using generating functions . . . 51

10 Partitions **57**
10.1 Fundamental questions & basic definitions 57
10.2 The partition function & Euler's formulae 61

11 Coding Theory **66**
11.1 Hadamard matrices 66
11.2 Codes and some bounds 72

12 Lattice Theory **76**
12.1 Basic definitions & examples 76
12.2 Zeta function & Möbius function 78
12.3 Applications of zeta and Möbius functions 84
12.4 Advanced countings with lattices 87

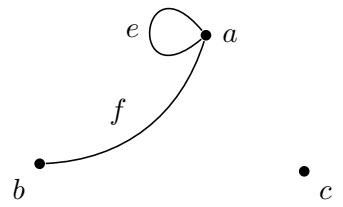
13 Advanced Topics on Graphs **94**

1 Graphs

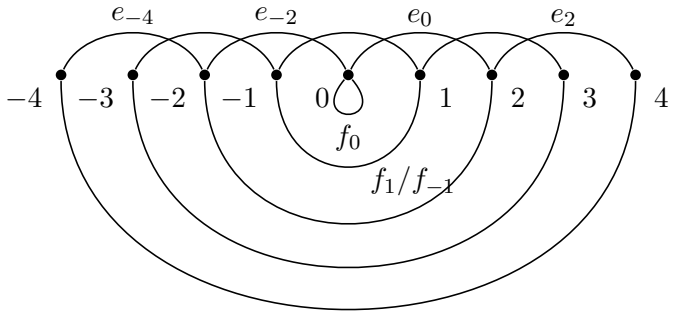
1.1 Basic definitions

Definition 1.1. A *graph* G is a pair of 2 sets: (V, E), where V is the set of vertices, and E is the set of edges, each $e \in E$ is associated with one or two vertices in V. In such case, we say v is *incident to* e.

Example 1.2. $V = \{a, b, c\}, E = \{e, f\}, e \mapsto \{a\} = \text{“}\{a, a\}\text{”}, f \mapsto \{a, b\}$



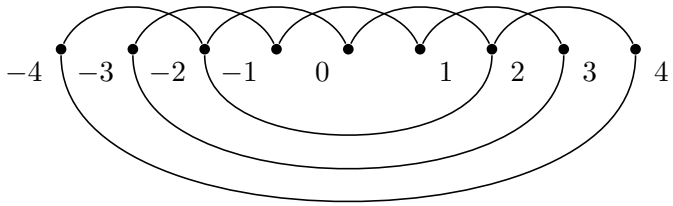
Example 1.3. $V = \mathbb{Z}, E = \{e_z, f_z : z \in \mathbb{Z}\}, e_z \mapsto \{z, z+2\}, f_z \mapsto \{z, -z\}$



Notice edges are distinct, even though vertices they are incident to are the same. We should think of f_3/f_{-3} as distinct edges.

Definition 1.4. A *simple graph* is a graph with *no self-loop* and *no multi-edges*.

Example 1.5. A simplified version of the graph we encounter in Example 1.3.



Definition 1.6. The *number of times* a vertex appears as an endpoint of an edge is its *degree*, often denoted as $\deg(v), v \in V$ or $\deg_G(v)$.

In the graph of Example 1.3, every vertex has degree 4, not always the same as number of edges a vertex is incident to: 0 is incident to only 3 edges, e_0, e_{-2}, f_0, but the loop f_0 counts twice.

In the graph of Example 1.5, $\deg(z) = \begin{cases} 2, & z \in \{-1, 0, 1\} \\ 3, & \text{else} \end{cases}$.

Definition 1.7. A graph $G = (V, E)$ is *finite* if both V and E are finite.

Theorem 1.8 (Handshake)**.** *If G is finite, then $\sum_{v \in V} \deg(v) = 2|E|$.*

Proof. Idea: both LHS and RHS count the same object: number of pairs (v, e), where v is an endpoint of e, with multiplicity.

Each v is in $\deg(v)$-many such pairs by Definition 1.6, so total is $\sum_{v \in V} \deg(v)$, which is the LHS.

On the other hand, e is in exactly 2 such pairs, total is $2|E| = \sum_{e \in E} 2$, which is RHS. □

Corollary 1.9. *There's no finite graph with an odd number of vertices of odd degree.*

Notice the corollary does not hold for infinite graphs.

Definition 1.10. Suppose we have two graphs $G = (V_G, E_G), H = (V_H, E_H)$, an *isomorphism* from G to H is a pair of bijections: $\varphi : V_G \to V_H, \psi : E_G \to E_H$, such that for all $v \in V_G, e \in E_G$, e is G-incident with v if and only if $\psi(e)$ is H-incident to $\varphi(v)$.

Definition 1.11. An *automorphism* of a graph is an isomorphism from the graph to itself.

Notice automorphisms form a group.

Sometimes it's not so easy to intuitively understand the isomorphisms and automorphisms on graphs. For automorphisms, a useful way to reason about it is to first locate the vertices we want to map to, then move the edges that are incident to it with it. Then, we can further move vertices that are incident with that edge, and so on and so forth. This offers a procedure-like way to reason about the structure of an automorphism.

1.2 Walks, trails and paths

Definition 1.12. Given a graph $G = (V, E)$, a $(G-)$ *walk* is a (finite) sequence

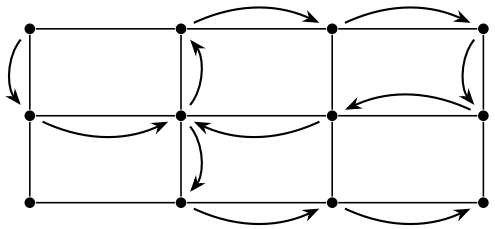
$$v_1 e_1 v_2 e_2 \dots v_k e_k v_{k+1},$$

with:

- each $v_i \in V$
- each $e_i \in E$
- each pair $v_i e_i, e_i v_{i+1}$ is incident, i.e., the endpoints of e_i are exactly v_i, v_{i+1}

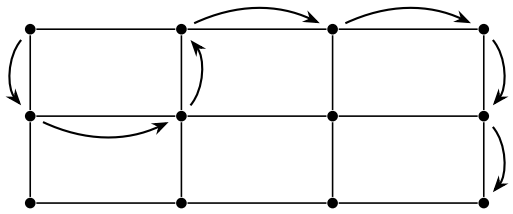
Definition 1.13. A *trail* is a walk in which no edge occurs twice.

Example 1.14. A trail.



Definition 1.15. A *path* is a trail in which no vertex occurs twice.

Example 1.16. A path.



Definition 1.17. Two vertices v, w are *connected* if there's a walk (path) from v to w.
Notice that

- Connectivity is an equivalence relation on V;
- Equivalence classes are called connected components of G;
- G is connected if it has exactly one connected component.

Definition 1.18. A walk/trail/path is *closed* if the start and end vertices coincide. Notice under this definition, a closed path has no edges, since otherwise its start vertex would occur twice.

Definition 1.19. A *cycle* is a closed trail with at least one edge, in which no vertex occurs twice, except for its start and end point.

Definition 1.20. A graph is called *Eulerian* if there is a closed walk (trail) using each edge exactly once.

Theorem 1.21 (Euler)**.** *Suppose G is a connected finite graph, then G is Eulerian if and only if every vertex has even degree.*

The proof relies on a lemma. We state it below.

Lemma 1.22. *If H is a finite graph with all degrees even and e is any edge of H, then there is a closed H-trail containing e.*

Proof of Lemma. Let u, v be two endpoints of e. Consider the following algorithm:

```
Let w = u;
Let L be a data structure, store e into L;
while w != v:
     find an edge with one endpoint w, call it f, and another
     endpoint z;
     if f not in L:
          add f to L;
          w = z;
output L;
```

We claim L found by above algorithm is the desired closed trail we want. This is obvious from the algorithm. Moreover, we will show the algorithm will indeed halt. Intuitively, it will halt since each vertex has even degree, so we can always find another edge to "get out".

The formal proof is by contradiction. Suppose otherwise, we get stuck in some intermediate round, which means that on a certain vertex, all of its edges have been used. Notice each time the algorithm sets w to a new vertex, it needs to "consume" two edges: one edge has its endpoints on old w and the new vertex, and the other edge is used as w "goes out" of the vertex. If it is the case of our assumption, then that vertex must have odd degree, since each time w visits it, it uses two edges, and the last time we set w to it, we only use one edge. This is a contradiction, since all vertices have even degree. Thus, the algorithm indeed halts, even within $|E|$ steps. □

With the lemma in hand, we are ready to prove Theorem 1.21.

Proof of Euler's Theorem. We prove two directions of the theorem.

($\Rightarrow$): If G has an Eulerian walk, then the degree of any vertex v is 2 times the number of occurrences of v in the walk, which is even.

($\Leftarrow$): Consider any closed trail t using a maximal number of edges, we will show that it witnesses Eulerian. Assume for a contradiction, there is some G-edge not in t. By connectivity of G, we may find an edge e not in t incident to a vertex x in t, let H be the graph obtained by deleting t-edges from G. Note that every vertex still has even H-degree, and also, e is an H-edge.

By Lemma 1.22, there is a closed H-trail, s, containing e. By concatenating t and s at x, which s passes through since it contains e, we obtain a larger G-trail, contradicting that t uses maximal number of edges. □

1.3 Spanning trees

Definition 1.23. A *tree* is a connected graph without cycles.

Remark 1.24. Trees must be simple graphs.

Theorem 1.25 (Cayley)**.** *Let $n \in \mathbb{N}$ and $n \geq 2$, there are exactly n^{n-2} distinct trees on the vertex set $[n]$.*

Above theorem can be interpreted in a logical way: there are n^{n-2} distinct binary relations on $[n]$ which are adjacency relations of trees.

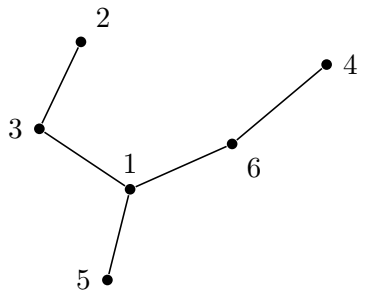
Proof. The idea is to encode trees by $n-2$ length sequences from $[n]$.

Note: Any tree with $n \geq 2$ vertices has at least 2 vertices of degree 1, which we call *leaves*.

Given a tree T on $[n]$, let $x_1 :=$ leaf with smallest label, $y_1 :=$ the unique vertex adjacent to x_1. Then, "prune", i.e., delete x_1 and the edge (x_1, y_1) from T, then recurse on the remaining tree, all the way down to y_{n-1}. By doing so, we get two vectors:

$$\vec{x} = x_1, x_2, \ldots, x_{n-1}, \vec{y} = \underbrace{y_1, y_2, \ldots, y_{n-2}}_{\textit{Prüfer code}}, y_{n-1}$$

The following is an example tree:



Corresponding $\vec{x}$ and $\vec{y}$ for it:

$$\vec{x} = 2, 3, 4, 5, 1, \vec{y} = \underbrace{3, 1, 6, 1}_{\textit{Prüfer code}}, 6$$

The reason we don't need y_{n-1} is, it is always the largest vertex in T, thus it won't provide any new information. This is because there are always at least 2 leaves, so the leaf with the smallest label is never n, hence n is never pruned and is the vertex left at the end.

Our goal now is to show that each of the n^{n-2} possible Prüfer codes corresponds to a unique tree on $[n]$. To do so, we prove a subclaim.

Proposition 1.26. *For each tree T on $[n]$ and vertex $v \in [n]$,*

$$\deg_T(v) = \textit{number of occurrences of } v \textit{ in } \operatorname{code}(T) + 1.$$

Proof of Subclaim. Consider two cases:

Case 1 $v < n$, then v will appear in $\vec{x}$ exactly once, when it is pruned, all other occurrences are all in Prüfer code, since when v appears in $\vec{x}$, it is a leaf with degree 1, and each time it appears in Prüfer code, we prune an edge that is incident to v, its degree goes down by 1.

Case 2 $v = n$, then the $+1$ part appears in y_{n-1}.

□

We next argue that from any sequence $y_1, \ldots, y_{n-2}$, we can recover $\vec{x}, \vec{y}$, and thus the tree. For $\vec{y}$, we just put n as y_{n-1} so it is completed. In order to recover $\vec{x}$, we do it coordinate-wise. To recover x_1, we scan vertices not appearing in Prüfer code, the least one must be x_1. Then we recurse on $y_2, \ldots, y_{n-2}$. This recovery algorithm is correct, since in round i, the remaining tree has code $y_i, \ldots, y_{n-2}$, so by the proposition, its leaves are exactly its vertices not in $y_i, \ldots, y_{n-2}$. The other vertices have already been put back to $\vec{x}$. So the vertices present in neither part are exactly the leaves of the remaining tree, and the least one is exactly what we've pruned in that round. Thus, the algorithm is correct.

It remains to show that every sequence $y_1, \ldots, y_{n-2}$ comes from some tree. Run the same procedure on it: in round i, at least $n-(i-1)-(n-1-i) = 2$ vertices are present in neither part, so we get distinct $x_1, \ldots, x_{n-1}$, all different from n. Put $y_{n-1} = n$. Since y_i is excluded in rounds $1, \ldots, i$, each y_i is n or some x_j with $j > i$. So following the edges $x_i y_i$ from any vertex leads to n. There is no cycle either, since the vertex x_i on it with the smallest i would need two edges to later vertices, but it only has $x_i y_i$. Thus these $n-1$ edges form a tree, and by the same reasoning as above, pruning it gives back $y_1, \ldots, y_{n-2}$. □

With Prüfer code, we can do some fancy countings on labeled trees.

Example 1.27. Q: How many trees on [100] have $\deg(5) = 40$?
A: We count corresponding Prüfer code. $\deg(5) = 40$ means in Prüfer code, 5 appears 39 times. The length of the code is 98, so we first choose 39 positions for 5, which yields $\binom{98}{39}$. Then in the remaining 59 positions, we can choose any of the remaining 99 vertices, which yields 99^{59}. Thus, the total number is $\binom{98}{39}99^{59}$.

Definition 1.28. Suppose G is a connected graph on V, a *spanning tree* for G is a tree on V whose edges are also G-edges.

In finite situation, typical algorithms for generating spanning trees are also heavily used in *graph reachability problem*, such as *BFS* and *DFS*.

Definition 1.29. K_n is the *complete graph* on n vertices.

We may reinterpret Theorem 1.25 as follows:

Theorem 1.30 (Cayley, reinterpreted)**.** *K_n has n^{n-2} spanning trees.*

There are many interesting relationships between graphs and linear algebra. For example, there is a theorem that states that for any finite connected simple graph G, number of spanning trees of G = determinant of $D - A$ with its i-th row and i-th column deleted (for any i), where A is the adjacency matrix of G and D is the diagonal matrix of degrees.

Other "spanning graphs":

Definition 1.31. A *Hamiltonian path* is a path using each vertex exactly once.

Definition 1.32. A *Hamiltonian cycle* is a cycle, except for its start and end point, that uses each vertex exactly once.

2 Coloring

2.1 Vertex and edge colorings

Definition 2.1. Given a simple graph $G = (V, E)$, a (proper) *vertex k-coloring* is a function $C : V \to k$, such that $\underbrace{\{v_1, v_2\} \in E \Rightarrow C(v_1) \neq C(v_2)}_{\text{properness}}$.

Trivially, one can show that if G is a simple graph on n vertices, it has a proper vertex n-coloring.

Definition 2.2. $\chi(G) :=$ least k such that G has a proper vertex k-coloring.

Theorem 2.3 (Wimpy, Brooks)**.** *If G is a finite simple graph with $\forall u \in V, \deg(u) \leq d$, then $\chi(G) \leq d + 1$.*

Proof. List vertices $v_1, \ldots, v_n$, first color v_1 arbitrarily; at stage k, color v_k such that $\forall i < k$, if $\{v_i, v_k\} \in E$, then $C(v_k) \neq C(v_i)$. This is achievable, since $\deg(v_k) \leq d$, so in worst case all its neighbors have consumed all d colors, but we have $d+1$ colors in total, so there is always one color that is available to color v_k. □

Example 2.4. K_{d+1} has $\deg(u) \leq d$, but requires $d + 1$-many colors. Remarkably, for $d \geq 3$, it is basically the **only** such example.

Theorem 2.5 (Brooks)**.** *Suppose $d \geq 3$ and G is a finite, simple connected graph, with $\forall v \in V, \deg(v) \leq d$. If G is not isomorphic to K_{d+1}, then $\chi(G) \leq d$.*

Proof. Assume for a contradiction that there exists a counterexample.

The proof will be by induction, we first fix a counterexample H, which is critical, in the sense that, deleting any vertex does not lead to a counterexample. Let $n = |V|$. We will require a lemma, the proof of the lemma is left as an exercise to the reader.

Lemma 2.6. *$\forall X \subseteq V$ with $X \neq \emptyset$ and $|X| \leq n - 3$, there are at least 3 distinct elements of $V \setminus X$ adjacent to some vertices in X.*

We have a list of claims, which we will prove one by one.

Proposition 2.7. *There exists a list $x_1, \ldots, x_n$ of V, such that:*

- $\deg(x_1) = d$
- *x_1 is adjacent to x_{n-1}, x_n*
- *x_{n-1}, x_n not adjacent*
- *For all $j > 1$, $\exists i < j$ such that x_i, x_j adjacent*

Proof of Subclaim. By Theorem 2.3, there exists a vertex of degree at least d, since otherwise, $\chi(H) \leq d$ is trivial. Let's call it x_1, so $\deg(x_1) = d$. If all neighbors of x_1 are adjacent to each other, then H is isomorphic to K_{d+1}, since these $d + 1$ vertices already have degree d each, so by connectivity there are no other vertices, so it's not possible. Pick x_{n-1}, x_n adjacent to x_1 but not to each other. To find x_2, consider $X = \{x_1\}$, by Lemma 2.6, it has at least 3 neighbors and at least one of them is **not** in $\{x_{n-1}, x_n\}$, pick one, call it x_2. Notice this gives us an algorithm: to find x_k for $k \leq n - 2$, consider $X = \{x_1, \ldots, x_{k-1}\}$, and find one of its neighbors outside X not in $\{x_{n-1}, x_n\}$, add it as x_k. □

We will then produce a d-coloring. We work from right to left in the list of $x_1, \ldots, x_{n-1}, x_n$:

- Color x_n and x_{n-1} the **same** color;
- Color x_k. x_k has at least one neighbor to the left that is not yet colored, so at most $d-1$ of its neighbors have already been colored, we pick any available color to color x_k;
- Color x_1. All d of x_1's neighbors are colored, but at least x_{n-1} and x_n get the **same** color, so we can use any available color. □

Definition 2.8. An *edge k-coloring* is a function $C : E \to k$.

Definition 2.9. A *monochromatic triangle* of a graph under certain edge coloring, C, is a K_3 that has all its edges colored the same color.

As a warm up, consider the following proposition:

Proposition 2.10. *If edges of K_6 are colored R/B, then there exists at least one monochromatic triangle.*

Proof. Fix a vertex v. In K_6, $\deg(v) = 5$, so in any edge coloring, at least 3 of edges incident to v are colored either all red or all blue. Without loss of generality, assume 3 of them are colored red. Then within its 3 neighbors, if any one edge is colored red, we obtain a red monochromatic triangle. Otherwise, all edges in the K_3 are colored blue, which indeed forms a blue monochromatic triangle. □

Theorem 2.11 (Goodman)**.** *Suppose edges of K_n are colored R/B, further, v_i has r_i-many red edges and $b_i = n-1-r_i$-many blue edges, then there are exactly $\binom{n}{3} - \frac{1}{2}\sum_{i\leq n} r_i(n-1-r_i)$-many monochromatic triangles.*

Proof. We prove by counting non-monochromatic triangles.

Notice in K_n, there are $\binom{n}{3}$ triangles in total, so it suffices to show there are exactly $\frac{1}{2}\sum_{i\leq n} r_i(n-1-r_i)$ non-monochromatic triangles.

Since each triangle consists of 3 edges, in a non-monochromatic triangle, 2 of them will be red or blue, and the other will have a different color. So we can view a triangle as being "spanned" by two edges, one red, one blue, and these 2 edges are incident to a single vertex. For each vertex v_i, there are $r_i(n-1-r_i)$ ways to choose these two edges. Notice that for each non-monochromatic triangle, there are two such vertices, therefore, the sum of all vertices double counts the number of non-monochromatic triangles. □

2.2 Ramsey's theorem

There are many other monochromatic graphs, some of them are even hypergraphs. One important observation is, if we want to find a monochromatic copy of some simple graph on p vertices, it suffices to find such monochromatic K_p.

Theorem 2.12 (Ramsey)**.** *Suppose $p, q \in \mathbb{N}^+$, then there is some $n \in \mathbb{N}^+$ such that for any R/B coloring of edges of K_n, either*

- *it contains a red copy of K_p;*
- *it contains a blue copy of K_q.*

Definition 2.13. Given p, q, the least such n is denoted by $R(p, q)$, or $N(p, q; 2)$.

Remark 2.14. As we have shown in Proposition 2.10, $R(3, 3) \leq 6$. In fact $R(3, 3) = 6$: in K_5, color a 5-cycle red, then the remaining 5 edges form another 5-cycle, color them blue. Since a 5-cycle has no triangle, there is no monochromatic triangle.

Proof. By induction on $p + q$.

Base case: $p = 1$ or $q = 1$. Then $n = 1$ works, since a single vertex is a red K_1 and also a blue K_1, vacuously. So $R(1, q) = R(p, 1) = 1$. Similarly, $R(2, 2) = 2$: K_1 has no edge, while the only edge of K_2 is colored either red or blue.

Inductive step: let $p, q \geq 2$, we know $R(p - 1, q)$ and $R(p, q - 1)$ exist, we need to show $R(p, q)$ exists. Choose $n = R(p - 1, q) + R(p, q - 1)$.

Fix some R/B coloring of K_n, fix any vertex of K_n, call it x_0, then at least one of the following holds, since otherwise x_0 has at most $(R(p - 1, q) - 1) + (R(p, q - 1) - 1) = n - 2$ edges:

Case 1 x_0 is incident with at least $R(p - 1, q)$ red edges;

Case 2 x_0 is incident with at least $R(p, q - 1)$ blue edges.

Without loss of generality, let's assume it is case 1, we zoom into $R(p - 1, q)$ of the vertices x_0 is adjacent to by red edges. By induction hypothesis, they contain either a red K_{p-1} or a blue K_q, if it is the latter case, then we are done. Otherwise, notice all edges between x_0 and them are red, so we have a red K_p as well. □

To dive further into Ramsey's theorem, we first introduce some set-theoretic notations.

Definition 2.15. Given a set X, let $[X]^r$ denote the family of subsets of X with exactly r-many elements.

So $[X]^2$ looks like a complete graph on X, analogously, $[X]^r$ is sometimes called the *complete r-uniform hypergraph* on X.

Theorem 2.16 (hyper Ramsey)**.** *Suppose $r, p, q \geq 1$, then there is some $n \in \mathbb{Z}$ such that whenever X is a set with $|X| = n$ and $C : [X]^r \to R/B$ is any coloring, either*

- *$\exists Y \subseteq X$, with $|Y| = p$ and $[Y]^r$ all red;*
- *$\exists Z \subseteq X$, with $|Z| = q$ and $[Z]^r$ all blue.*

Definition 2.17. The least such n is denoted by $N(p, q; r)$.

Proof. Two layers of induction. We prove:

1. $\forall p, q$, $N(p, q; r)$ exists by induction on r.

   Base case: $r = 1$ is trivial by pigeonhole: if $|X| = p + q - 1$, then at least p singletons are red or at least q are blue; $r = 2$ is Theorem 2.12.

   Inductive step: we assume $\forall p, q$, $N(p, q; r)$ exists. We wish to show $N(p, q; r + 1)$ exists, this will be done by induction on $p + q$.

2. Suppose X is some huge finite set and we have some coloring: $C : [X]^{r+1} \to R/B$.

   Fix any $x_0 \in X$ and put $X' = X \setminus \{x_0\}$, we induce a coloring $D : [X']^r \to R/B$, by $D(A) = C(A \cup \{x_0\})$. We can thin down to big $Y' \subseteq X'$ all D-red or $Z' \subseteq X'$ all D-blue. Thin Y' down to Y'' that has $p - 1$ red or q blue. We want $|Y'|$ to be at least $N(p - 1, q; r + 1)$ or $|Z'|$ to be at least $N(p, q - 1; r + 1)$, and this requires $|X'|$ to be at least $N(N(p - 1, q; r + 1), N(p, q - 1; r + 1); r)$, therefore the parameter n that will satisfy this is $n = N(N(p - 1, q; r + 1), N(p, q - 1; r + 1); r) + 1$. The proof can be then completed analogously as Theorem 2.12. The base case of this inner induction is $p = 1$ or $q = 1$, where $n = 1$ works, since a one-element set Y has $[Y]^{r+1} = \emptyset$, which is all red and all blue. □

The above proof uses two layers of induction, hence is quite confusing. The most important takeaway is the method used in Theorem 2.12. One way to think about it is to consider what n will satisfy the requirement so that we can do a similar argument as Theorem 2.12, and this is what we have done in the proof above.

The proof in Theorem 2.12 shows that

$$R(p, q) \leq R(p - 1, q) + R(p, q - 1) \tag{1}$$

We can derive a tighter bound due to such a recurrence.

Corollary 2.18. $R(p, q) \leq \binom{p+q-2}{p-1}$

Proof. By induction on $p + q$ using (1). Base case: $R(1, q) = 1 = \binom{q-1}{0}$ and $R(p, 1) = 1 = \binom{p-1}{p-1}$.

Notice we can write $R(p, q)$ as

$$\begin{aligned} R(p, q) &\leq R(p - 1, q) + R(p, q - 1) \\ &\leq \binom{p + q - 3}{p - 2} + \binom{p + q - 3}{p - 1} && \text{inductive hypothesis} \\ &= \binom{p + q - 2}{p - 1} \end{aligned}$$

While the last equality is due to the property of binomial coefficient:

$$\binom{n}{k} = \binom{n - 1}{k} + \binom{n - 1}{k - 1}$$

A combinatorial interpretation for this equality: you want to choose a k-element subset of $[n]$. There are two kinds of subsets you can choose:

- Either include n, in this case, you choose $k-1$ elements from remaining $[n-1]$, which yields $\binom{n-1}{k-1}$;
- Not include n, in this case, you choose k elements from $[n-1]$, which yields $\binom{n-1}{k}$. □

Corollary 2.19. $R(p,p) \leq 4^{p-1}$

Proof.

$$\begin{aligned} R(p,p) &\leq \binom{p+p-2}{p-1} \\ &= \binom{2(p-1)}{p-1} \\ &\leq 2^{2(p-1)} \\ &= 4^{p-1} \end{aligned}$$

□

Theorem 2.20. *For $p \geq 2$, $R(p,p) \geq 2^{p/2} = (\sqrt{2})^p$.*

Proof. The proof uses a famous and important proof technique in combinatorics, called *probabilistic method*.

Suppose $n < 2^{p/2}$, we need to show that there exists some coloring of K_n into R/B with no monochromatic K_p. To do so, we do some countings.

- Total edge colorings: for each edge, we have two choices, and for K_n, we have $\binom{n}{2}$ edges, so the total is $2^{\binom{n}{2}}$.
- Monochromatic colorings (overestimate): to color a monochromatic K_p, we first choose p vertices, within this K_p, we have two ways to color it, which yields $2\binom{n}{p}$. For the remaining edges, we can color them arbitrarily, which yields $2^{\binom{n}{2}-\binom{p}{2}}$, so the total is $2\binom{n}{p}2^{\binom{n}{2}-\binom{p}{2}}$. Notice this number overestimates the total monochromatic colorings, since in remaining edges, it can also form a monochromatic K_p.

Goal: $2\binom{n}{p}2^{\binom{n}{2}-\binom{p}{2}} < 2^{\binom{n}{2}}$. Manipulate a bit, we have: $\binom{n}{p} < 2^{\binom{p}{2}-1} = 2^{\frac{p^2-p}{2}-1}$. To show it, we prove a subclaim.

Proposition 2.21. *For $n < 2^{p/2}$, $\binom{n}{p} < 2^{p^2/2-p+1}$.*

Proof of Subclaim.

$$\begin{aligned} \binom{n}{p} &= \frac{n!}{p!(n-p)!} \\ &\leq \frac{n^p}{2^{p-1}} \\ &< \frac{(2^{p/2})^p}{2^{p-1}} \\ &= 2^{p^2/2-p+1} \end{aligned}$$

□

Notice $\frac{p^2-p}{2} - 1 \geq \frac{p^2}{2} - p + 1$ as long as $p \geq 4$, since the difference is $\frac{p}{2} - 2$. Thus, by Proposition 2.21, we have proved the goal for $p \geq 4$. For $p = 2, 3$ the bound holds directly: $R(2,2) = 2 = 2^{2/2}$, and $R(3,3) = 6 > 2^{3/2}$. □

To summarize our above results, we have that, for each $p \geq 3$,

$$(\sqrt{2})^p \leq R(p,p) \leq 4^p$$

For all theorems and corollaries below, the proof will either be omitted or be a sketch.

Theorem 2.22 (infinite Ramsey)**.** *Suppose $C : [\mathbb{N}]^r \to R/B$, then either*

- *$\exists$ infinite $Y \subseteq \mathbb{N}$ such that $[Y]^r$ all red; or*
- *$\exists$ infinite $Z \subseteq \mathbb{N}$ such that $[Z]^r$ all blue.*

Corollary 2.23 (Ramsey)**.** *Suppose α is an arbitrary binary relation on $\mathbb{N}$, then there is an infinite subset of $\mathbb{N}$ on which α coincides with one of*

$$\emptyset, <, >, \neq, =, \leq, \geq, \mathbb{N}^2$$

Theorem 2.24 (Happy Ending)**.** *$\forall p \geq 1$, there is some $N \in \mathbb{N}$ such that whenever you have N points in the plane with no 3 of them collinear, then some p of them form a convex p-gon.*

Proof Sketch. Choose $N = N(p, p; 3)$, suppose we have $X = \{x_0, \ldots, x_{N-1}\} \subseteq \mathbb{R}^2$, define a coloring $C : [X]^3 \to R/B$. Suppose we have $\{x_a, x_b, x_c\}$ with $a < b < c$, then color them red if they form a clockwise cycle, blue if they form a counterclockwise cycle. By the choice of N, some p of the points have all their triples colored the same, and it's not hard to see that none of these p points lies inside a triangle formed by three others, so they form a convex p-gon. □

3 Extremal Graph Theory

Theorem 3.1 (Turán)**.** *Let $n, p \in \mathbb{N}$ with $p \geq 2$, if G is a simple graph on n vertices with more than $M(n,p) = \frac{p-2}{2(p-1)}n^2 - \frac{r(p-1-r)}{2(p-1)}$ edges, where $n = t(p-1)+r$, with $1 \leq r \leq p-1$, then G has K_p as a subgraph.*

Note: $M(n,p)$ is the number of edges in the complete balanced $(p-1)$-partite graph on n vertices.

Further notice that $t(p-1) < n \leq (t+1)(p-1)$, so in order to prove the theorem, we do induction on t.

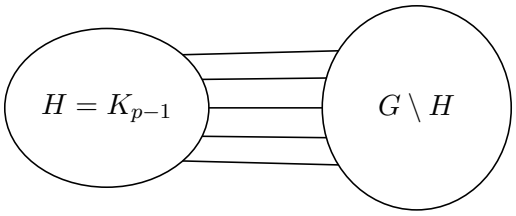
Proof. By induction on t.

Base case: for $t = 0$, we have $0 < n \leq p-1$, so $r = n$, in this case,

$$\begin{aligned} M(n,p) &= \frac{p-2}{2(p-1)}r^2 - \frac{p-1-r}{2(p-1)}r \\ &= \frac{pr^2 - 2r^2 - pr + r + r^2}{2(p-1)} \\ &= \frac{(p-1)r^2 - (p-1)r}{2(p-1)} \\ &= \frac{r^2 - r}{2} \\ &= \binom{r}{2} \\ &= \binom{n}{2} \end{aligned}$$

Hence, $M(n,p)$ edges give us a complete graph. Since $n \leq p-1$, G cannot contain a K_p as a subgraph, and indeed, the maximum number of edges of G is at most $M(n,p)$, since it is the number of edges on a complete graph.

Inductive step: assume that for some $t \in \mathbb{N}^+$, the proposition holds for all n with $(t-1)(p-1) < n \leq t(p-1)$. Consider G on n vertices, where $t(p-1) < n \leq (t+1)(p-1)$, without K_p and having as many edges as possible. Then G must contain a K_{p-1}, say H. To see this, notice G is not complete since $n \geq p$, so by maximality, adding any missing edge uv to G creates a K_p. Deleting v from that K_p leaves a K_{p-1} in G.



We have three kinds of edges.

- Edges within $G \setminus H$. In this part, notice there are $n-p+1$ vertices, which lies in the interval between $(t-1)(p-1)$ and $t(p-1)$, so by inductive hypothesis, there are at most $M(n-p+1,p)$ edges in this part.

- Edges within H. Since H is K_{p-1}, this number counts to $\binom{p-1}{2}$.
- Edges between $G \setminus H$ and H. For any vertex in $G \setminus H$, it cannot have more than $p-2$ adjacent vertices in H, otherwise this will form a K_p, so we can squeeze at most $p-2$ edges between them, the total number counts to at most $(p-2)(n-p+1)$.

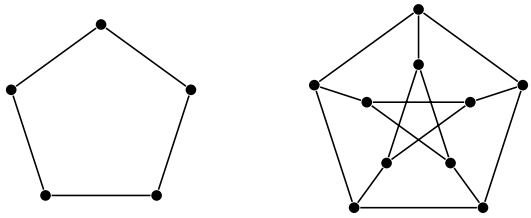
By summing up these three parts, we summarize that G has at most $\binom{p-1}{2} + (p-2)(n-p+1) + M(n-p+1,p) = M(n,p)$ edges. For the last equality, notice $n-p+1$ has the same r as n, so with $q = p-1$, we have

$$M(n,p) - M(n-q,p) = \frac{q-1}{2q}(n^2 - (n-q)^2) = \frac{(q-1)(2n-q)}{2} = \binom{q}{2} + (q-1)(n-q).$$

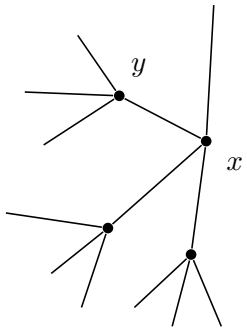
Notice the $M(n,p)$ bound is *tight*. To see this, take the complete balanced $(p-1)$-partite graph on n vertices, which has exactly $M(n,p)$ edges. It has no K_p, since among any p of its vertices, two lie in the same part and are not adjacent. Moreover, we notice that if we add any kind of edge to it, a K_p will be formed. This completes the proof. □

Theorem 3.2. *If G is a simple graph on n vertices with no C_3 or C_4 then G has at most $\frac{1}{2}n\sqrt{n-1}$ edges.*

Remark 3.3. Some graphs that have no C_3 or C_4, and exactly $\frac{1}{2}n\sqrt{n-1}$ edges:



Proof. Assume G has no C_3 or C_4, then we can visualize G by *block*. As an illustration:



For one block around a vertex x, there are $1 + \deg(x) + \sum_{y \in N(x)}(\deg(y) - 1) \leq n$ vertices, where we can rewrite the inequality as

$$\sum_{y \in N(x)} \deg(y) \leq n - 1$$

This is because x, its neighbors, and the neighbors of each $y \in N(x)$ other than x are all distinct: an edge inside $N(x)$ would give a C_3, and a common neighbor other than x of two vertices of $N(x)$

would give a C_4. Sum over all x, we have

$$\sum_{x\in V}\sum_{y\in N(x)} \deg(y) \le n(n-1)$$

Let $\chi(x,y)$ be the indicator function for adjacency relation between x, y, i.e.,

$$\chi(x,y) = \begin{cases} 1, & \text{if } x \text{ adjacent to } y \\ 0, & \text{else} \end{cases}$$

Then we can rewrite the inequality as

$$\begin{aligned}
\sum_{x\in V}\sum_{y\in N(x)} \deg(y) &= \sum_{x\in V}\sum_{y\in V} \chi(x,y)\deg(y) \\
&= \sum_{y\in V}(\deg(y)\underbrace{\sum_{x\in V}\chi(x,y)}_{\deg(y)}) \\
&= \sum_{y\in V}\deg(y)^2 \\
&\le n(n-1)
\end{aligned}$$

To proceed with the argument, we recall Cauchy–Schwarz inequality:

Theorem 3.4 (Cauchy–Schwarz)**.** *Let $\vec{v}, \vec{w} \in \mathbb{V}$, where $\mathbb{V}$ is some real vector space with a dot product. Then $\vec{v}\cdot\vec{w} \le \|\vec{v}\| \times \|\vec{w}\|$. Here $\cdot$ denotes the dot product, and $\times$ denotes the product of scalars.*

If we view $\vec{v} = (v_1, \ldots, v_n)$ and $\vec{w} = (1, \ldots, 1)$, then we have

$$v_1 + \cdots + v_n \le \sqrt{v_1^2 + \cdots + v_n^2}\cdot\sqrt{n}$$

A little bit of manipulation will yield

$$\frac{(v_1 + \cdots + v_n)^2}{n} \le v_1^2 + \cdots + v_n^2$$

So

$$\frac{(2|E|)^2}{n} = \frac{(\sum_{y\in V}\deg(y))^2}{n} \le \sum_{y\in V}\deg(y)^2 \le n(n-1)$$

where the first equality comes from Theorem 1.8. Finally, we have

$$|E|^2 \le \frac{n^2(n-1)}{4} \Rightarrow |E| \le \frac{1}{2}n\sqrt{n-1}$$

□

Theorem 3.5. *If G is a simple graph with $n \ge 3$ vertices such that $\forall v \in V, \deg(v) \ge \frac{n}{2}$, then G admits a Hamiltonian cycle, C_n.*

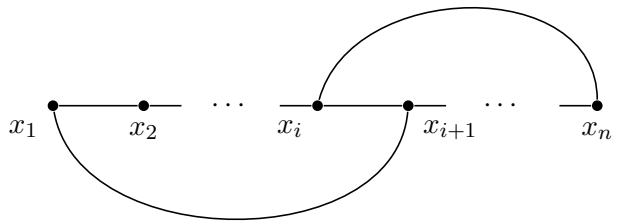
Proof. Assume for a contradiction that it is not the case, take a counterexample G on n vertices with the most edges. Note: G is not complete, since $n \geq 3$ and complete implies G admits a C_n.

Therefore, there exist $y, z \in V$ such that y is not adjacent to z. Adding yz to G keeps every degree at least $\frac{n}{2}$, so by maximality, the new graph has a Hamiltonian cycle, which must use yz. Removing yz from it, we get a path $y = x_1, x_2, \ldots, x_n = z$ from y to z through all the vertices.

Consider the following two sets:

$$A = \{i \in [n-1] : y \text{ is adjacent to } x_{i+1}\}$$
$$B = \{i \in [n-1] : z \text{ is adjacent to } x_i\}$$

Since $\deg(y), \deg(z) \geq \frac{n}{2}$, $|A|, |B| \geq \frac{n}{2}$. By pigeonhole principle, $A \cap B \neq \emptyset \Rightarrow \exists i \in A \cap B$. This results in the following graph:



Now we present a Hamiltonian cycle from x_1 to x_n, back to x_1:

$$x_1 \rightsquigarrow x_i \rightsquigarrow x_n \rightsquigarrow x_{i+1} \rightsquigarrow x_1$$

This contradicts our assumption, which states G does not admit a C_n. □

4 Matching Theory

4.1 Hall's Theorem and Systems of Distinct Representatives

Definition 4.1. Given a finite, simple graph $G = (V, E)$, a (partial) *matching* is $M \subseteq E$ such that each $v \in V$ is incident with at most one $e \in M$.

Matchings are easiest to understand on *bipartite graphs*, which leads to the next definition.

Definition 4.2. $G = (V, E)$ is *bipartite* if $V = X \sqcup Y$, such that each $e \in E$ is incident to one vertex in X and one in Y. Here $\sqcup$ denotes *disjoint union*.

Definition 4.3. Given a bipartite graph G, M is a *complete matching* from X to Y if every $x \in X$ is matched, i.e., an injection f from X to Y such that x and $f(x)$ are adjacent.

Definition 4.4. Given $G = (V, E)$ and $A \subseteq V$, let $N_G(A) = \{y \in V : \exists x \in A, \{x, y\} \in E\}$. In English, this means "G-neighbors of A".

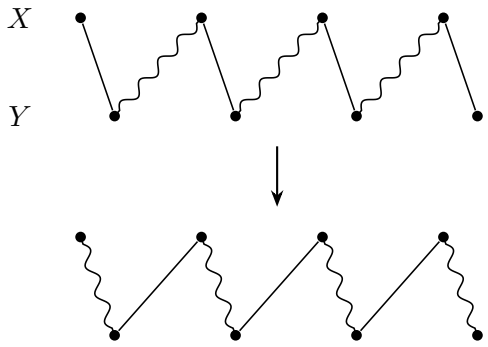
Proposition 4.5. *If G is bipartite on $X \sqcup Y$ admitting a complete matching from X to Y, then for all $A \subseteq X$, $|A| \leq |N_G(A)|$.*

Proof. Fix a complete matching M. For all $A \subseteq X$, $|A| = |N_M(A)| \leq |N_G(A)|$. □

Definition 4.6. A bipartite graph G on $X \sqcup Y$ satisfies *Hall's condition* if for all $A \subseteq X, |A| \leq |N_G(A)|$.

Theorem 4.7 (Hall)**.** *If G is a finite simple bipartite graph on $X \sqcup Y$ satisfying Hall's condition, then it admits a complete matching from X to Y.*

Proof. The fundamental move is *augmenting path*. The figure below illustrates the idea:

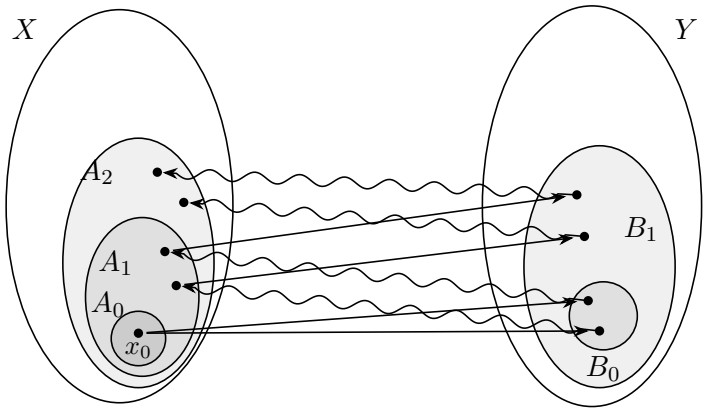


Originally, 2 endpoints are unmatched, and the path is alternating between matched and unmatched. We can extend this matching by putting all edges in this path that are not in the matching into the matching, and edges that are in the matching out of the matching. Since two endpoints are unmatched, we've extended the size of matching by 1. The following claim will help to complete the proof.

Proposition 4.8. *If M is a matching admitting no augmenting path, then every $x \in X$ is matched.*

Proof of Claim. Assume for a contradiction that some $x_0 \in X$ is unmatched. Define recursively for each $n \in \mathbb{N}$, the sets $A_n \subseteq X, B_n \subseteq Y$:

- Stage 0, $A_0 = \{x_0\}, B_0 = N_G(A_0)$;
- Stage n, $A_n = A_{n-1} \cup N_M(B_{n-1}), B_n = N_G(A_n)$.



We claim that $|A_n| < |A_{n+1}|$. To prove this claim, consider the following sequence of inequalities:

$$\begin{aligned} |A_n| &\leq |N_G(A_n)| && \text{Hall's condition} \\ &= |B_n| && \text{definition of } B_n \\ &= |N_M(B_n)| \\ &< |A_{n+1}| \end{aligned}$$

Notice $|B_n| = |N_M(B_n)|$, since every $y \in B_n$ is matched: by construction, y is reached from x_0 by a path that alternates between edges not in M and edges in M, starting with one not in M, so if y were unmatched, this path would be augmenting. And distinct matched vertices have distinct partners. The last less than relation is due to x_0 being unmatched, and A_{n+1} will include x_0. This is a contradiction since by this claim, we can infinitely run the algorithm for infinite number of stages, which is not possible since G is a finite graph. Hence, every $x \in X$ is matched. □

The above claim also completes the proof of the theorem, since a matching of maximum size admits no augmenting path. □

We also provide an alternative proof of Theorem 4.7.

Proof. By induction on $|X|$.

Base case: $|X| = 0$, then the statement is vacuous. $|X| = 1$, then since $|X| \leq |N_G(X)|$, just arbitrarily pick a neighbor of the only vertex $x \in X$, and this completes the matching.

Inductive step: we consider two cases.

Case 1 Suppose $\forall A \subseteq X$ with $\emptyset \neq A \neq X$, we have $|A| < |N_G(A)|$. In this case, we just arbitrarily pick an edge $e = (x, y)$ for $x \in X, y \in Y$, and discarding e and both x and y, we have a graph with $|X|$ being 1 less. Hall's condition still holds, since every nonempty $A \subseteq X \setminus \{x\}$ is not X, so we originally have $|A| < |N_G(A)| \Rightarrow |A| \leq |N_G(A)| - 1$, and removing y shrinks $N_G(A)$ by at most 1, thus the condition still holds. By inductive hypothesis, we have a complete matching on the remaining graph, and if we put x and y back, we obtain a complete matching from X to Y.

Case 2 Suppose $\exists A \subseteq X$ with $\emptyset \neq A \neq X$ and $|A| = |N_G(A)|$. Then we match each vertex in A to a vertex in $N_G(A)$ by inductive hypothesis, since $|A| < |X|$, and the graph between A and $N_G(A)$ satisfies Hall's condition, because $N_G(A') \subseteq N_G(A)$ for $A' \subseteq A$, and remove both A from X and $N_G(A)$ from Y. It remains to show that the remaining graph still satisfies Hall's condition. Assume otherwise the condition does not hold, then in the remaining graph, $\exists B \subseteq X'$ with $|B| > |N_{G'}(B)|$. Since originally the condition holds, it must be the case that some vertices in $N_G(B)$ are also in $N_G(A)$, and they got removed. Notice A and B are disjoint, so $|A \cup B| = |A| + |B|$. Further, $N_G(A) \cap N_G(B) \neq \emptyset$, let's say their overlap part has cardinality k for k being some positive natural, so

$$\begin{aligned} |N_G(A) \cup N_G(B)| &= |N_G(A)| + |N_G(B)| - k \\ &= |A| + |N_G(B)| - k \\ &= |A| + |N_{G'}(B)| \\ &< |A| + |B| \\ &= |A \cup B| \end{aligned}$$

which contradicts Hall's condition on original graph G. Therefore, the remaining graph still satisfies Hall's condition, and we again apply inductive hypothesis on remaining graph, which is smaller since $A \neq \emptyset$, to obtain a complete matching, then put back A and $N_G(A)$, we have gained a complete matching on G, as desired.

□

Definition 4.9. Suppose $\mathcal{A} = \{A_1, \ldots, A_n\}$ is a family of finite sets. A *system of distinct representatives*, *SDR*, is a sequence $a_1, \ldots, a_n$, such that

- $a_i \neq a_j$ when $i \neq j$
- $a_i \in A_i$

Definition 4.10. Such a family satisfies *Hall's condition* if $k \leq |A_{i_1} \cup \cdots \cup A_{i_k}|$ for $i_1 < \cdots < i_k$.

Intuitively, this means for any k sets we choose from $\mathcal{A}$, the cardinality of their union is at least k.

Corollary 4.11. *If $\mathcal{A}$ satisfies Hall's condition, then it admits an SDR.*

Proof. Build a graph G on $X \sqcup Y$, $X = \mathcal{A}, Y = \bigcup \mathcal{A} = A_1 \cup \cdots \cup A_n$. G will render adjacent $A \in X$ and $a \in Y$ if and only if $a \in A$. Notice for $\mathcal{B} \subseteq X$, $N_G(\mathcal{B})$ is the union of the sets in $\mathcal{B}$, so G satisfies Hall's condition. By Theorem 4.7, there exists a complete matching from X to Y, fix such a matching, and for $A \in X$, put a that is matched with it as its representative. We therefore have an SDR for $\mathcal{A}$. □

4.2 Applications of Hall's matching

Theorem 4.12 (D. Kőnig)**.** *Suppose A is a finite matrix with entries 0 or 1. Define:*

- *$m :=$ min number of rows or columns needed to cover all 1's.*
- *$M :=$ max number of 1's, no two of which share a row or column.*

Then $m = M$.

Example 4.13. Consider the following matrix:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

In this matrix, we have $m = M = 2$.

Proof. To show $m = M$, we first show $m \geq M$, then $M \geq m$.

$m \geq M$: for each independent 1, we need a row or a column to cover it, so $m \geq M$.

$M \geq m$: fix a covering with m rows or columns, we need to build a set of m-many independent 1's. Without loss of generality, we assume it covers the first r rows and c cols of A, consider the following collection:

$$\mathcal{R} = \{R_1, \ldots, R_r\}, R_i = \{j > c : a_{ij} = 1\}$$

We claim that $\mathcal{R}$ satisfies Hall's condition, i.e., $k \leq |R_{i_1} \cup \cdots \cup R_{i_k}|$.

Assume for a contradiction that there exist k rows with $|R_{i_1} \cup \cdots \cup R_{i_k}| < k$, this means that the 1's of these k rows that have not yet been covered by the c cols lie in fewer than k cols, so replace these rows with those fewer cols, we have obtained a better covering, contradicting the optimal covering. So by Corollary 4.11, we have an SDR for $\mathcal{R}$, this SDR forms a set of r-many independent 1's.

The same argument can be applied on columns, which yields c-many independent 1's.

In total, we have $r + c = m$ independent 1's, since the first set uses the first r rows and cols after the first c, while the second uses the first c cols and rows after the first r, therefore $M \geq m$. □

Next theorem is a baby version of Birkhoff's Theorem.

Definition 4.14. A *permutation matrix* is a square 0/1 matrix such that each row and column has exactly one 1, i.e., a permutation.

Theorem 4.15 (Baby Birkhoff)**.** *Suppose A is a square matrix with non-negative integer entries such that each row and column sums to some fixed $l > 0$, then A is the sum of l-many permutation matrices.*

Example 4.16. Consider the following matrix, where $l = 5$:

$$\begin{bmatrix} 3 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 2 \end{bmatrix}$$

We can write it as a summation of

$$2\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Note that a permutation matrix is essentially a mapping of rows to cols.

Proof. By induction on l.

Base case: $l = 1$, then A itself is a permutation matrix.

Inductive step: build a graph G on $\text{Rows} \sqcup \text{Cols}$: row_i is adjacent to col_j if and only if $A_{ij} > 0$. We claim that G satisfies Hall's condition. To prove the claim, we need to show that any k-many rows are adjacent to at least k-many cols.

Pick k rows arbitrarily. The sum of these k rows is kl, since each col contains at most l of this sum, we need at least k-many cols to cover this sum. Thus, Hall's condition is satisfied.

So we have a complete matching in G from Rows to Cols, subtract the corresponding permutation matrix, which leaves non-negative integer entries, since we only subtract 1 from positive entries, with rows and cols summing to $l - 1$, then apply inductive hypothesis on remaining matrix, we've completed the proof. □

Remark 4.17. The formal version of Birkhoff's Theorem states that, l can be non-negative real number (and A has non-negative real entries), and A is a non-negative linear combination of permutation matrices with coefficients summing to l, instead of exactly l-many. The proof can be done similarly, by induction on $\text{nnz}(A)$, where nnz denotes number of non-zero entries.

5 Posets & Extremal Set Theory

Definition 5.1. A *partial order* (on some set) is a binary relation $\leq$ satisfying

- Reflexive, $x \leq x$;
- Antisymmetry, $x \leq y \wedge y \leq x \Rightarrow x = y$;
- Transitive, $x \leq y \wedge y \leq z \Rightarrow x \leq z$.

Definition 5.2. Suppose $(P, \leq)$ is a poset and $B \subseteq P$,

- If any two elements of B can be compared, B is called a (combinatorial) *chain*;
- If no two elements of B can be compared, B is called a (combinatorial) *anti-chain*.

Theorem 5.3 (Dilworth)**.** *Suppose $(P, \leq)$ is a finite poset, let*

- $m :=$ *min number of chains* $C_1, \ldots, C_m \subseteq P$ *with* $P = C_1 \cup \cdots \cup C_m$.
- $M :=$ *max size of an anti-chain in* P.

Then $M = m$.

Proof. Notice $m \geq M$ is obvious: for each element in the max-size anti-chain, we need at least one chain to cover it.

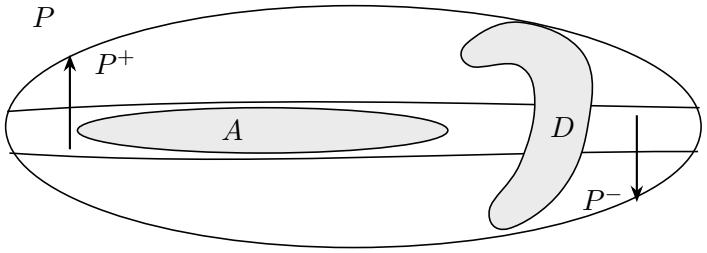
We establish the other direction by induction on $|P|$.

Base case: $|P| = 0$, then the statement is vacuous; $|P| = 1$, then the size of any anti-chain is 1, and we have exactly one chain.

Inductive step: let $D \subseteq P$ be a maximal chain, i.e., it cannot be extended. Consider $P \setminus D$.

Case 1 Max anti-chain size in $P \setminus D$ is $\leq M - 1$, by inductive hypothesis, there are chains $C_1 \cup \cdots \cup C_{M-1}$ which cover $P \setminus D$, then we can add D back, we obtain an M-cover for P.

Case 2 There is an anti-chain $A = \{a_1, \ldots, a_M\} \subseteq P \setminus D$. Note that A is still maximal in P, so for every $x \in P$, x is comparable to at least one $a_i \in A$. Put $P^+ = \{x \in P : \exists a \in A, a \leq x\}, P^- = \{x \in P : \exists a \in A, x \leq a\}$. Notice $P^+ \cup P^- = P, P^+ \cap P^- = A$.



Observe: $|P^+| < |P|$, to see this, let d be the least element of D, we claim $d \notin P^+$, since otherwise, we can extend D by the element in A that is smaller than d, which contradicts D being maximal. By a similar argument, we have $|P^-| < |P|$.

Thus, we can apply inductive hypothesis on P^+ and P^-, whose max anti-chain size is still M since both contain A, to obtain $C_1^+, \ldots, C_M^+$ with $P^+ = C_1^+ \cup \cdots \cup C_M^+$ and $C_1^-, \ldots, C_M^-$

with $P^- = C_1^- \cup \cdots \cup C_M^-$, such that $a_i \in C_i^+ \cap C_i^-$, since each of these chains contains at most one element of A, and every a_i is covered. Put $C_i = C_i^+ \cup C_i^-$, we get an M-cover for P. Notice C_i is a chain, since a_i is the least element of C_i^+: if $x \in C_i^+$ and $x < a_i$, then since $x \in P^+$, $a \leq x < a_i$ for some $a \in A$, which is impossible in an anti-chain. Similarly, a_i is the greatest element of C_i^-.

□

Theorem 5.4 (Mirsky)**.** *Suppose $(P, \leq)$ is a finite poset, let*

- $n :=$ *min number of anti-chains needed to cover P.*
- $N :=$ *max size of chain in P.*

Then $n = N$.

Proof. $n \geq N$ is trivial, for each element in the max-size chain, we need one anti-chain to cover it.

To prove $N \geq n$, we induct on $|P|$.

Base case is exactly the same as in Theorem 5.3.

Inductive step: consider $A = \{a \in P : \forall p \in P, a \leq p \Rightarrow a = p\}$, i.e., A is the collection of *maximal elements* of P. Certainly, A is an anti-chain. We work in $P \setminus A$.

Proposition 5.5. *The maximal size of a chain in $P \setminus A$ is at most $N - 1$.*

Proof of Claim. Fix a largest chain C in $P \setminus A$. In P, it can be extended to a strictly larger chain, since its largest element is not in A, i.e., not maximal, so there is a maximal element of P above it (P is finite). Since maximal elements are contained in A, we can pick one $a_i \in A$ to extend C. Thus, $|C| \leq N - 1$. □

By induction hypothesis, $P \setminus A$ can be covered by $N - 1$ anti-chains, in P, extend such covering by A, we obtain an N-cover of P, as desired. □

One particularly important poset: $(\mathcal{P}(X), \subseteq)$.

Definition 5.6. $\mathcal{A} \subseteq \mathcal{P}(X)$ is an *intersecting family* if $\forall A_i, A_j \in \mathcal{A}$, $A_i \cap A_j \neq \emptyset$.

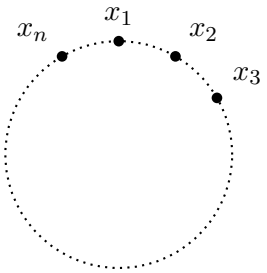
We ask the following question: suppose $|X| = n$ and $k \leq n$, if $\mathcal{A} \subseteq [X]^k$ and is an intersecting family, how big can $\mathcal{A}$ be?

Observation: if $k > n/2$, then $[X]^k$ is already an intersecting family. What about $k \leq n/2$?

Consider the following obvious construction: pick some $x_0 \in X$, put $\mathcal{A} = \{A \in [X]^k : x_0 \in A\}$, this is an intersecting family with $|\mathcal{A}| = \binom{n-1}{k-1}$.

Theorem 5.7 (Erdős–Ko–Rado)**.** *If $|X| = n, k \leq n/2$ and $\mathcal{A} \subseteq [X]^k$ is an intersecting family, then $|\mathcal{A}| \leq \binom{n-1}{k-1}$.*

Proof. Place elements of X on a circle:



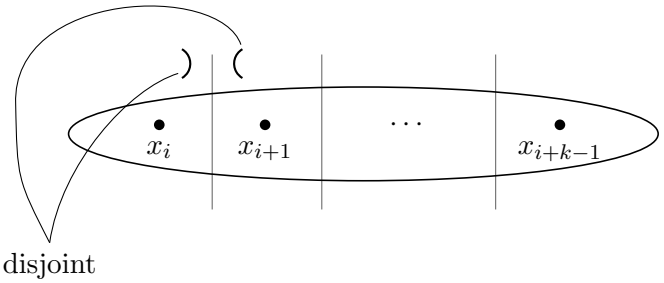
Let $\mathcal{S} = \{S_1, S_2, \ldots, S_n\}$ consist of "consecutive k-blocks", on the circle. Formally,

$$S_i = \{x_i, \ldots, x_{i+k-1}\},$$

with indices modulo n. We prove the following claim, which is key to the overall proof.

Proposition 5.8. *If $B \subseteq \mathcal{S}$ is an intersecting family, then $|B| \leq k$.*

Proof. Suppose $S_i \in B$, consider these $k-1$ "gaps":



Every other block in B meets S_i, so it either starts just after one of these gaps or ends just before one of them. For the gap between x_{i+j-1} and x_{i+j} $(1 \leq j \leq k-1)$, the blocks S_{i+j-k} and S_{i+j} on its two sides occupy $2k \leq n$ consecutive positions, so they are disjoint, and B contains at most one of them. Thus, B contains at most $1 + (k-1) = k$ blocks. □

There are $n!$ ways to put x's on the circle. Given such a placement $\pi : X \to$ circle, let S_π denote the corresponding family of blocks. So the claim shows:

$$\sum_\pi |\mathcal{A} \cap S_\pi| \leq \sum_\pi k = kn!$$

A second claim will establish the final result.

Proposition 5.9. $\sum_\pi |\mathcal{A} \cap S_\pi| = |\mathcal{A}| \cdot n \cdot k!(n-k)!$.

Proof. Fix $A \in \mathcal{A}$, consider its contribution to the overall summation.

Given a particular block, there are $k!$ ways to place A into that block, $(n-k)!$ ways to arrange all non-A elements. There are n blocks in total, so A contributes exactly $n \cdot k!(n-k)!$ to the summation, so

$$\sum_\pi |\mathcal{A} \cap S_\pi| = |\mathcal{A}| \cdot n \cdot k!(n-k)!$$ □

We thus have

$$\begin{aligned} |\mathcal{A}| \cdot n \cdot k!(n-k)! &\leq kn! \\ |\mathcal{A}| &\leq \frac{n!}{k!(n-k)!}\frac{k}{n} \\ &= \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \binom{n-1}{k-1} \end{aligned}$$

□

6 Flows & Networks

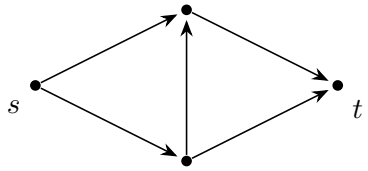
6.1 Max-flow and Min-cut

Definition 6.1. A *directed graph* is a graph with edges assigned as ordered pairs.

Definition 6.2. A *network* is a (typically simple, finite) directed graph with two special vertices:

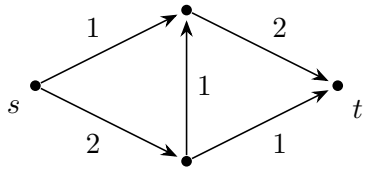
- s : source (only out-edges)
- t : sink (only in-edges)

Example 6.3. A network with 4 vertices and 5 edges.



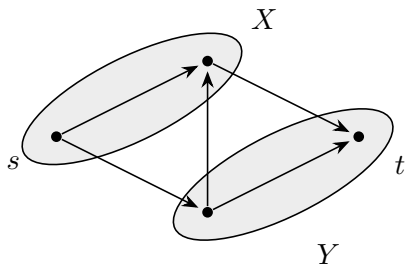
Definition 6.4. A *flow* in a network is a function $f : E \to [0, \infty)$ such that for all $v \neq s, t$, $\text{inflow}(v) = \text{outflow}(v)$, where $\text{inflow}(v) = \sum_{e, \text{ edges into } v} f(e)$, $\text{outflow}(v) = \sum_{e, \text{ edges out of } v} f(e)$.

Example 6.5. A flow of Example 6.3.



Definition 6.6. A *cut* in a network is a partition $V = X \sqcup Y$ with $s \in X, t \in Y$.

Example 6.7. A cut of Example 6.3.



Definition 6.8. The *strength* of a flow f, given a cut from X to Y, is $\sum_{e \text{ edges } X \to Y} f(e) - \sum_{e \text{ edges } Y \to X} f(e)$.

Example 6.9. In the flow of Example 6.5 with cut of Example 6.7, the strength from X to Y is $2 + 2 - 1 = 3$.

Proposition 6.10. *Given a flow on a (finite) network, any two cuts see the same strength.*

Proof. It suffices to check that if $X \sqcup Y = V$ is a cut and $v \in Y$, $v \neq t$, then $X' = X \cup \{v\}, Y' = Y \setminus \{v\}$ see the same strength as X, Y. We wish to check:

$$\sum_{e:X\to Y} f(e) - \sum_{e:Y\to X} f(e) = \sum_{e:X'\to Y'} f(e) - \sum_{e:Y'\to X'} f(e)$$

which is equivalent to

$$\sum_{e:X\to Y} f(e) - \sum_{e:X'\to Y'} f(e) = \sum_{e:Y\to X} f(e) - \sum_{e:Y'\to X'} f(e)$$

Further notice

$$\sum_{e:X\to Y} f(e) - \sum_{e:X'\to Y'} f(e) = \sum_{e:X\to v} f(e) - \sum_{e:v\to Y'} f(e)$$

and

$$\sum_{e:Y\to X} f(e) - \sum_{e:Y'\to X'} f(e) = \sum_{e:v\to X} f(e) - \sum_{e:Y'\to v} f(e)$$

Take the difference of the above two equations, we have

$$\sum_{e:X\to v} f(e) - \sum_{e:v\to X} f(e) + \sum_{e:Y'\to v} f(e) - \sum_{e:v\to Y'} f(e) = 0$$

since the LHS is exactly $\text{inflow}(v) - \text{outflow}(v)$: every edge at v comes from or goes to X or Y'. So we have

$$\sum_{e:X\to Y} f(e) - \sum_{e:Y\to X} f(e) - \sum_{e:X'\to Y'} f(e) + \sum_{e:Y'\to X'} f(e) = 0$$

Thus,

$$\sum_{e:X\to Y} f(e) - \sum_{e:Y\to X} f(e) = \sum_{e:X'\to Y'} f(e) - \sum_{e:Y'\to X'} f(e)$$

as desired. □

Definition 6.11. A *capacity* of a network is a function $C : E \to [0, \infty)$, for convenience, we'll assume $C : E \to \mathbb{N}$.

Definition 6.12. A flow *obeys* a capacity C, if $\forall e \in E, f(e) \leq C(e)$.

Question: Given a capacity, what is the max strength of a flow obeying it?

Definition 6.13. Given a capacity C and a cut $X \sqcup Y$, the corresponding *cut-capacity* is $C(X, Y) = \sum_{e:X\to Y} C(e)$.

Proposition 6.14. *If f is a flow obeying C and $X \sqcup Y$ is any cut, then* $\text{strength}(f) \leq C(X, Y)$.

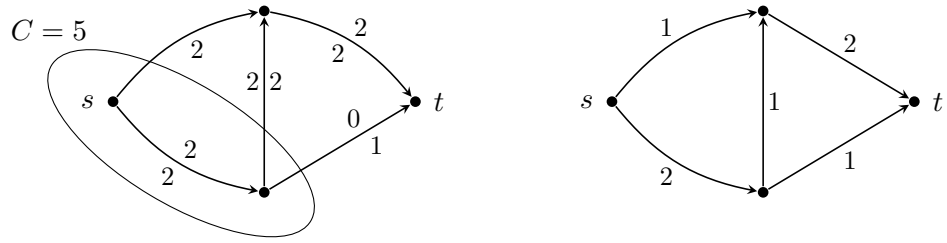
Proof.

$$\begin{aligned}
\text{strength}(f) &= \sum_{e:X\to Y} f(e) - \sum_{e:Y\to X} f(e) \\
&\leq \sum_{e:X\to Y} f(e) + 0 \\
&\leq \sum_{e:X\to Y} C(e) + 0 \\
&= C(X, Y)
\end{aligned}$$

□

Theorem 6.15 (Ford–Fulkerson)**.** *Max-flow = Min-cut, i.e., if* $r = \min_{X \sqcup Y \text{ is a cut}} C(X, Y)$*, then there is a flow obeying* C *of strength* r*.*

Example 6.16. The flow on the left meets the max-flow & min-cut requirement.



Proof. Given a flow f obeying C, a path $s = v_1 e_1 v_2 e_2 \dots e_k v_{k+1}$ is *augmenting* if

- $f(e_i) < C(e_i)$ when $v_i \xrightarrow{e_i} v_{i+1}$, in this case we can add value to f.
- $f(e_i) > 0$ when $v_i \xleftarrow{e_i} v_{i+1}$, in this case we can subtract value from $f(e_i)$.

If there is an augmenting path from s to t, we can increase the flow's strength.

Assume we now have a flow $\hat{f}$ obeying C with no such augmenting path from s to t, we will build a cut $X \sqcup Y$ such that $\text{strength}(\hat{f}) = C(X, Y)$. Such an $\hat{f}$ exists: since C is integer-valued, start with the zero flow and keep changing the flow along an augmenting path from s to t by the smallest available amount, which is a positive integer. Each step raises the strength by at least 1, and the strength never exceeds r, so this stops.

Put $X = \{v \in V : \exists \text{ an augmenting path from } s \text{ to } v \text{ in } \hat{f}\}, Y = V \setminus X$. Note $s \in X$ and $t \in Y$, so the cut is valid.

Proposition 6.17. $\text{strength}(\hat{f}) = C(X, Y)$.

Proof of Claim. $\text{strength}(\hat{f}) = \sum_{e:X\to Y} \hat{f}(e) - \sum_{e:Y\to X} \hat{f}(e) = \sum_{e:X\to Y} C(e) - 0 = C(X, Y)$. The main part we wish to prove is

1. $\sum_{e:X\to Y} \hat{f}(e) = \sum_{e:X\to Y} C(e)$
2. $\sum_{e:Y\to X} \hat{f}(e) = 0$

For the first part, suppose it is not the case, then some edge e from some $u \in X$ to some $w \in Y$ has $\hat{f}(e) < C(e)$. Since we already have an augmenting path from s to u, we can then extend the path by e to w, contradicting the definition of X and Y.

For the second part, the similar argument applies, if an edge from Y to X has non-zero flow, then we can extend the augmenting path backward along it. Thus, $\text{strength}(\hat{f}) = C(X, Y)$. □

The above claim also completes the proof of the theorem, since $\text{strength}(\hat{f}) = C(X, Y) \geq r$, and by the previous proposition, $\text{strength}(\hat{f}) \leq r$. □

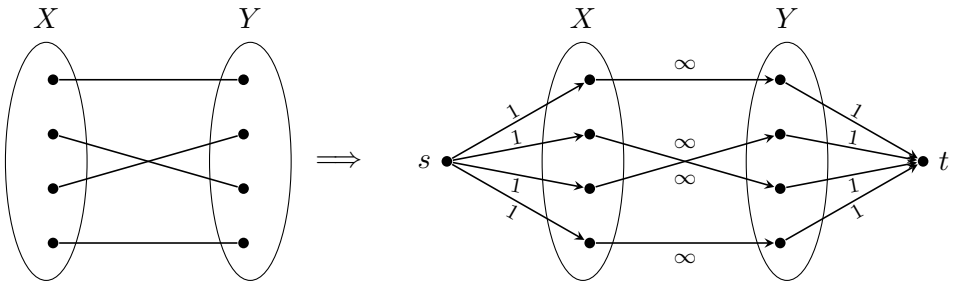
6.2 More flows and applications

Theorem 6.18. *Suppose we have a network with integer-valued capacity $C : E \to \mathbb{N}$, then there is an integer-valued flow $f : E \to \mathbb{N}$ obeying C satisfying* strength$(f) =$ *min-cut.*

The proof of this theorem combines Theorem 6.15 and a theorem that will be proved later, so we omit the proof of theorem.

Below, we present an alternative proof of Theorem 4.7.

Proof. We will convert G into a network, G^*, as the figure presented below.



More formally, we add two vertices s, t, add and direct edges from s to all vertices in X, direct all edges from X to Y, and add and direct edges from all vertices in Y to t. For $s \to X$ and $Y \to t$ edges, we give them capacities 1. For remaining edges, we give them capacities M such that $M \ggg |E|, M \ggg |V|$. Think of M as `INT_MAX` in programming languages.

Proposition 6.19. *Min-cut* $= |X|$.

Proof of Claim. We claim that there is a cut of capacity $|X|$: $S = \{s\}, T = V^* \setminus \{s\}$.

We need to show that if S, T is a cut, then $C(S, T) \geq |X|$. Put $A = S \cap X$.

Case 1 $N_G(A) \not\subseteq S$, i.e., there exists a vertex $y \in T$ such that some $x \in A$ is adjacent to y, then $C(S, T) \geq M \geq |X|$.

Case 2 $N_G(A) \subseteq S$, i.e., all G-neighbors of A are also included in S. Then $C(S, T)$ is at least $|X \setminus A|$, which is edges from s to $X \setminus A$, plus $|N_G(A)|$, which counts edges from $N_G(A)$ to t. Because G admits Hall's condition, $|A| \leq |N_G(A)|$, thus $|X \setminus A| + |N_G(A)| \geq |X \setminus A| + |A| = |X|$, $C(S, T) \geq |X|$, as desired.

□

Thus, there is an integer-valued flow $f : E \to \mathbb{N}$ obeying C, such that strength$(f) = |X|$. We claim such f gives a complete matching from X to Y. To see this, consider the cut $S = X \cup \{s\}, T = Y \cup \{t\}$. The strength of this cut is exactly $|X|$, moreover, for each $x \in X$, there is exactly one edge with flow 1 from x to a vertex $y \in Y$, all other edges out of x all have flow 0. This is true because we must have inflow$(x) =$ outflow(x), and all in-flow x receives comes from s, which is at most 1. Since the outflows of all $x \in X$ add up to the strength $|X|$ of this cut, each of them is exactly 1, and since f is integer-valued, it is carried by a single edge. For y, we claim that at most one in-edge has flow 1. Suppose otherwise, there are more edges with flow 1, notice outflow$(y) \leq 1$, so this is not possible.

Thus, by following the max-flow, we obtain a complete matching from X to Y. □

In general, we can "round" flows to be integer-valued.

Definition 6.20. A *circulation* on a directed graph is a function $f : E \to \mathbb{R}$ such that $\forall v \in V$, $\text{inflow}(v) = \text{outflow}(v)$.

Flows are circulations up to encoding. We add and direct an edge from t to s, and in turn, we reduce a flow into a circulation.

Theorem 6.21. *Suppose f is a circulation on a directed graph G, then there is an integer-valued circulation $g : E \to \mathbb{Z}$ satisfying that $\forall e \in E, g(e) = \begin{cases} \lfloor f(e) \rfloor \\ \lceil f(e) \rceil \end{cases}$. Equivalently, $\lfloor f(e) \rfloor \leq g(e) \leq \lceil f(e) \rceil$.*

Proof. For each circulation g, let $\text{nonint}(g) := |\{e \in E : g(e) \notin \mathbb{Z}\}|$, choose a circulation g satisfying $\lfloor f(e) \rfloor \leq g(e) \leq \lceil f(e) \rceil$ with $\text{nonint}(g)$ minimal. We'll argue that $\text{nonint}(g) = 0$.

Toward a contradiction, suppose $\text{nonint}(g) > 0$. Consider the subgraph with edges $D = \{e \in E : g(e) \notin \mathbb{Z}\}$, obviously, $D \neq \emptyset$.

Notice that no vertex is incident to exactly one edge in D, since $\text{inflow}(v) = \text{outflow}(v)$, $\pm g(e) +$ (a sum of integers) $= 0$ is not possible. So the subgraph induced by D has no leaves, which means it has a cycle.

Add some ϵ to the flow to the cycle, we obtain a circulation with more integer edges than g, contradicting that g has minimum number of non-integer edges. To be precise, going around the cycle, we add ϵ on the edges traversed forward and subtract ϵ on the edges traversed backward, which keeps inflow = outflow at every vertex. Every edge e of the cycle is in D, so $\lfloor f(e) \rfloor < g(e) < \lceil f(e) \rceil$. Take the largest $\epsilon > 0$ that keeps every value in $[\lfloor f(e) \rfloor, \lceil f(e) \rceil]$, then at least one edge of the cycle becomes an integer, and no edge outside the cycle changes. □

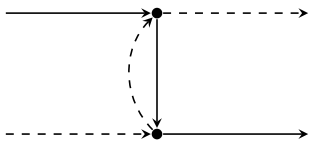
Theorem 6.22 (Menger)**.** *Given a finite simple graph $G = (V, E)$ and distinct vertices s, t let*

- *$M :=$ max number of edge-disjoint paths from s to t.*
- *$m :=$ min number of edges in an s-t cut.*

Then $m = M$.

Proof. We construct a graph G^* by directing all edges from s to $N_G(s)$, directing all edges from $N_G(t)$ to t, and for all other vertices u, v, if there is an edge $\{u, v\}$, then we change it to $(u, v), (v, u)$. Give all edges capacities 1.

Obviously, m = min-cut, and by Theorem 6.15, we have m = max-flow. It remains to show that M = max-flow. First, $M \leq m$, since each of M edge-disjoint paths from s to t must use an edge of any s-t cut. Let f be an integer-valued max-flow, which exists by the integrality theorem above, so $\text{strength}(f) = m$. The proof strategy will be, constructing m edge-disjoint paths, using f. Notice the annoying part is that if both $(u, v), (v, u)$ have flow 1, we might have two paths using these two edges, but in G, they are the same edge, as an illustrating example:



Notice by setting $f((u,v)) = f((v,u)) = 0$, the strength of f has not been changed, so we can make such a move. More generally, if some edges with flow 1 form a directed cycle, setting the flow on them to 0 keeps a flow of the same strength, since each vertex on the cycle loses one unit of inflow and one unit of outflow, and the cycle avoids s and t. So without loss of generality, there is no such cycle. By doing so, we claim that max-flow f yields a set of edge-disjoint paths from s to t. Consider the following algorithm:

```
u = s
while there exists some edge with flow 1:
     if u = t:
          u = s
          continue
     let (u,v) be an edge with flow 1
     remove (u,v)
     u = v
assert u = t
```

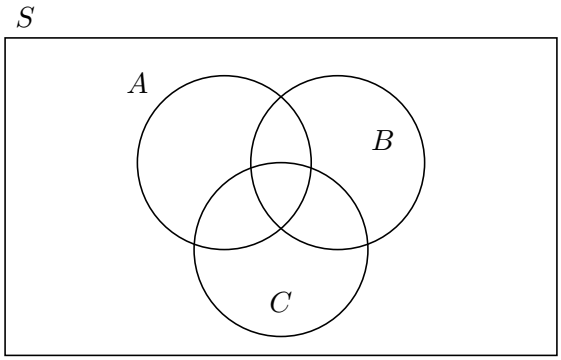
Our goal is to show this algorithm terminates without getting stuck. Suppose otherwise that the algorithm gets stuck at some round, then it must be the case that we have followed an edge with flow 1 to v, and find no out-edge with flow 1, this contradicts $\text{inflow}(v) = \text{outflow}(v)$. It cannot get stuck at $u = s$ either: if some edge still has flow 1, following edges with flow 1 backward from it never repeats a vertex, since there is no directed cycle, so it must stop, and by inflow = outflow it can only stop at s. Moreover, this algorithm produces edge-disjoint paths, since we have avoided two paths using $(u,v),(v,u)$ by assigning both of them 0, and each walk from s to t never repeats a vertex, again because there is no directed cycle of edges with flow 1. Thus, we have $M = \text{max-flow}$. □

7 Principle of Inclusion & Exclusion

7.1 Inclusion & Exclusion

We start with an inspiring Venn diagram of this topic.

Example 7.1. Let $A, B, C \subseteq S$ be finite sets, what is $|S \setminus (A \cup B \cup C)|$?



$$|S \setminus (A \cup B \cup C)| = |S| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$$

We provide a generalization of the above result, which will be central in this section.

Setup: Let S be a finite set, $E_1, \ldots, E_r$ be subsets of S. For each $M \subseteq [r]$, put $N(M) = |\bigcap_{i \in M} E_i|$, put, for each $j \in [r]$, $N_j = \sum_{M \in [r]^j} N(M)$.

Theorem 7.2. $|S \setminus \bigcup_{i \leq r} E_i| = |S| - N_1 + N_2 - \cdots + (-1)^r N_r$.

Proof. We argue for each $s \in S$:

1. if $s \notin \bigcup_i E_i$, then s contributes 1 to the sum;
2. if $s \in \bigcup_i E_i$, then s contributes 0 to the sum.

Suppose $s \notin \bigcup_i E_i$, then s only appears in $|S|$ part, its contribution is exactly 1.

Suppose $s \in \bigcup_i E_i$, let $M = \{i \leq r : s \in E_i\}$, and $k = |M| \geq 1$, then its contribution is:

$$\underbrace{|S| - N_1 + N_2 - \cdots + (-1)^k N_k - \cdots + (-1)^r N_r}_{1 - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k} + 0 + \cdots + 0}$$

This is because s is counted in $N(M')$ exactly when $M' \subseteq M$, so it is counted $\binom{k}{j}$ times in N_j. By the binomial theorem, it is

$$\sum_{i=0}^{k} \binom{k}{i} (-1)^i 1^{k-i} = [1 + (-1)]^k = 0$$

□

Example 7.3. Counting derangements:

Definition 7.4. Given a set X, let $S_X = \{\sigma : X \to X : \sigma \text{ is a bijection}\}$, i.e., S_X is the set of all permutations, let $D_X = \{\sigma \in S_X : \forall x \in X, \sigma(x) \neq x\}$, i.e., D_X is the set of all *derangements*.

Proposition 7.5. *Suppose* $|X| = n \in \mathbb{N}$*, then* $|D_X| := d_n = \sum_{i=0}^{n} \frac{(-1)^i}{i!} n!$.

Proof. Put $S = S_X$, so $|S| = n!$. Put, for each $x \in X$, $E_x = \{\sigma \in S : \sigma(x) = x\}$, so $D_X = S \setminus \bigcup_{x \in X} E_x$. For each $M \subseteq X$, $N(M) = |\{\sigma : \forall x \in M, \sigma(x) = x\}|$, to count it, we fix $|M|$ points and permute remaining points, which yields $(n-|M|)!$. Then $N_j = \sum_{M \in [X]^j} N(M) = \binom{n}{j}(n-j)! = \frac{n!}{j!(n-j)!}(n-j)! = \frac{n!}{j!}$.

Finally,

$$\begin{aligned} d_n &= |S| + \sum_{i=1}^{n} (-1)^i N_i \\ &= n! + \sum_{i=1}^{n} (-1)^i \frac{n!}{i!} \\ &= n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} \end{aligned}$$

□

Corollary 7.6. *A randomly chosen permutation has a probability* $\approx \frac{1}{e}$ *of being a derangement.*

Proof. By Proposition 7.5, we have

$$\frac{d_n}{|S_X|} = \sum_{i=0}^{n} \frac{(-1)^i}{i!} \approx \frac{1}{e}$$

□

Proposition 7.7. $\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n = n!$.

Proof. For X, Y with $|X| = |Y| = n$, the sum counts number of surjections from X to Y. Since $|X| = |Y|$, any surjection is a bijection, so this number is $n!$, as RHS shows.

Let $S = \{\text{All functions } f : X \to Y\}$, for each $y \in Y$, put $E_y = \{f : y \notin \text{image}(f)\}$, so given an $M \subseteq Y$, we have $N(M) = (n - |M|)^n$, first rule out $|M|$ y's then count the total number of functions. So $N_j = \sum_{M \in [Y]^j} (n-|M|)^n = \binom{n}{j}(n-j)^n$. By Theorem 7.2, we have this number being $n^n + \sum_{i=1}^{n} (-1)^i \binom{n}{i} (n-i)^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n$, which is LHS.

Notice the same argument works for $|X| = k$: now $N(M) = (n-|M|)^k$, so $\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^k$ is the number of surjections from a k-element set to an n-element set. □

Example 7.8. If $k < n$, $\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^k = 0$, since there is no surjection from $[k]$ to $[n]$.

Definition 7.9. For $n \geq 1$, the *Euler function*, ϕ, counts the number of $k \leq n$ such that $\gcd(k, n) = 1$.

Example 7.10.

$$\phi(20) = 20 - (\text{multiples of } 2 + \text{multiples of } 5) + (\text{multiples of } 2 \ \& \ 5) = 20 - (10 + 4) + 2 = 8$$

Theorem 7.11. $\sum_{d|n} \phi(d) = n$.

Proof. It's easier to evaluate $\sum_{d|n} \phi(\frac{n}{d})$, which is the same sum, since $d \mapsto \frac{n}{d}$ permutes the divisors of n. We claim that for each $d \mid n$, there are exactly $\phi(\frac{n}{d})$ integers $m \leq n$ such that $\gcd(m,n) = d$. This is because, such m has form $m'd$, such that $\gcd(m', \frac{n}{d}) = 1$ and $m' \leq \frac{n}{d}$. So $\sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} |\{m \leq n : \gcd(m,n) = d\}| = |\{m \leq n\}| = n$. □

Definition 7.12. For $n \geq 1$, the *Möbius function*, μ, is defined as

$$\mu(n) = \begin{cases} 1, & \text{if } n = \underbrace{p_1 \cdots p_k}_{\text{even number of distinct primes}} \\ -1, & \text{if } n = \underbrace{p_1 \cdots p_k}_{\text{odd number of distinct primes}} \\ 0, & \text{not square-free} \end{cases}$$

Specifically, we have $\mu(1) = 1$.

Theorem 7.13. $\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{if } n = 1 \\ 0, & \textit{otherwise} \end{cases}$.

Proof. For $n = 1$ the sum is $\mu(1) = 1$. Assume $n > 1$ and $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, the only divisors which contribute to the sum have the form $\prod_{i \in A} p_i$, for $A \subseteq [r]$, since the others are not square-free. There are $\binom{r}{i}$ such divisors with $|A| = i$, and $r \geq 1$ since $n > 1$. So $\sum_{d|n} \mu(d) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} = 0$. □

7.2 Description, Involution, Exception

We first recall the binomial theorem:

Theorem 7.14 (Binomial)**.**

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Plug $x = 1, y = 1$, we get

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Plug $x = -1, y = 1$, we get, for $n \geq 1$,

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$$

A combinatorial interpretation of the above result is, for $[n]$, the number of subsets with cardinality even is equal to the number of subsets with cardinality odd. We give a proof of this.

Definition 7.15. Let X be a set. A *toggle* of x to X is a function f such that $f(X, \{x\}) = \begin{cases} X \cup \{x\}, & \text{if } x \notin X \\ X \setminus \{x\}, & \text{if } x \in X \end{cases}$. We use $\oplus$ to denote it.

Remark 7.16. Given an ordering $x_1, x_2, \ldots$ of elements in the ground set that X lives in, we can think of X as a binary string. If $x_i \in X$, then the ith index of the binary string is 1, otherwise it is 0. In such a scheme, $\oplus$ is essentially the *XOR* function, or coordinate-wise addition in $\mathbb{Z}_2$.

Proposition 7.17. *Let S be a finite set such that $|S| = n \geq 1$, let S_e denote subsets of S with cardinality even, and S_o denote subsets of S with cardinality odd. Then $|S_e| = |S_o|$.*

Proof. Fix an element of S and call it 1. We define an involution from S_e to S_o. Consider the following involution $f : S_e \to S_o$, with $f(X) = X \oplus \{1\}$, note that $f(f(X)) = f(X \oplus \{1\}) = X \oplus (\{1\} \oplus \{1\}) = X$, so f is indeed an involution. The same formula defines f on S_o, and f changes the size of a set by exactly 1, so it maps S_e into S_o and S_o into S_e.

Since f is an involution, f is also a bijection, therefore $|S_e| = |S_o|$. □

Example 7.18. Evaluate $\sum_{i=0}^{k} (-1)^i \binom{n}{i}$. We work on $[n]$, with $n \geq 1$. Let $S_i = \{T \subseteq [n] : |T| = i\}$, define $f : \bigcup_{i=0}^{k} S_i \setminus E \to \bigcup_{i=0}^{k} S_i \setminus E$ as $f(X) = X \oplus \{1\}$. What will be the exception here? Well, for all subsets with cardinality k that do not contain 1, we'll make them into a set with cardinality $k+1$, which is not contained in this summation. Thus, $|E| = \binom{n-1}{k}$. Moreover, notice for $X, f(X)$, their size differs by exactly 1, so they have opposite parity and therefore can be canceled out. Thus, we have

$$\sum_{i=0}^{k} (-1)^i \binom{n}{i} = (-1)^k \binom{n-1}{k}$$

Example 7.19. Evaluate $\sum_{i=0}^{n} \binom{n}{i} \binom{m+n-i}{k-i} (-1)^i$, for $n \leq k \leq m+n$.

- **Description:** $S_i = (X, Y)$, $X \subseteq [n], |X| = i, Y \subseteq [m+n] \setminus X, |Y| = k - i$.

- **Involution:** given (X, Y), toggle the smallest $x \in [n]$ that lies in exactly one of X and Y, if such x exists, then $f(X, Y) = (X \oplus \{x\}, Y \oplus \{x\})$. Notice this is an involution, and changes parity of $|X|$.
- **Exception:** if $X \neq \emptyset$, then we can always find such an x. However, if $X = \emptyset$ and $Y \subseteq [m+n] \setminus [n]$, then there is no element in X and Y that comes from $[n]$, we therefore cannot toggle. In such case, we have $i = 0$ and there are exactly $\binom{m}{k}$ such Y's.

Thus, we have

$$\sum_{i=0}^{n} \binom{n}{i} \binom{m+n-i}{k-i} (-1)^i = \binom{m}{k}$$

Example 7.20. Prove the identity $\sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = d_n$.

- **Description:** S_k = words of length $n-k$, without repeats, with $\Sigma = [n]$.
- **Involution:** Given a word ω, let x be the min element of {numbers missing from ω} $\cup$ {numbers in natural position}. If x is missing from ω, put it in its natural position, otherwise delete x.

  Example 7.21. We give an example for $n = 3$. The mappings are presented below.

  $$\emptyset - 1, 3 - 13, 31 - 321, 32 - 132, 2 - 12, 21 - 213, 23 - 123$$

  Notice $231, 312$ cannot be mapped.

- **Exception:** derangements of $[n]$.

Thus, we have

$$\sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = d_n$$

A more natural interpretation is let S_k denote words of length k instead of $n-k$, this still works, as long as a word of length k now gets the sign $(-1)^{n-k}$, since the following identity holds:

$$\sum_{i=0}^{n} \frac{(-1)^i}{i!} = \sum_{i=0}^{n} \frac{(-1)^{n-i}}{(n-i)!}$$

To see this, let $k = n - i$, so RHS can be written as

$$\sum_{n-k=0}^{n} \frac{(-1)^k}{k!} = \sum_{k=n}^{0} \frac{(-1)^k}{k!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Example 7.22. Recall the nth Fibonacci number F_n, a combinatorial interpretation of F_n is, it counts the number of boards of size $1 \times n$ consisting of 1×1 squares and 1×2 dominos. With this indexing, $F_0 = F_1 = 1$ (the empty board counts once) and $F_2 = 2$.

First, notice $F_n = 1 + \sum_{j=0}^{n-2} F_j$, we case on the position of the rightmost domino: if it covers cells $j+1$ and $j+2$, the cells to its right are squares and the first j cells form any of the F_j boards

of size $1 \times j$. There is exactly one board consisting of all squares, and all others are counted in the sum.

We try to evaluate $\sum_{j=1}^{n}(-1)^j F_j$. Define the involution to be toggling the leftmost tile of the board: if it's a square, replace it with a domino, and if it's a domino, replace it with a square. The exception is the board of $1 \times n$ with the leftmost tile being square, and there are exactly F_{n-1} such boards. Thus,

$$\sum_{j=1}^{n}(-1)^j F_j = (-1)^n F_{n-1}$$

8 Elementary Counting & Stirling Numbers

We start by counting functions.

- **Question:** How many functions from $[k]$ to $[n]$?
  Answer: n^k.
- **Question:** How many surjections from $[k]$ to $[n]$?
  Answer: As we have shown in Proposition 7.7, $\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^k$.
- **Question:** How many injections from $[k]$ to $[n]$?
  Answer: We need some definitions first.

  Definition 8.1. The *falling factorial* of the tuple (n,k) is defined as

  $$n(n-1)\cdots(n-k+1) = \begin{cases} \frac{n!}{(n-k)!}, & \text{if } k \le n \\ 0, & \text{otherwise} \end{cases}$$

  We use $(n)_k$ to denote it.

  Answer: $(n)_k$.

The following concern the number of integer solutions of an equation.

- **Question:** How many solutions in non-negative integers x_i to $x_1+x_2+\cdots+x_k=n$? More formally, what is $|\{\vec{x}\in\mathbb{N}^k : \sum_i \vec{x}_i = n\}|$?
  Answer: We claim it is $\binom{n+k-1}{k-1}$. Starting with $n+k-1$ "amorphous" objects, convert $k-1$ of them into "walls". Then we have n objects remaining, with k parts.
- **Question:** How about x_i's are positive?
  Answer: We claim it is $\binom{n-1}{k-1}$. This time we start with n objects, insert "walls" into gaps so that the n objects have k parts, there are $n-1$ gaps to insert.

Example 8.2. How many k-element subsets of $[n]$ with no two elements consecutive?

The key to this problem is, instead of counting elements that we have chosen, we count elements that remain unchosen. Fix $n-k$ triangles, we choose positions to insert squares so that no two squares are adjacent to each other. There are $n-k+1$ positions for us to choose, and we choose k, this yields

$$\binom{n-k+1}{k}$$

Definition 8.3. A *partition* of a set X into k parts is an equivalence relation on X with k-many classes.

The key aspect of partition is, parts themselves are not ordered.

Example 8.4. Let's list partitions of $\{a,b,c,d\}$ into 2 parts.

$$a|bcd, b|acd, c|abd, d|abc, ab|cd, ac|bd, ad|bc$$

There are 7 partitions in total.

Definition 8.5. Let $S(n,k) :=$ number of partitions of an n-element set into exactly k parts. $S(n,k)$ is called *Stirling number of the second kind*.

Some edge cases: $S(0,0) = 1$, $S(n,k) = 0$ if $k > n$.

Proposition 8.6. $S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$.

Proof. Partitions of X into k parts is essentially a surjection from X to $[k]$, without ordering. The total number of surjections from X to $[k]$, as in Proposition 7.7, is

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$$

Then we break all permutations of these k parts by dividing it by $k!$. □

Theorem 8.7. $S(n,k) = k \cdot S(n-1,k) + S(n-1,k-1)$.

Proof. Fix X of size n and some $x \in X$. The strategy will be "delete x and see what happens".

Case 1 x is related to some other elements. So given a partition of $X \setminus \{x\}$ into k parts, there are k possible ways we can put x back, into any of these parts. Hence, number of this case is $k \cdot S(n-1,k)$.

Case 2 x isn't related to anything else. We obtain a partition of $n-1$ elements into $k-1$ parts, number of this case is $S(n-1,k-1)$.

Sum over these two cases, we have

$$S(n,k) = k \cdot S(n-1,k) + S(n-1,k-1)$$

□

Definition 8.8. Consider the following two "bases" of polynomials:

- **Standard basis:** $x^0 = 1, x^1 = x, x^2 = x^2, \ldots$.
- **Stirling basis:** $(x)_0 = 1, (x)_1 = x, (x)_2 = x(x-1), (x)_3 = x(x-1)(x-2), \ldots$.

Theorem 8.9. *For any* $n \in \mathbb{N}$, $x^n = \sum_{k=0}^{n} S(n,k)(x)_k$.

Example 8.10. $x^3 = 1[x^3 - 3x^2 + 2x] + 3[x^2 - x] + 1[x] + 0[1]$, where $S(3,3) = 1, S(3,2) = 3, S(3,1) = 1, S(3,0) = 0$.

Proof. It suffices to show the equality $z^n = \sum_{k=0}^{n} S(n,k)(z)_k$ for all integers $z > 0$, since two polynomials that agree at infinitely many points are equal.

- LHS: counts functions from $[n]$ to $[z]$.
- We will show RHS counts the same thing.

  Given $f : [n] \to [z]$, put $k = |\operatorname{image}(f)|$, count functions with these k images. There are $\binom{z}{k}$ possible images. For each image, there are $k! \cdot S(n,k)$ functions that surject to it, so in total it's

  $$\binom{z}{k}k! \cdot S(n,k) = \frac{z!}{k!(z-k)!}k! \cdot S(n,k) = S(n,k)(z)_k$$

  Summing over k, we get the desired result.

□

Definition 8.11. $s(n,k)$, *Stirling number of the first kind*, is defined as the coefficient of x^k in $(x)_n = \sum_{k=0}^{n} s(n,k)x^k$.

Definition 8.12. $c(n,k)$, *unsigned Stirling number of the first kind*, is defined as $c(n,k) = |s(n,k)|$, it counts "elements of S_n with exactly k cycles".

Theorem 8.13. $\sum_{k=m}^{n} S(n,k)s(k,m) = \begin{cases} 1, & \text{if } m = n \\ 0, & \text{otherwise} \end{cases}$

The proof is left as an exercise to the reader.

9 Generating Functions & Formal Power Series

9.1 Generating functions: prelude

Suppose $(a_n)_{n\in\mathbb{N}}$ is some sequence of numbers.

Definition 9.1. The corresponding *ordinary generating function* is the expression $\sum_n a_n x^n$, where x is some variable symbol.

Definition 9.2. The corresponding *exponential generating function* is the expression $\sum_n \frac{a_n}{n!} x^n$.

We can think of them as "functions":

$$x \mapsto \sum_n a_n x^n, x \mapsto \sum_n \frac{a_n}{n!} x^n$$

Warm-up:

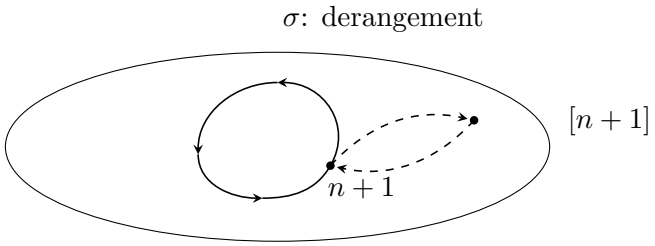
1. $a_n = 1$ for all n, then OGF $= \sum_n 1 \cdot x^n \approx \frac{1}{1-x}$, EGF $= \sum_n \frac{x^n}{n!} \approx e^x$.
2. $a_n = n$, OGF $= \sum_n n \cdot x^n$, we know $\sum_n x^n = \frac{1}{1-x}$, differentiate yields $\sum_n n \cdot x^{n-1} = \frac{1}{(1-x)^2} \Rightarrow$ $\sum_n n \cdot x^n = \frac{x}{(1-x)^2}$, EGF $= \sum_n n \cdot \frac{x^n}{n!} = \sum_{n\geq 1} \frac{x^n}{(n-1)!} = x \sum_{n\geq 1} \frac{x^{n-1}}{(n-1)!} = x \sum_n \frac{x^n}{n!} = xe^x$.

From OGF, f or EGF, g, we can "recover" a_n like so:

$$a_n = \frac{f^{(n)}(0)}{n!} = g^{(n)}(0)$$

Proposition 9.3. *$d_{n+1} = n(d_n + d_{n-1})$, for $n \geq 1$.*

Proof. We derive such recurrence by considering any fixed derangement, σ, on $[n+1]$.



By the definition of a derangement, we know that $\sigma(n+1) \neq n+1$, so there are n choices for $\sigma(n+1)$, let's say $\sigma(n+1) = j$. j either

- takes a while to cycle back;
- immediately cycle back.

Case 1 Assume $\sigma(n+1) = j, \sigma(k) = n+1, k \neq j$, we will obtain a derangement τ on $[n]$ from σ, by setting

$$\tau(l) = \begin{cases} \sigma(l), & \text{if } l \neq k \\ j, & \text{if } l = k \end{cases}$$

This is a bijection onto the derangements of $[n]$: from τ we recover $k = \tau^{-1}(j)$, and then σ.

Case 2 Delete both $n+1$ and j, this bijects σ to one specific derangement on $[n] \setminus \{j\}$.

Sum over two cases, we have

$$d_{n+1} = n(d_n + d_{n-1})$$

□

Consider EGF, $g(x) = \sum_n d_n \frac{x^n}{n!}$, $g'(x) = \sum_{n\geq 1} n \cdot d_n \frac{x^{n-1}}{n!} = \sum_n d_{n+1} \frac{x^n}{n!}$, and then

$$\begin{aligned}(1-x)g'(x) &= \sum_n d_{n+1}\frac{x^n}{n!} - \sum_n d_{n+1}\frac{x^{n+1}}{n!} \\ &= \sum_n n(d_n + d_{n-1})\frac{x^n}{n!} - \sum_n n \cdot d_n \frac{x^n}{n!} \\ &= \sum_{n\geq 1} d_{n-1}\frac{x^n}{(n-1)!} \\ &= xg(x)\end{aligned}$$

So $g'(x) = \frac{x}{1-x}g(x) \Rightarrow g(x) = \frac{e^{-x}}{1-x}$, using $g(0) = d_0 = 1$.

Recall Definition 8.5, $S(n,k)$ = number of partitions of $[n]$ into exactly k-many non-empty parts. We know that $S(n,k) = k \cdot S(n-1,k) + S(n-1,k-1)$. Consider EGFs, $g_k(x) = \sum_n S(n,k)\frac{x^n}{n!} = \sum_{n\geq k} S(n,k)\frac{x^n}{n!}$. Then

$$\begin{aligned}g_k'(x) &= \sum_n S(n+1,k)\frac{x^n}{n!} \\ &= \sum_n k \cdot S(n,k)\frac{x^n}{n!} + \sum_n S(n,k-1)\frac{x^n}{n!} \\ &= k \cdot g_k(x) + g_{k-1}(x)\end{aligned}$$

Proposition 9.4. $g_k(x) = \frac{1}{k!}(e^x - 1)^k$.

Proof. Induct on k.

Base case: $k = 0$, $S(0,0) = 1, S(n,0) = 0$, for $n > 0$. $g_0(x) = 1 = \frac{1}{0!}(e^x-1)^0 = 1$.
$k = 1$, $S(0,1) = 0, S(n,1) = 1$, for $n > 0$. $g_1(x) = \sum_{n\geq 1} \frac{x^n}{n!} = e^x - 1 = \frac{1}{1!}(e^x-1)^1$.

Inductive step: $g_k'(x) = k \cdot g_k(x) + g_{k-1}(x) = k \cdot g_k(x) + \frac{1}{(k-1)!}(e^x-1)^{k-1}$, solve the differential equation yields the result. Notice $h(x) = \frac{1}{k!}(e^x-1)^k$ also solves it, since $h'(x) = \frac{1}{(k-1)!}(e^x - 1)^{k-1}((e^x-1)+1) = k \cdot h(x) + \frac{1}{(k-1)!}(e^x-1)^{k-1}$, and $h(0) = 0 = S(0,k) = g_k(0)$. A power series solution $\sum_n c_n x^n$ is determined by c_0, since comparing coefficients of x^n gives c_{n+1} from c_n, thus $g_k = h$. □

9.2 Formal power series

Definition 9.5. Let $\mathbb{C}[[x]]$ denote the ring of formal power series in x with complex coefficients. Given any sequence $(a_n)_{n\in\mathbb{N}}$ of complex numbers, we get a power series $f(x) = \sum_n a_n x^n \in \mathbb{C}[[x]]$, with some basic operations:

- **Addition:** If $f(x) = \sum_n a_n x^n, g(x) = \sum_n b_n x^n$, then $(f+g)(x) = f(x) + g(x) = \sum_n (a_n + b_n)x^n$.
- **Multiplication:** $(f \cdot g)(x) = f(x)g(x) = \sum_n c_n x^n$, where $c_n = \sum_{i\le n} a_i b_{n-i}$.

Throughout the section, we'll use $f(x)$ to denote $\sum_n a_n x^n$ and $g(x)$ to denote $\sum_n b_n x^n$ for some sequences $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$.

Proposition 9.6. $\frac{1}{1-x} = \sum_n x^n$.

Proof. We want to show $(1-x)\sum_n x^n = 1$, where $f(x) = 1-x$, with $a_0 = 1, a_1 = -1$ and all other $a_i = 0$. Let $g(x) = \sum_n x^n$, consider the coefficients of $f(x)g(x)$:

$$c_0 = a_0b_0 = 1, c_1 = a_0b_1 + a_1b_0 = 0, c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 1 - 1 + 0 = 0, \ldots, c_n = 0$$

The reason why all subsequent c_i's are 0 is, the only non-zero parts that contribute to c_i is $a_0b_i + a_1b_{i-1}$, and this is exactly $1 - 1 = 0$. Thus, $\sum_n c_n x^n = 1$, as desired. □

More generally, if $f(x)$ has $a_0 \neq 0$, then it has a multiplicative inverse in $\mathbb{C}[[x]]$. To find such an inverse, we can "back-solve" for b_n using $c_0 = 1, \ldots, c_n = 0$.

Definition 9.7. *Derivative:* Given $f(x)$, define $f'(x) = \sum_{n\ge 1} n a_n x^{n-1} = \sum_n (n+1)a_{n+1}x^n$.

Example 9.8. If $f(x) = \sum_n \frac{x^n}{n!}$, then $f'(x) = \sum_n (n+1)\frac{x^n}{(n+1)!} = \sum_n \frac{x^n}{n!} = f(x)$, we denote $f(x)$ by e^x.

Proposition 9.9. *Some rules of calculus:*

1. $(f+g)' = f' + g'$
2. $(f \cdot g)' = f' \cdot g + f \cdot g'$
3. $(f^k)' = k \cdot f^{k-1} \cdot f'$

Proof of rule 2. Let $f(x), g(x)$ be two formal power series. By Definition 9.7, we have $f'(x) = \sum_n (n+1)a_{n+1}x^n$, $g'(x) = \sum_n (n+1)b_{n+1}x^n$, $(f \cdot g)(x) = \sum_n c_n x^n$, where $c_n = \sum_{i\le n} a_i b_{n-i}$. We know that $(f \cdot g)' = \sum_n (n+1)c_{n+1}x^n$, we wish to show that $f' \cdot g + f \cdot g'$ also equals the RHS.

$$(f' \cdot g)(x) = \sum_n \Big(\sum_{i\le n} (i+1)a_{i+1}b_{n-i} \Big) x^n$$

$$(f \cdot g')(x) = \sum_n \Big(\sum_{i\le n} a_i(n+1-i)b_{n+1-i} \Big) x^n$$

$$\Rightarrow \sum_{1\le i\le n+1} i a_i b_{n+1-i} + \sum_{0\le i\le n} a_i(n+1-i)b_{n+1-i} = (n+1)\sum_i a_i b_{n+1-i} = (n+1)c_{n+1}$$

□

Definition 9.10. *Composition:* Given $f(x), g(x)$ with $b_0 = 0$, then $(f \circ g)(x) = f(g(x))$ is defined by $\sum_n a_n (g(x))^n$.

Consider $g(x) = 1 + x$, then $(g(x))^n = (1+x)^n = 1 + \text{stuff}$, then $f \circ g = \sum_n a_n (g(x))^n = (\sum_n a_n \cdot 1) + \text{stuff}$, where the first part has already evaluated to some infinite sum, which is bad. On the other hand, if $b_0 = 0$, then for each n, the least non-zero coefficient of $(g(x))^n$ is at least at position n, for example, $(x + x^2 + \cdots)^k = x^k + \text{stuff}$.

Definition 9.11. *Chain rule:* Let $f(x), g(x)$ be formal power series with $b_0 = 0$, then $(f \circ g)' = (f' \circ g) \cdot g'$.

Example 9.12. Consider $g(x) = \sum_{n \geq 1} (-1)^{n+1} \frac{x^n}{n} = \log(1+x)$, note $g'(x) = \sum_n (-1)^n x^n = \frac{1}{1+x}$.

Then $\log e^x = \log(1 + (e^x - 1))$, the derivative of that is $\frac{1}{1+(e^x-1)} \cdot e^x = 1$, hence $\log e^x = c_0 + x$, where $c_0 = 0$, since $e^x - 1$ has constant term 0.

Example 9.13. Fix k, how many solutions to $\sum_{i=1}^k x_i = n$ in non-negative integers?
The answer is $\binom{n+k-1}{k-1} = a_n$.

We do it instead using formal power series. Let's consider the product

$$\underbrace{(1 + x + x^2 + \cdots)(1 + x + x^2 + \cdots)\cdots}_{k \text{ times}}$$

as $\sum_n a_n x^n$. The coefficient of x^n is exactly the number of ways to choose from these k parts. To see this, notice $1 = x^0$, so $x^n = x^a x^b \cdots = x^{a+b+\cdots}$, exactly k parts with each part non-negative integers. Thus a_n counts exactly the number of ways to choose non-negative integer solutions to above equation. We therefore have

$$f(x) = \underbrace{(1 + x + x^2 + \cdots)(1 + x + x^2 + \cdots)\cdots}_{k \text{ times}} = \left(\frac{1}{1-x}\right)^k = \sum_n \binom{n+k-1}{n} x^n$$

9.3 Finite calculus

Topics we cover in this section:

- Taylor series
- Power series
- Partial fractions
- Generating functions

Definition 9.14. Let f be a function which is infinitely differentiable at 0, then we write $f(x) = f(0) + f'(0)x + \frac{f''(0)}{2}x^2 + \cdots = \sum_n \frac{f^{(n)}(0)}{n!}x^n$ as the *Taylor series of f about* 0.

Example 9.15. *Geometric series:*

$$f(x) = (1-x)^{-1}, f(0) = 1, f'(x) = -(1-x)^{-2}\cdot(-1) = (1-x)^{-2}, f'(0) = 1,$$
$$f''(x) = -2(1-x)^{-3}\cdot(-1) = 2(1-x)^{-3}, f''(0) = 2, \ldots$$
$$\Rightarrow \frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_n x^n$$

Example 9.16. *Exponential:*
$f(x) = e^x$, notice $f'(x) = e^x$, so

$$f^{(n)}(0) = e^0 = 1 \Rightarrow f(x) = e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_n \frac{x^n}{n!}$$

Manipulating power series:

- Addition: $\sum_n a_n x^n + \sum_n b_n x^n = \sum_n (a_n + b_n)x^n$

  Example 9.17. Consider the following:

$$\begin{aligned}
\frac{1+x}{1-2x} &= (1+x)\frac{1}{1-\underbrace{2x}_{y}} \\
&= (1+x)\frac{1}{1-y} \\
&= (1+x)\sum_n y^n \\
&= (1+x)\sum_n (2x)^n \\
&= \sum_n (2x)^n + \sum_n 2^n x^{n+1} \\
&= (1 + 2x + 4x^2 + \cdots) + (x + 2x^2 + 4x^3 + \cdots) \\
&= 1 + 3x + 6x^2 + \cdots \\
&= 1 + \sum_{n\geq 1} 2^n x^n + \sum_{n\geq 1} 2^{n-1} x^n \\
&= 1 + \sum_{n\geq 1} (2^n + 2^{n-1})x^n
\end{aligned}$$

- Multiplication: $(f \cdot g)(x) = \sum_n c_n x^n$, where $c_n = \sum_{i \le n} a_i b_{n-i}$

  Example 9.18. Recall Proposition 7.5, d_n:

  $$\frac{e^{-x}}{1-x} = (1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \cdots)(1 + x + x^2 + \cdots)$$

  So $\frac{d_n}{n!}$ as a coefficient is exactly $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

- Differentiation.

  Example 9.19. We consider the family of $((1-x)^k)_{k \in \mathbb{Z}^{<0}}$.

  $$\begin{aligned}
  \frac{1}{1-x} &= 1 + x + x^2 + x^3 + \cdots \\
  \frac{d\frac{1}{1-x}}{dx} &= (1-x)^{-2} = 0 + 1 + 2x + 3x^2 + 4x^3 + \cdots \\
  &= \sum_n (n+1)x^n \\
  \frac{d\frac{1}{(1-x)^2}}{dx} &= 2(1-x)^{-3} = 2 + 6x + 12x^2 + \cdots \\
  &\Rightarrow (1-x)^{-3} = 1 + 3x + 6x^2 + \cdots = \sum_n \binom{n+2}{n} x^n
  \end{aligned}$$

  In general, $\frac{1}{(1-x)^k} = \sum_n \binom{n+k-1}{n} x^n$.

- Integration.

  Example 9.20. Consider $\frac{1}{1+x}$. We know that $\frac{1}{1-x} = 1 + x + x^2 + \cdots$, so $\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots$. Integration of $\frac{1}{1+x}$ is $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$, so $\log 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$

- Partial fraction.

  Example 9.21. It is easy to evaluate $\frac{1}{x+3} + \frac{1}{x+2}$:

  $$\frac{1}{x+3} + \frac{1}{x+2} = \frac{2x+5}{(x+2)(x+3)} = \frac{2x+5}{x^2+5x+6}$$

  However, it is hard to decompose a fraction into partial fractions. Consider decomposing the following.

  $$\frac{x-7}{x^2-9x+20} = \frac{x-7}{(x-4)(x-5)} = \frac{A}{x-4} + \frac{B}{x-5}$$

  We then have

  $$A(x-5) + B(x-4) = x - 7 \Rightarrow A = 3, B = -2$$

Example 9.22. Decompose the following:

$$\frac{x}{x^4-1}$$

$$\begin{aligned}\frac{x}{x^4-1} &= \frac{x}{(x^2+1)(x+1)(x-1)}\\ &= \frac{A}{x-1}+\frac{B}{x+1}+\frac{Cx+D}{x^2+1}\\ &\Rightarrow x = A(x+1)(x^2+1)+B(x-1)(x^2+1)+(Cx+D)(x^2-1)\end{aligned}$$

Plug in $x=1$, we have $1=4A, A=\frac{1}{4}$;
Plug in $x=-1$, we have $-1=-4B, B=\frac{1}{4}$.
$\Rightarrow x=\frac{x}{2}(x^2+1)+(Cx+D)(x^2-1)$
Plug in $x=i$, we have $i=-2(Ci+D)$;
Plug in $x=-i$, we have $-i=-2(-Ci+D)$.
$\Rightarrow C=-\frac{1}{2}, D=0$
$\Rightarrow \frac{x}{x^4-1}=\frac{1/4}{x-1}+\frac{1/4}{x+1}+\frac{-x/2}{x^2+1}$

General procedure of using generating functions to solve recurrences:

Step 1 We have some sequence $(a_n)_{n\in\mathbb{N}}$, we want to find a closed-form expression for a_n.

Step 2 Express it in generating function $f(x)=\sum_n a_n x^n$ or $g(x)=\sum_n a_n \frac{x^n}{n!}$.

Step 3 Solve for $f(x)$.

Step 4 Find an explicit form for a_n.

Example 9.23. Solve for $(a_n)_{n\in\mathbb{N}}$, where $a_0=1, a_1=2, a_n=3a_{n-1}+4a_{n-2}$, for $n\geq 2$.
Define $f(x)=\sum_n a_n x^n$, then

$$\begin{aligned}a_n x^n &= 3a_{n-1}x^n + 4a_{n-2}x^n\\ \sum_{n\geq 2} a_n x^n &= 3\sum_{n\geq 1} a_n x^{n+1} + 4\sum_{n\geq 0} a_n x^{n+2}\\ \Rightarrow f(x)-1-2x &= 3x(f(x)-1)+4x^2 f(x)\\ 4x^2 f(x)+3xf(x)-f(x)-x+1 &= 0\\ f(x) &= \frac{x-1}{4x^2+3x-1}\\ &= \frac{x-1}{(4x-1)(x+1)}\\ &= \frac{A}{4x-1}+\frac{B}{x+1}\\ A(x+1)+B(4x-1) &= x-1\\ &\Rightarrow \begin{cases}A=-0.6\\ B=0.4\end{cases}\end{aligned}$$

So we have

$$f(x) = \frac{-0.6}{4x-1} + \frac{0.4}{x+1}$$

where $\frac{0.6}{1-4x} = 0.6\frac{1}{1-4x} = 0.6\sum_n 4^n x^n$, $\frac{0.4}{1+x} = 0.4\frac{1}{1+x} = 0.4\sum_n (-1)^n x^n$, so $f(x) = \sum_n [0.6 \cdot 4^n + 0.4 \cdot (-1)^n]x^n$, and indeed, we have

$$a_n = 0.6 \cdot 4^n + 0.4 \cdot (-1)^n$$

9.4 Solving recurrences using generating functions

Recall from last time, we have

$$\left(\frac{1}{1-x}\right)^k = \sum_n \binom{n+k-1}{n} x^n$$

The following is a generalization of Theorem 7.14.

Theorem 9.24 (General binomial)**.** *Suppose $q \in \mathbb{Q}$, then*

$$(1+x)^q = \sum_n \frac{(q)_n}{n!} x^n = \sum_n \frac{q(q-1)\cdots(q-n+1)}{n!} x^n$$

Example 9.25. If $q \in \mathbb{N}$, then $\frac{(q)_n}{n!} = \binom{q}{n}$, we get the usual binomial theorem.

Example 9.26. If $q = -1$, then

$$\begin{aligned}(1+x)^{-1} &= \sum_n \frac{(-1)(-2)\cdots(-n)}{n!} x^n \\ &= \sum_n (-1)^n x^n \\ &= \sum_n (-x)^n \\ &= \frac{1}{1-(-x)} \\ &= \frac{1}{1+x}\end{aligned}$$

Example 9.27. $q = -k$ for $k \in \mathbb{N}$, then

$$\begin{aligned}(1+x)^{-k} &= \sum_n \frac{(-k)(-k-1)\cdots(-k-n+1)}{n!} x^n \\ &= \sum_n (-1)^n \frac{(k+n-1)(k+n-2)\cdots k}{n!} x^n \\ &= \sum_n (-1)^n \binom{n+k-1}{n} x^n\end{aligned}$$

Example 9.28. $q = \frac{1}{2}$, so

$$\begin{aligned}(1+x)^{\frac{1}{2}} &= \sum_n \frac{1/2(-1/2)(-3/2)\cdots(1/2-n+1)}{n!}x^n \\ &= \sum_n \frac{1(1-2)(1-4)\cdots(1-2n+2)}{2^n n!}x^n \\ &= 1 + \sum_{n\geq 1}(-1)^{n-1}\frac{(2n-3)(2n-5)\cdots 1}{2^n n!}x^n \\ &= 1 + \sum_{n\geq 1}(-1)^{n-1}\frac{(2n-2)!}{(2^{n-1}(n-1)!)2^n n!}x^n \\ &= 1 + \sum_{n\geq 1}\frac{(-1)^{n-1}}{2^{2n-1}n}\binom{2n-2}{n-1}x^n\end{aligned}$$

The proof of Theorem 9.24 is left as an exercise to the reader. We highlight two important steps in showing the validity of Theorem 9.24:

Step 1 Base case: $(1+x)^1 = \ldots$

Step 2 Closure: $(1+x)^q(1+x)^r = (1+x)^{q+r}$

Example 9.29. Consider words in 3 letters with $\Sigma = \{A, B, C\}$, with no two consecutive BC or CB. How many such words of length n? Call it a_n.

Let's start with small n.

- $a_0 = 1$, the empty word.
- $a_1 = 3$, we have A, B, C.
- $a_2 = 7$, we have $AA, AB, AC, BB, BA, CA, CC$.

Proposition 9.30. *For $n \geq 2$, $a_n = 2a_{n-1} + a_{n-2}$.*

Proof. Take cases on how words of length n start:

$$A, BA, BB, CA, CC$$

Notice there are a_{n-1} words starting with A, since this puts no constraints on subsequent letters. Group words starting with BA, BB, CC, there are a_{n-1} words of this group, since if we omit the first letter, they start with A, B, C, so they cover all words with length $n-1$. There are a_{n-2} words starting with CA, since again starting with A puts no constraints. □

Now consider OGF, $f(x) = \sum_n a_n x^n$, so

$$\begin{aligned}
(1-2x-x^2)f(x) &= 1 + x + \sum_{n\geq 2}(a_n - 2a_{n-1} - a_{n-2})x^n \\
&= 1 + x \\
f(x) &= \frac{1+x}{1-2x-x^2} \\
1-2x-x^2 &= (1-\alpha x)(1-\beta x) && \text{where } \alpha = 1+\sqrt{2}, \beta = 1-\sqrt{2} \\
f(x) &= \frac{\frac{1}{2}\alpha}{1-\alpha x} + \frac{\frac{1}{2}\beta}{1-\beta x} \\
&= \sum_n \frac{1}{2}(\alpha^{n+1} + \beta^{n+1})x^n
\end{aligned}$$

Thus, there are exactly $a_n = \frac{1}{2}(\alpha^{n+1} + \beta^{n+1})$ valid words of length n.

Some tricks: in general, when having recurrence like $a_n = 4a_{n-1} + 6a_{n-2} - 7a_{n-3}$, do something like $(1 - 4x - 6x^2 + 7x^3)f(x) =$ some polynomial.

Definition 9.31. Given a list of n objects (in order) and some binary operation, the *Catalan number* counts the number of ways to associate the product or add "parentheses". We use μ_n to denote it.

Some values of μ_n with small n:

$$\mu_0 = 1, \mu_1 = 1, \mu_2 = 1, \mu_3 = 2, \mu_4 = 5$$

Observe that $\mu_n = \sum_{m=1}^{n-1} \mu_m \mu_{n-m}$ for $n \geq 2$, the way to reason about it is we can choose a position m to add parentheses from 1 to m, and from $m+1$ to n.

Recall: $c_n = \sum_{i \leq n} a_i b_{n-i}$.

Define $a_n = \begin{cases} \mu_n, & \text{if } n > 0 \\ 0, & \text{if } n = 0 \end{cases}$

Consider OGF, $f(x) = \sum_n a_n x^n$.

Proposition 9.32. $f(x)^2 = f(x) - x$.

Proof.

$$\begin{aligned}
f(x)^2 &= \sum_n \Big(\sum_{m=0}^{n} a_m a_{n-m} \Big) x^n \\
&= \sum_{n \geq 2} a_n x^n && \text{by recurrence of } \mu_n \\
&= f(x) - x
\end{aligned}$$

Notice the terms $m = 0$ and $m = n$ vanish since $a_0 = 0$, so the coefficients of x^0 and x^1 are 0. The last step uses $a_0 = 0$ and $a_1 = \mu_1 = 1$. □

So we have $f^2 = f - x$, solve for f, we have

$$f = \frac{1 \pm \sqrt{1-4x}}{2}$$

since $f(0) = 0$, $f = \frac{1-\sqrt{1-4x}}{2}$.

The power series $(1-4x)^{\frac{1}{2}} = (1+(-4x))^{\frac{1}{2}}$, using Example 9.28, we have

$$(1+(-4x))^{\frac{1}{2}} = 1 + \sum_{n\geq 1}(-1)^{n-1}\frac{1}{2^{2n-1}n}\binom{2n-2}{n-1}(-4x)^n = 1 - \sum_{n\geq 1}\frac{2}{n}\binom{2n-2}{n-1}x^n$$

Finally, we have

$$\mu_n = \begin{cases} \frac{1}{n}\binom{2n-2}{n-1}, & \text{if } n > 0 \\ 1, & \text{if } n = 0 \end{cases}$$

We remind reader of the 4 basic steps of using generating functions to solve recurrences:

Step 1 Find some recurrence relation for a_n.

Step 2 Deduce a functional equation for OGF or EGF.

Step 3 Solve for OGF/EGF.

Step 4 Glean information about $(a_n)_{n\in\mathbb{N}}$.

Example 9.33. Recall that an *involution* on a set X is a function $i : X \to X$ such that for all $x \in X$, $i^2(x) = x$.

Let a_n = number of involutions of an n-element set, so $a_0 = 1, a_1 = 1, a_2 = 2, a_3 = 4$.

Proposition 9.34. *For $n \geq 2$, $a_n = a_{n-1} + (n-1)a_{n-2}$.*

Proof. Without loss of generality, let $X = [n]$, consider arbitrary involution $i : X \to X$, examine $i(1)$.

Case 1 $i(1) = 1$, there are a_{n-1} of such involutions.

Case 2 $i(1) \neq 1$, first note there are $n-1$ choices for $i(1)$, for each choice, there are a_{n-2} of such involutions, so in total, it's $(n-1)a_{n-2}$.

□

To solve it, we first try OGF, $f(x) = \sum_n a_n x^n$,

$$\begin{aligned} f'(x) &= \sum_n (n+1)a_{n+1}x^n \\ &= \sum_n (n+2)a_{n+1}x^n - \sum_n a_{n+1}x^n \\ &= \sum_n (a_{n+3} - a_{n+2})x^n - \sum_n a_{n+1}x^n \end{aligned}$$

This seems extremely hard to solve, so we instead try EGF, $f(x) = \sum_n a_n \frac{x^n}{n!}$.

$$\begin{aligned}
f'(x) &= \sum_n a_{n+1} \frac{x^n}{n!} \\
&= \sum_n \frac{a_n + n a_{n-1}}{n!} x^n \\
&= \sum_n \frac{a_n}{n!} x^n + \sum_n \frac{n a_{n-1}}{n!} x^n \\
&= f(x) + \sum_{n \geq 1} \frac{a_{n-1}}{(n-1)!} x^n \\
&= f(x) + x f(x) \\
&= (1+x) f(x)
\end{aligned}$$

Try $f(x) = e^{g(x)}$, then $f'(x) = g'(x) e^{g(x)} = g'(x) f(x)$, so $g'(x) = 1 + x$, $g(x) = x + \frac{x^2}{2} + c$, then $f(x) = e^{\frac{x^2}{2} + x + c}$ with $f(0) = 1$, so $c = 0 \Rightarrow f(x) = e^{\frac{x^2}{2} + x}$.

Last step: find closed-form for a_n.

$$\begin{aligned}
f(x) &= \sum_n a_n \frac{x^n}{n!} \\
&= e^{\frac{x^2}{2} + x} \\
&= e^{\frac{x^2}{2}} \cdot e^x \\
&= \Big(\sum_n \frac{1}{n!} \Big(\frac{x^2}{2} \Big)^n \Big) \cdot \Big(\sum_n \frac{x^n}{n!} \Big) \\
&= \Big(\sum_n \frac{x^{2n}}{2^n n!} \Big) \cdot \Big(\sum_n \frac{x^n}{n!} \Big)
\end{aligned}$$

So comparing coefficients of x^n:

$$\frac{a_n}{n!} = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{2^k k! (n-2k)!}$$

Finally,

$$a_n = n! \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{2^k k! (n-2k)!}$$

The value of a_n hints at a purely combinatorial interpretation of this result:

An involution has (even-sized) *support*, where $\operatorname{spt}(i) = \{x \in X : i(x) \neq x\}$. We count involutions with $|\operatorname{spt}(i)| = 2k$:

- choose the support: $\binom{n}{2k} = \frac{n!}{(2k)!(n-2k)!}$.
- choose i(least thing in the support), there are $2k - 1$ choices, then i(least remaining thing) has $2k - 3$ choices, so on and so forth.

So the number of involutions with support of size $2k$ is

$$\begin{aligned}\frac{n!}{(n-2k)!(2k)!}(2k-1)(2k-3)\cdots 3\cdot 1 &= \frac{n!}{(2k)(2k-2)\cdots 4\cdot 2(n-2k)!}\\ &= \frac{n!}{2^k k!(n-2k)!}\end{aligned}$$

Sum over k, we get the desired result.

10 Partitions

10.1 Fundamental questions & basic definitions

We first ask the fundamental questions with regard to partitions: how many ways are there to chop an n-element set X up into k-many pieces?

To answer, we first need to classify with respect to elements and parts.

1. Elements of X are distinguishable & parts are distinguishable.

   Example 10.1. $n = 4, k = 2$. We consider putting elements into left part:

   - Put 1 element, there are 4 ways;
   - Put 2 elements, $\binom{4}{2}$ ways;
   - Put 3 elements, $\binom{4}{3}$ ways.

   In total, there are $4 + \binom{4}{2} + \binom{4}{3} = 14$ ways.

   Notice this is exactly the same as counting surjections from $[n]$ to $[k]$. So the answer is

   $$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

2. Elements are distinguishable & parts are not.

   Example 10.2. $n = 4, k = 2$. Again, we put elements into left part:

   - Put 1 or 3 elements, there are 4 ways;
   - Put 2 elements, there are $\binom{4}{2}/2 = 3$ ways.

   In total, there are 7 ways.

   In this case, we get Definition 8.5, Stirling number of the second kind, $S(n, k)$, so the answer is

   $$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} (k-i)^n (-1)^i$$

   Also, EGF,

   $$f(x) = \sum_{n} \frac{1}{n!} S(n,k) x^n = \frac{1}{k!} (e^x - 1)^k$$

3. Elements are not distinguishable & parts are distinguishable.

   Example 10.3. $n = 4, k = 2$, we visualize it in a table:

L	○ ○ ○	○ ○	○
R	○	○ ○ ○	○ ○ ○

   In total, there are 3 such ways.

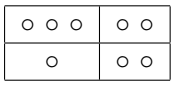
For each $i \leq k$, let $x_i :=$ number of elements in part i, we have the requirement that $\sum_{i=1}^{k} x_i = n$, so we are really counting solutions in positive integers to $\sum_{i=1}^{k} x_i = n$. The answer is

$$\binom{n-1}{k-1}$$

As we have n objects, then insert $k-1$ "walls" in $n-1$ gaps, so they form k parts.

4. Both elements and parts are not distinguishable. Surprisingly, this is the **hard** case.

   Example 10.4. $n = 4, k = 2$.

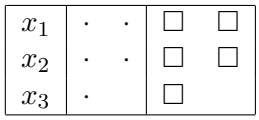
   

   There are only 2 ways.

   We denote this number by $p_k(n)$, it is the same as counting positive integer solutions to $\sum_{i=1}^{k} x_i = n$ with $x_1 \geq x_2 \geq \cdots \geq x_k$.

   A useful way of visualizing such partitions is via *Ferrers diagrams* or *Young tableaux*.

   Example 10.5. 3 parts with $2 + 2 + 1 = 5$.

   The dot figure is a Ferrers diagram, while the square one is a Young tableau.

Some computations for small k:

$$p_0(n) = \begin{cases} 1, & \text{if } n = 0 \\ 0, & \text{if } n \neq 0 \end{cases}$$

$$p_1(n) = \begin{cases} 0, & \text{if } n = 0 \\ 1, & \text{if } n \neq 0 \end{cases}$$

Proposition 10.6. $p_2(n) = \lfloor \frac{n}{2} \rfloor$.

Proof. We split into two parts. In the first part, we can put $n-1, n-2, \ldots, n - \lfloor \frac{n}{2} \rfloor$, till here, the first part still has at least as many objects as the second part, and one more step would make it smaller. Thus, there are $\lfloor \frac{n}{2} \rfloor$ ways in total. □

Proposition 10.7. *The OGF for* $p_3(n)$ *is* $\sum_n p_3(n)x^n = \frac{x^3}{(1-x)(1-x^2)(1-x^3)}$.

Proof. We will use a big trick in many proofs: instead of examining the rows, examine the columns. Consider a Ferrers diagram for $p_3(n)$:

x_1	○	○	○	○	○	○
x_2	○	○	○	○		
x_3	○	○	○			

We denote the number of columns with height 3 by y_3, with height 2 by y_2, and with height 1 by y_1. So counting positive integer solutions of $x_1 + x_2 + x_3 = n$ with $x_1 \geq x_2 \geq x_3$ is the **same** as counting non-negative integer solutions to $y_1 + 2y_2 + 3y_3 = n$, with $y_3 \neq 0$.

The OGF is thus

$$\underbrace{(1 + x + x^2 + \cdots)}_{y_1}\underbrace{(1 + x^2 + x^4 + \cdots)}_{y_2}\underbrace{(x^3 + x^6 + \cdots)}_{y_3} = \frac{1}{1-x}\frac{1}{(1-x^2)}\frac{x^3}{(1-x^3)}$$

□

Do partial fractions on $f(x) = \sum_n p_3(n)x^n$, we get

$$f(x) = x^3\left(\frac{1}{6(1-x)^3} + \frac{1}{4(1-x)^2} + \frac{17}{72(1-x)} + \frac{1}{8(1+x)} + \frac{1}{9(1-\omega x)} + \frac{1}{9(1-\bar{\omega}x)}\right)$$

where $\omega^3 = 1$ and $\omega \neq 1$. We can then estimate that $|p_3(n) - \frac{n^2}{12}| < \frac{1}{2}$.

Proposition 10.8. *For $k \leq n$, we have*

$$\frac{1}{k!}\binom{n-1}{k-1} \leq p_k(n) \leq \frac{1}{k!}\binom{n + \binom{k}{2} - 1}{k-1}$$

Proof. We prove two inequalities by establishing a surjection and an injection.

(left $\leq$): we map solutions to $x_1 + \cdots + x_k = n$ in positive integers to solutions of $y_1 + \cdots + y_k = n$ with $y_1 \geq \cdots \geq y_k \geq 1$, by putting x_i in order.

Example 10.9. Consider $n = 4, k = 2$.

- x_i scheme: $3 + 1, 2 + 2, 1 + 3$
- y_i scheme: $3 + 1, 2 + 2$.

Map $3 + 1, 1 + 3$ to $3 + 1$, $2 + 2$ to $2 + 2$.

This map is

- surjective, since the solution to y_i's is a subset of solution to x_i's.
- at most $k!$-to-one, since the x_i's mapped to a solution $\vec{y}$ are rearrangements of $\vec{y}$, and there are at most $k!$ of them, with exactly $k!$ when all y_i's are distinct.

Thus, we have $k! \cdot p_k(n) \geq \binom{n-1}{k-1}$.

(right $\leq$): we proceed in two steps.

Step 1 Inject $p_k(n)$ to $A = \{\text{partitions of } n + \binom{k}{2} \text{ into } k \text{ different-sized parts}\}$. Notice $|A| \leq p_k(n + \binom{k}{2})$.

Step 2 Bound $|A| \leq \frac{1}{k!}\binom{n + \binom{k}{2} - 1}{k-1}$.

Step 1 Given $x_1 + \cdots + x_k = n$ where $x_1 \geq \cdots \geq x_k \geq 1$, we wish to map it to $y_1 + \cdots + y_k = n + \binom{k}{2}$ with $y_i > y_{i+1}$. Formally, we map x_i to y_i, with $y_i = x_i + (k - i)$. Since $x_i \geq x_{i+1}$, $x_i - i \geq x_{i+1} - i > x_{i+1} - (i + 1)$, therefore the map is valid. Moreover, notice $1+2+\cdots+(k-1) = \frac{((k-1)+1)(k-1)}{2} = \binom{k}{2}$, so we have established the mapping with desired property.

Step 2 Notice y_i's are all distinct, so for each $\vec{y} \in A$, the $k!$-many permutations of $\vec{y}$ are also all distinct, and different $\vec{y}$'s give different permutations, all of which are positive integer solutions to $y_1 + \cdots + y_k = n + \binom{k}{2}$, so we have $k! \cdot |A| \leq \binom{n+\binom{k}{2}-1}{k-1}$.

Combine these two cases, we have

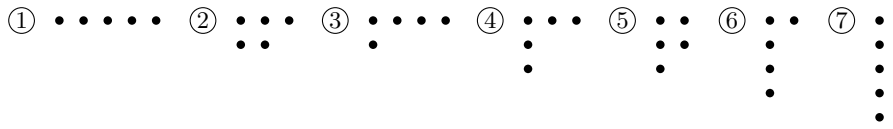
$$\frac{1}{k!}\binom{n-1}{k-1} \leq p_k(n) \leq |A| \leq \frac{1}{k!}\binom{n+\binom{k}{2}-1}{k-1}$$
$$\Rightarrow \frac{1}{k!}\binom{n-1}{k-1} \leq p_k(n) \leq \frac{1}{k!}\binom{n+\binom{k}{2}-1}{k-1}$$

As desired. □

10.2 The partition function & Euler's formulae

Definition 10.10. Define $p(n) :=$ number of unordered partitions of n into non-empty parts, so $p(n) = \sum_{k \le n} p_k(n) = p_n(2n)$.

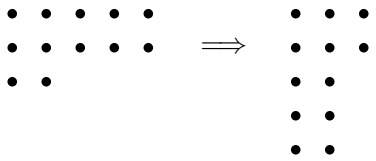
Example 10.11. $p(5) = 7$.



Remark 10.12. We give a sketch of proof of the above equality. The first equality is by definition, for the second one we can think of Ferrers diagram of $p_n(2n)$, it has n rows and total $2n$ dots. Fix a diagram and remove the first column, we now have n dots with potentially fewer than n rows, since some of the rows might be empty. This establishes a one-to-one mapping with $p(n)$, since for different diagrams of $p_n(2n)$, at least one row has different number of dots, so after removing the first column, the resulting two diagrams still differ in that row. The mapping is also onto: a partition of n has at most n parts, so we can pad it with empty rows to n rows and add back a first column of height n.

Definition 10.13. Given an unordered partition on n, its *conjugate partition* is what you get by flipping the Ferrers diagram.

Example 10.14. Consider $12 = 5 + 5 + 2$.



This results in $12 = 3 + 3 + 2 + 2 + 2$.

Example 10.15. Partitions of n into k-many parts, $p_k(n)$, have the Ferrers diagram of k rows, i.e., the first column has height k. Its conjugate then has the first row consisting of k dots. This establishes a bijection between partitions of n into k-many parts and partitions of n with largest part of size k.

Theorem 10.16 (Euler's partition formula)**.** *The OGF of $p(n)$ is*

$$p(x) = \sum_n p(n)x^n = \prod_{k=1}^{\infty} (1 - x^k)^{-1}$$

Proof. Expand RHS, we have

$$\underbrace{(1 + x + x^2 + \cdots)}_{k=1}\underbrace{(1 + x^2 + x^4 + \cdots)}_{k=2}\underbrace{(1 + x^3 + x^6 + \cdots)}_{k=3}\cdots$$

Coefficients of x^n in the product can be viewed as follows: how many parts of size k will be put? I.e., solutions to $a_1 \cdot 1 + a_2 \cdot 2 + \cdots + a_n \cdot n = n$, with $a_i \ge 0$. This is exactly $p(n)$. □

Note: to compute, for example $p(5) = 7$, it suffices to find coefficient of x^5 in

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)}$$

We introduce some variations of Euler's partition formula.

Proposition 10.17. *If $a_n :=$ number of partitions of n into different-sized pieces, then the OGF is $f(x) = \sum_n a_n x^n = \prod_{k\geq 1}(1+x^k)$.*

Proof. Expanding RHS$=(1+x)(1+x^2)(1+x^3)\cdots$, coefficient of x^n can be viewed as whether or not to choose a part of size i, or more formally, it is the solution to $a_1 \cdot 1 + a_2 \cdot 2 + \cdots + a_n \cdot n = n$, with each $a_i \in \{0, 1\}$. □

Proposition 10.18. *If $b_n :=$ number of partitions of n into odd-sized parts, then OGF: $g(x) = \sum_n b_n x^n = \prod_{k\geq 1}(1-x^{2k-1})^{-1}$.*

Proof. Expanding RHS$=(1+x+x^2+x^3+\cdots)(1+x^3+x^6+\cdots)(1+x^5+x^{10}+\cdots)\cdots$, a similar argument that has been exploited in the proof of Theorem 10.16 can be used here and establish the equality. □

Corollary 10.19 (Euler)**.** *$f(x) = g(x)$, i.e., number of partitions into different-sized parts=number of partitions into odd-sized parts.*

Proof. Behold

$$\begin{aligned}
f(x) &= \prod_{k\geq 1}(1+x^k) \\
&= \prod_{k\geq 1}\frac{1-x^{2k}}{1-x^k} \\
&= \frac{(1-x^2)(1-x^4)(1-x^6)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots} \\
&= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots} && \text{cancel out even exponent parts} \\
&= \prod_{k\geq 1}(1-x^{2k-1})^{-1} \\
&= g(x)
\end{aligned}$$

□

We also provide a sketch for a direct counting argument.

Direct Proof Sketch. Recall given integer $z > 0$, z factors uniquely as $2^k \cdot o$, where o is some odd number. Given $y_1 + \cdots + y_k = n$ with $y_i > y_{i+1}$, we can decompose it into $(2^{m_1} + 2^{m_2} + \cdots) \cdot 1 + (2^{l_1} + 2^{l_2} + \cdots) \cdot 3 + \cdots$ □

Recall: $p(x) = \sum_n p(n)x^n = \prod_{k\geq 1}(1-x^k)^{-1}$, we have just computed $g(x) = \prod_{k\geq 1}(1+x^k)$, then it is natural to consider $\prod_{k\geq 1}(1-x^k)$. We try to write out a few terms of the expansion:

$$\prod_{k\geq 1}(1-x^k) = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} + \cdots$$

Definition 10.20. The *pentagonal number* is the number of dots used to form a pentagon. The mth pentagonal number is denoted by $\omega(m)$. Moreover, $\omega(m) = \frac{m(3m-1)}{2}$.

Remark 10.21. Though combinatorially, $\omega(-m)$ for $m \in \mathbb{N}$ should be undefined, $\omega(-m) = \frac{-m(-3m-1)}{2} = \frac{m(3m+1)}{2} = \omega(m) + m$.

Theorem 10.22 (Euler Pentagonal Number Theorem)**.**

$$\prod_{k\geq 1}(1-x^k) = 1 + \sum_{m\geq 1}(-1)^m(x^{\omega(m)} + x^{\omega(-m)})$$

Proof. The equivalent form is to write $\prod_{k\geq 1}(1-x^k) = \sum_n q_n x^n$, where

$$q_n = \begin{cases} (-1)^m, & \text{if } n = \omega(m) \text{ for } m \in \mathbb{Z} \\ 0, & \text{otherwise} \end{cases}$$

The proof strategy is 3 steps:

Step 1 Find a combinatorial interpretation of q_n.

Step 2 Description, involution, exception.

Step 3 Look for pentagons.

Recall that $\prod_{k\geq 1}(1+x^k) = \sum_n a_n x^n$, where a_n = number of partitions of n into different-sized parts.

Definition 10.23. $p_e(n) :=$ number of partitions of n into an even number of different-sized parts, $p_o(n) :=$ number of partitions of n into an odd number of different-sized parts. So $a_n = p_e(n) + p_o(n)$.

Proposition 10.24. $q_n = p_e(n) - p_o(n)$.

Proof of Claim. In the expansion of $\prod_k(1-x^k) = (1-x)(1-x^2)(1-x^3)\cdots$, the coefficients of x^n counts ways of writing $(-1)^r x^n = (-x^{k_1})(-x^{k_2})\cdots(-x^{k_r})$, where $r =$ number of parts. Notice it is very similar to the argument used in the proof of Proposition 10.17, where odd coefficients are all -1, evens are all 1. □

So the problem becomes to show that

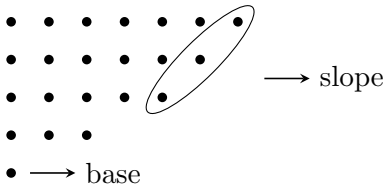
$$p_e(n) - p_o(n) = \begin{cases} (-1)^m, & n = \omega(m), m \in \mathbb{Z} \\ 0, & \text{else} \end{cases}$$

We examine Ferrers diagrams.

Definition 10.25. The *base* of a Ferrers diagram are dots in the bottom row.

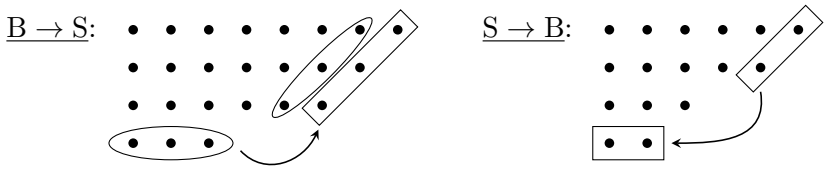
Definition 10.26. The *slope* of a Ferrers diagram are dots directly south-west of the north-east corner.

As an example, the base and slope for the following Ferrers diagram:



Say a Ferrers diagram is *type B* if size of base $\leq$ size of slope, *type S* if size of base $>$ size of slope.

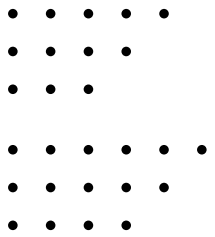
We (partially) define an involution i : type B $\leftrightarrow$ type S as follows:



Note the involution i, with exception:

- either adds a single row
- or removes a single row

So i matches up $p_e(n)$ and $p_o(n)$. The exceptions arise when the base and slope overlap and are too small:



In type B exception, toggle base will make partition invalid, and in type S exception, toggle slope will make two equal-sized parts, so the result is no longer a partition into different-sized parts.

Remarkably, in type B exception, $n = \omega(m)$, and in type S exception, $n = \omega(m) + m = \omega(-m)$, where m is the number of rows. Each such n has exactly one exception, which has m parts, so it contributes $(-1)^m$ to $p_e(n) - p_o(n)$. Every other n has no exception, so $p_e(n) - p_o(n) = 0$. This completes our proof. □

Recall: $\prod_{k\geq 1}(1-x^k)^{-1} = \sum_n p(n)x^n$, we see

$$\Big(\sum_n q_n x^n\Big)\Big(\sum_n p(n)x^n\Big) = \prod_{k\geq 1}(1-x^k)\prod_{k\geq 1}(1-x^k)^{-1} = 1$$

Corollary 10.27. *For all $n > 0$, $\sum_{k=0}^{n} q_k p(n-k) = 0$.*

Proof. By multiplication of formal power series, for $n > 0$, the coefficient of x^n in the product above is $\sum_{k=0}^{n} q_k p(n-k) = 0$. □

This hints that

$$\sum_{k=0}^{n} q_k p(n-k) = p(n) + \sum_{m>0} (-1)^m [p(n-\omega(m)) + p(n-\omega(-m))]$$

where $p(j) = 0$ for $j < 0$. So we have a fast and recursive way of computing $p(n)$:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + \cdots$$

Example 10.28.

$$p(0) = 1, p(1) = p(0) = 1, p(2) = p(1) + p(0) = 2$$
$$p(3) = p(2) + p(1) = 3, p(4) = p(3) + p(2) = 5$$
$$p(5) = p(4) + p(3) - p(0) = 7, p(6) = p(5) + p(4) - p(1) = 11$$
$$p(7) = p(6) + p(5) - p(2) - p(0) = 15, p(8) = p(7) + p(6) - p(3) - p(1) = 22, \ldots$$

11 Coding Theory

11.1 Hadamard matrices

We start with a motivating example.

Example 11.1. Suppose we have 4 possible messages, and we only wish to transmit binary strings: $00, 01, 10, 11$.
Question: What if there is a "high likelihood" that ≤ 1 bit gets flipped?
Answer: One obvious solution is adding *redundancy*.

$$000000$$
$$000111$$
$$111000$$
$$111111$$

Here is a better solution:

$$00000$$
$$00111$$
$$11100$$
$$11011$$

Exercise: show that 4 bits do not suffice.

Definition 11.2. Suppose Σ is a finite alphabet, given two Σ-words of length n, $v, w \in \Sigma^n$, their *Hamming distance* is $d(v, w) = |\{i : v_i \neq w_i\}|$.

In general, we are interested in finding $C \subseteq \Sigma^n$ such that

- $|C|$ is large.
- $\forall v, w \in C, v \neq w \Rightarrow d(v, w)$ is large.

The extreme case of $d(v, w)$ large is a family of codes called *Reed–Muller* codes: $C \subseteq \{0, 1\}^n$ and $v, w \in C, v \neq w \Rightarrow d(v, w) = \frac{n}{2}$.

Example 11.3. The following is a Reed–Muller code of length 4:

$$0000$$
$$0011$$
$$0101$$
$$0110$$

If we replace 0 by 1, 1 by -1, we get

$$++++$$
$$++--$$
$$+-+-$$
$$+--+$$

Above, we use $+$ to denote 1 and $-$ to denote -1. Notice the above vectors are orthogonal to each other.

Definition 11.4. A *Hadamard matrix* of order n is an $n \times n$ matrix with entries ± 1, such that any 2 distinct rows are orthogonal with respect to dot product. More formally, H is Hadamard if and only if $HH^T = nI$.

Example 11.5. Hadamard matrix of order $1, 2, 4$:

$$\begin{bmatrix}+\end{bmatrix}, \begin{bmatrix}+ & + \\ + & -\end{bmatrix}, \begin{bmatrix}+ & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & +\end{bmatrix}$$

Note that since $HH^T = nI$, we have $H^{-1} = \frac{H^T}{n}$, so $H^T H = H^{-1}(HH^T)H = H^{-1}nIH = nH^{-1}H = nI$, hence columns are also pairwise orthogonal.

Note also that if one flips the sign of an entire row or column, or shuffles rows or columns, the result remains Hadamard.

From now on, we'll assume Hadamard matrices are *normalized*, in the sense that the first row and column are all $+$'s (all remaining rows/cols have half $+$'s and $-$'s).

Theorem 11.6. *If H is a Hadamard matrix of order $n > 2$, then n is a multiple of 4.*

Proof. Without loss of generality assume H is normalized, we write the first 3 rows in H and shuffle columns so that it looks like:

$$\begin{array}{l} +\ldots+\ldots+\ldots+\ldots \\ +\ldots+\ldots-\ldots-\ldots \\ \underbrace{+\ldots}_{a}\underbrace{-\ldots}_{b}\underbrace{+\ldots}_{c}\underbrace{-\ldots}_{d} \end{array}$$

we know that $a + b + c + d = n$, the goal is to show $a = b = c = d = \frac{n}{4}$.

- $R_1 \perp R_2 : a + b = c + d$
- $R_1 \perp R_3 : a + c = b + d$
- $R_2 \perp R_3 : a + d = b + c$

Add the above three equations, we get

$$\begin{aligned} 3a + b + c + d &= 2b + 2c + 2d \\ &\Rightarrow 3a = b + c + d \\ &\Rightarrow 4a = a + b + c + d = n \\ &\Rightarrow a = \frac{n}{4} \end{aligned}$$

Then it's trivial to show that $a = b = c = d$. □

A famous open question is whether n is a multiple of 4 is also sufficient for a Hadamard matrix of order n to exist. The smallest open case is $n = 668$, since for $n = 428$, it was constructed in 2005.

Question: How do we build large Hadamard matrices?

Definition 11.7. The *Kronecker product* is defined on two matrices $A = (a_{ij}), B$, by $A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ \dots & \dots & \dots & \dots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}$ for A being an $m \times n$ matrix.

Example 11.8. $A = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} -1 & 3 \\ 0 & 4 \end{bmatrix}, A \otimes B = \begin{bmatrix} -2 & 6 & -1 & 3 \\ 0 & 8 & 0 & 4 \\ -1 & 3 & 0 & 0 \\ 0 & 4 & 0 & 0 \end{bmatrix}$

Facts:

- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, when the product is defined.
- $(A \otimes B)^T = A^T \otimes B^T$.

Proposition 11.9. *If H_1, H_2 are Hadamard matrices, then so is $H_1 \otimes H_2$.*

Proof. Assume H_1 is of order a and H_2 is of order b, then we need to show $H_1 \otimes H_2$ is Hadamard of order ab, i.e.,

$$(H_1 \otimes H_2)(H_1 \otimes H_2)^T = abI$$

Consider the following sequence of equalities:

$$\begin{aligned} (H_1 \otimes H_2)(H_1 \otimes H_2)^T &= (H_1 \otimes H_2)(H_1^T \otimes H_2^T) \\ &= (H_1 H_1^T) \otimes (H_2 H_2^T) \\ &= aI_a \otimes bI_b \\ &= abI_{ab} \end{aligned}$$

□

This gives us the first way of constructing Hadamard matrix: start with $\begin{bmatrix} + & + \\ + & - \end{bmatrix}$, repeatedly do Kronecker product with it, this gives a Hadamard matrix of every order $n = 2^m$, for $m \geq 1$.

How about Hadamard matrices of other orders?

Definition 11.10. A *field* is a structure $\mathbb{F} = (F, 0_{\mathbb{F}}, 1_{\mathbb{F}}, +_{\mathbb{F}}, \times_{\mathbb{F}})$, where arithmetic "makes sense".

Example 11.11. Let p be a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

It turns out that whenever $q = p^k$ is a prime power, there exists a *unique* (up to isomorphism) field of cardinality q.

Next goal: Build a Hadamard matrix for $n = 12$.

We consider a fundamental question: what is positivity? In $\mathbb{R}$, we usually think of it in an order-theoretical way. However, this does not develop a good intuition for fields. In fact, there is an *algebraic* definition for positivity:

Definition 11.12. Let $\mathbb{F}$ be a finite field, then r is *positive* if and only if r is a *quadratic residue*, i.e.,

- $r \neq 0$
- $\exists s, r = s^2$

Definition 11.13. Given a finite field $\mathbb{F}$, the *square word*, $\square$, is a mapping:

$$\square : a \to \begin{cases} 0, & \text{if } a = 0 \\ +, & \text{if } a \text{ is a quadratic residue} \\ -, & \text{if } a \neq 0 \text{ and is not a quadratic residue} \end{cases}$$

Example 11.14. Consider $\mathbb{F} = \mathbb{Z}/11\mathbb{Z}$.

	0	1	2	3	4	5	6	7	8	9	10
$\square$	0	+	−	+	+	+	−	−	−	+	−

We leave the following as exercises for readers to check:

- If $|\mathbb{F}|$ is odd, then half of non-zero elements are quadratic residues.
- If $|\mathbb{F}|$ is finite, then $\square(ab) = \square(a)\square(b)$.

As a hint, notice there always exists a *generator* in $\mathbb{F}$, considering exponents of the generator g might be helpful.

Definition 11.15. For each $k \in \mathbb{F}$, the *k-translated square word*, $\square_k$, is defined as a mapping:

$$\square_k(a) = \square(a - k)$$

So in $\mathbb{F}_{11}$, we have $\square_5$:

	0	1	2	3	4	5	6	7	8	9	10
$\square_5$	−	−	−	+	−	0	+	−	+	+	+

Proposition 11.16. *For $|\mathbb{F}|$ being odd, if $j \neq k$, then $\square_j \cdot \square_k = -1$.*

Proof. Without loss of generality, let's assume $j = 0, k \neq 0$, so we want

$$\begin{aligned} &\sum_{a \in \mathbb{F}} \square(a)\square(a-k) = -1 \\ \Rightarrow &\sum_{a \neq 0} \square(a)\square(a-k) = -1 \end{aligned}$$

$$\begin{aligned} \sum_{a \neq 0} \square(a)\square(a-k) &= \sum_{a \neq 0} \square(a)\square(a(1-k/a)) \\ &= \sum_{a \neq 0} \square(a)\square(a)\square(1-k/a) \\ &= \sum_{a \neq 0} \square(1-k/a) \\ &= \sum_{b \neq 1} \square(b) \\ &= -1 \end{aligned}$$

Here $j = 0$ is fine, since the shift $a \mapsto a + j$ turns $\square_j \cdot \square_k$ into $\square_0 \cdot \square_{k-j}$. Notice $b = 1 - k/a$ runs over $\mathbb{F} \setminus \{1\}$ as a runs over $\mathbb{F} \setminus \{0\}$, since $k \neq 0$. The last equality holds since half of the non-zero elements are quadratic residues, so $\sum_{b \neq 1} \square(b) = \sum_{b \in \mathbb{F}} \square(b) - \square(1) = 0 - 1$. □

We build a matrix of 11×11, where the ith row is just $\square_i$. Then we augment it by adding a row, with the first entry 0 and all other $+$'s, and a column of the first entry 0 and all other $-$'s, to obtain a 12×12 matrix. Let C_{11} denote the resulting matrix, we first try to explore some properties of C_{11}.

Proposition 11.17. *C_{11} is a*

(1) 12×12 *matrix*

(2) antisymmetric: $C_{11}^T = -C_{11}$

(3) 0*'s always on the main diagonal*

(4) ± 1*'s elsewhere*

(5) $C_{11} C_{11}^T = (12 - 1)I$

Proof. We prove (2) and (5).

- Antisymmetry: The first row and column is antisymmetric by our augmentation. For other entries, we need to show that $\square_a(b) = -\square_b(a)$, i.e., $\square(b - a) = -\square(a - b)$, this is true since $\square(-1) = \square(10) = -1$, so $-1 \cdot \square(a - b) = \square(-1) \cdot \square(a - b) = \square(b - a)$.
- $C_{11} C_{11}^T = 11I$: we need to show that different rows of C_{11} are pairwise orthogonal, and the dot product of a row with itself is 11. The first part follows from Proposition 11.16, we have $\square_j \cdot \square_k = -1$ for $j \neq k$, recall we have appended $-$'s to both rows, so their dot product is $-1 + 1 = 0$. The new first row $(0, +, \ldots, +)$ is orthogonal to every row $(-, \square_i)$ as well: their dot product is $0 + \sum_{a \in \mathbb{F}} \square(a - i) = 0$, since half of the non-zero elements of $\mathbb{F}_{11}$ are quadratic residues. The second part is due to the fact that each row has a 0 and all other entries are ± 1.

□

In fact, C_{11} belongs to a family of matrices, which we introduce below.

Definition 11.18. An $n \times n$ matrix is a *conference matrix* if

- 0's along main diagonal.
- ± 1 elsewhere.
- $CC^T = (n - 1)I$.

Proposition 11.19. *If C is an antisymmetric conference matrix, then $C + I$ is Hadamard.*

Proof. $(C + I)(C + I)^T = CC^T + C + C^T + I = (n - 1)I + C - C + I = nI$ □

So we obtain a Hadamard matrix of order 12 by adding I_{12} to C_{11}.
What about $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$? Observe that

	0	1	2	3	4
$\square$	0	+	−	−	+

This time we augment the 5×5 matrix with row i equal to $\square_i$ by a row of 0 and all +'s, and a column that is exactly the same as the row. Notice C_5 is a symmetric conference matrix, the reason is $\square(-1) = \square(4) = 1$.

Proposition 11.20. *If C is a symmetric conference matrix, then*

$$\begin{bmatrix} C+I & C-I \\ C-I & -C-I \end{bmatrix}$$

is Hadamard.

We leave the above proposition to the reader to check.

Interestingly, C_5 is symmetric since its square word is a palindrome, C_{11} is antisymmetric since its square word is an anti-palindrome. As in our above observation, whether $C_{\mathbb{F}}$ is symmetric or antisymmetric is determined by $\square(-1)$, since all we need to do is to check $\square_a(b)$ and $\square_b(a)$. If $\square(-1) = 1$, then $C_{\mathbb{F}}$ is symmetric, otherwise, it's antisymmetric.

Lemma 11.21 (Algebra blackbox)**.** *If $\mathbb{F}$ is a finite field, then*

- $|\mathbb{F}| \equiv 1 \pmod 4 \Rightarrow \square(-1) = 1$
- $|\mathbb{F}| \equiv 3 \pmod 4 \Rightarrow \square(-1) = -1$

By the blackbox lemma (Lemma 11.21), we have the following theorem, which is a direct application of the lemma and the construction we illustrated above.

Theorem 11.22 (Paley)**.** *Let q be a prime power.*

(1) If $q \equiv 3 \pmod 4$, then there is a Hadamard matrix of order $q+1$.

(2) If $q \equiv 1 \pmod 4$, then there is a Hadamard matrix of order $2(q+1)$.

11.2 Codes and some bounds

Definition 11.23. A *code* of length n is a subset $C \subseteq \Sigma^n$.

Definition 11.24. The *mindist* of C is $\text{mindist}(C) = \min_{x \neq y \in C} d(x, y)$, where $d(x, y)$ is the Hamming distance (Definition 11.2) between x and y.

Definition 11.25. C is *e-error-correcting* if $\text{mindist}(C) \geq 2e + 1$.

The intuition behind this definition is, in order to correct up to e errors, two different codewords $x, y \in C$ must differ in a lot of positions. More specifically, in the worst case the adversary can change e positions of x and e positions of y so that corresponding positions of x and y are all the same, so we need an additional position to differ, so that we can tell the difference between x and y, thus, $\text{mindist}(C)$ is at least $2e + 1$.

Definition 11.26. Given a word $x \in \Sigma^n$, the *Hamming ball* around x with *radius* r is all words $y \in \Sigma^n$ such that $d(x, y) \leq r$. We use $B_r(x) = \{y \in \Sigma^n : d(x, y) \leq r\}$ to denote.

The intuition behind *e-error-correction* is best illustrated using the definition of Hamming ball: C is *e-error-correcting* if and only if $\forall x \neq y \in C$, $B_e(x) \cap B_e(y) = \emptyset$.

We present two not-so-hard but useful bounds on codes.

Theorem 11.27 (Singleton Bound)**.** *If $C \subseteq \Sigma^n$ has* $\text{mindist}(C) \geq d$*, then* $|C| \leq |\Sigma|^{n-d+1}$.

Proof. We will show we can map each codeword $x \in C$ to its prefix of $n - d + 1$ positions, and this mapping is an injection. Let $x \neq y \in C$, since $\text{mindist}(C) \geq d$, we know that $d(x, y) \geq d$, so let's consider in what positions do they differ, especially for the last $d - 1$ positions. Below, we use $\text{suf}(x)$ to denote the suffix $d - 1$ positions of x.

Case 1 Suppose not all suffix $d-1$ positions differ, in this case, $d(\text{suf}(x), \text{suf}(y)) < d$, so there must be some positions in prefix $n - d + 1$ places that x, y differ.

Case 2 Suppose all suffix $d-1$ positions differ, then $d(\text{suf}(x), \text{suf}(y)) = d-1$, however, $d(x, y) \geq d$, so at least one position in prefix $n - d + 1$ places differ.

Therefore, this mapping is injective: two different codewords have two distinct $n - d + 1$ prefixes. We hence have the inequality $|C| \leq |\Sigma|^{n-d+1}$. □

Theorem 11.28 (Hamming Bound)**.** *If $C \subseteq \Sigma^n$ is e-error-correcting, then* $|C| \leq \frac{|\Sigma|^n}{\sum_{i=0}^{e} \binom{n}{i}(|\Sigma|-1)^i}$.

Proof. We examine the size of Hamming ball around a codeword $x \in C$. Given $x \in \Sigma^n$, we first claim the set $\{y \in \Sigma^n : d(x, y) = i\}$ has size $\binom{n}{i}(|\Sigma| - 1)^i$. To see this, we start with x, first choose i positions for y to differ from x, then for each of these positions, we can choose any symbol except the one that x has, so $|\Sigma| - 1$ choices. In total, the set has size $\binom{n}{i}(|\Sigma| - 1)^i$.

Thus, $|B_e(x)| = \sum_{i=0}^{e} \binom{n}{i}(|\Sigma| - 1)^i$. Recall that e-error-correction is equivalent to $\forall x \neq y \in C$, $B_e(x) \cap B_e(y) = \emptyset$, so we have

$$|C| \cdot |B_e(x)| \leq |\Sigma|^n$$

□

Definition 11.29. If a code C meets the Hamming bound, then it is called *perfect*.

Example 11.30. A trivial perfect code.

The code $C = \{000, 111\} \subseteq \{0,1\}^3$ is perfect 1-error-correcting, since $\text{mindist}(C) = 3$, moreover,

$$|C| = 2 = \frac{2^3}{\binom{3}{0} + \binom{3}{1}}$$

Example 11.31. Let $\Sigma = \{0,1,2\}$, ternary alphabet, code C has $n = 4$, then

$$C = \{0000, 0111, 0222, 1012, 2021, 1120, 2210, 1201, 2102\}$$

is perfect 1-error-correcting, since $\text{mindist}(C) = 3$, moreover,

$$|C| = 9 = \frac{3^4}{\binom{4}{0} + \binom{4}{1}(3-1)}$$

Example 11.32. The following is the famous binary Hamming code. $C = \{(a,b,c,d,a+b+c,a+b+d,a+c+d) : a,b,c,d \in \mathbb{F}_2\}$, it is also perfect 1-error-correcting.

Codes often arise as (vector) subspaces of $\mathbb{F}^n$, in this case, they are called *linear codes*. In this case, we can use a finite field $\mathbb{F}$ as our alphabet, we view words of $\mathbb{F}^n$ as a vector space over $\mathbb{F}$.

Definition 11.33. A q-ary $[n,k]$-code is a subspace C of $\mathbb{F}_q^n$ with $\dim(C) = k$. So $|C| = q^k$.

Definition 11.34. The *weight*, w, of $x \in \mathbb{F}^n$ is $d(x, \vec{0}) = |\{i \leq n : x(i) \neq 0\}|$.

So $d(x,y) = w(x-y)$.

Proposition 11.35. *If $C \subseteq \mathbb{F}^n$ is a linear code, then* $\text{mindist}(C) = \min_{x \neq \vec{0} \in C} w(x)$.

Proof. Since C is a linear code, it is a linear subspace of $\mathbb{F}^n$. Let $x \neq y \in C$ be two codewords in C that minimize $d(x,y)$, so $\text{mindist}(C) = d(x,y)$. Since C is a subspace, we have $x - y \in C$. It remains to show that $d(x,y) = w(x-y)$, to see this, consider an arbitrary index i. If $x_i = y_i$, then i does not count to $d(x,y)$, and $x_i - y_i = 0$, so it also does not count to $w(x-y)$. On the other hand, if $x_i \neq y_i$, it counts to $d(x,y)$, and $x_i - y_i \neq 0$, so it also counts to $w(x-y)$. Therefore, $d(x,y) = w(x-y)$, so $\text{mindist}(C) = w(x-y) \geq \min_{z \neq \vec{0} \in C} w(z)$, since $x - y \neq \vec{0}$. Notice every $z \neq \vec{0}$ in C also has $w(z) = d(z, \vec{0}) \geq \text{mindist}(C)$, since $\vec{0} \in C$. The equality hence holds. □

Since C is a linear subspace of $\mathbb{F}^n$, it does admit some succinct representation.

Definition 11.36. If C is an $[n,k]$-code over $\mathbb{F}$, we say a matrix G is a *generating matrix* for C:

- G is $k \times n$.
- $C =$ row space of G.

Example 11.37. Consider the 3×7 matrix over $\mathbb{F}_2$:

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} : \mathbb{F}_2^7 \to \mathbb{F}_2^3$$

let $C = \ker(H)$, since $\text{rank}(H) = 3$, due to the I_3 in the last 3 columns, $\dim(C) = 7 - 3 = 4$, so $|C| = 2^4 = 16$.

Proposition 11.38. *C is perfect 1-error-correcting.*

Proof. If C is 1-error-correcting, then it is perfect, since

$$|C| = 16 = \frac{2^7}{\binom{7}{0} + \binom{7}{1}}$$

So it suffices to show C is 1-error-correcting, or equivalently, $\text{mindist}(C) \geq 3$, which is also equivalent to showing that $\forall x \in \ker(H) \setminus \{\vec{0}\}, w(x) \geq 3$. Fix an x. Let $c_1, c_2, \ldots, c_7$ denote columns of H.

Subclaim 1 $w(x) \neq 1$. Toward a contradiction, if $x \in \ker(H)$ with $w(x) = 1$, let's say $x_j = 1$, then $Hx = c_j$. However, none of H's columns is $\vec{0}$, a contradiction.

Subclaim 2 $w(x) \neq 2$. Again toward a contradiction, if $x \in \ker(H)$ with $w(x) = 2$, let's say $x_i = x_j = 1$ with $i \neq j$, then $Hx = c_i + c_j$, examine columns of H, we will find that no two of its columns sum to $\vec{0}$, a contradiction.

□

Theorem 11.39 (Hamming)**.** *Suppose $\mathbb{F}$ is a finite field with $|\mathbb{F}| = q$. If $n = \frac{q^k-1}{q-1}$, $k \in \mathbb{N}^+$, then there is a perfect 1-error-correcting code $C \subseteq \mathbb{F}^n$.*

Proof. We just need to build a $k \times n$ matrix H such that

- all columns are non-zero in $\mathbb{F}^k$;
- no column is a scalar multiple of another.

Then we let $C = \ker(H)$ and calculate $|\ker(H)|$.

Start with $\mathbb{F}^k \setminus \{\vec{0}\}$, the size is $q^k - 1$. Then notice that the scalar multiple relation is an equivalence relation on $\mathbb{F}^k \setminus \{\vec{0}\}$, since

- x is a scalar multiple of x.
- If x is a scalar multiple of y, then y is a scalar multiple of x.
- If x is a scalar multiple of y and y is a scalar multiple of z, then x is a scalar multiple of z.

So our strategy will be choosing one vector from each of these equivalence classes. Notice each equivalence class contains exactly $q - 1$ vectors: fix an x, there are q scalar multiples of it, and we drop $\vec{0}$. Thus, there are exactly $\frac{q^k-1}{q-1} = n$ classes, so choosing one vector from each class gives n vectors that meet our criteria.

We then calculate $|\ker(H)|$:

$$\begin{aligned}
|\ker(H)| &= q^{n-k} \\
&= \frac{q^n}{\binom{n}{0} + \binom{n}{1}(q-1)} \\
&= \frac{q^n}{1 + n(q-1)} \\
&= \frac{q^n}{1 + q^k - 1} \\
&= \frac{q^n}{q^k} \\
&= q^{n-k}
\end{aligned}$$

Where the first equality holds since $\text{rank}(H) = k$: the class of each standard basis vector e_i of $\mathbb{F}^k$ gives a column that is a non-zero multiple of e_i, so the columns of H span $\mathbb{F}^k$.

To show it is 1-error-correcting, we use an argument that is similar to the proof in Example 11.37, i.e., $\forall x \in C \setminus \{\vec{0}\}, w(x) \geq 3$. First notice $w(x) \neq 1$, since no column is $\vec{0}$. Moreover, $w(x) \neq 2$: assume otherwise, then we have $ac_i + bc_j = \vec{0}$ for some $a, b \neq 0 \in \mathbb{F}$ and $i \neq j$, where $c_1, \ldots, c_n$ denote the columns of H. Then

$$\begin{aligned}
ac_i + bc_j &= \vec{0} \\
ac_i &= -bc_j \\
c_i &= -\frac{b}{a}c_j
\end{aligned}$$

i.e., c_i is a scalar multiple of c_j, which cannot be the case.

Thus, C is perfect 1-error-correcting. □

12 Lattice Theory

12.1 Basic definitions & examples

Recall the definition of a partial order (Definition 5.1), i.e., a binary relation on a set that is

- Reflexive.
- Antisymmetric.
- Transitive.

Definition 12.1. A *linear order* is a partial order that is *total*, i.e., $\forall x, y, x \leq y \vee y \leq x$.

Proposition 12.2. *Every finite poset admits a linear extension, i.e., given $(P, \leq)$, we can find a linear order $\leq_L$ on P such that $x \leq y \Rightarrow x \leq_L y$.*

Proof. By induction on $|P|$.

Base case: if $|P| = 0$, then it's vacuous. $|P| = 1$ is also vacuous.

Inductive step: find a maximal element $p_{max} \in P$, i.e., $\forall q, p_{max} \leq q \Rightarrow p_{max} = q$, in English, there is no element that is larger than p_{max}. We delete p_{max} from P, the inductive hypothesis states that there is a valid linear extension in $P \setminus \{p_{max}\}$, we denote it by $\leq_{L'}$. Define $\leq_L$ on P as follows:

For any $x \neq y \in P$:

- If $x, y \neq p_{max}$, then $\leq_L (x, y) = \leq_{L'} (x, y)$;
- Without loss of generality, let's say $x = p_{max}$, then put $y \leq_L p_{max}$.

This is a valid linear order extending $\leq$, since for x, y other than p_{max}, the validity is handled by inductive hypothesis, and for p_{max}, we have $q \leq_L p_{max}$ for every q by construction, and by its maximal property, there is no $q \neq p_{max}$ with $p_{max} \leq q$ to respect. □

Definition 12.3. Given a poset $(P, \leq)$, $S \subseteq P$ and $p \in P$, we say that p is the *least upper bound* or *supremum* of S if

- $\forall s \in S$, $s \leq p$ and
- $\forall x \in P$, $((\forall s \in S, s \leq x) \Rightarrow p \leq x)$.

Definition 12.4. Given a poset $(P, \leq)$, $S \subseteq P$ and $p \in P$, we say that p is the *greatest lower bound* or *infimum* of S if

- $\forall s \in S$, $p \leq s$ and
- $\forall x \in P$, $((\forall s \in S, x \leq s) \Rightarrow x \leq p)$.

Remark 12.5. If such p exists for S, then it's unique by antisymmetry, for supremum, we denote it by $\bigvee S$, for infimum, we denote it by $\bigwedge S$.

Definition 12.6. A poset $(P, \leq)$ is an (order) *lattice* if whenever $S \subseteq P$ is finite, $\bigvee S$ and $\bigwedge S$ exist.

Remark 12.7. Lattices always have *greatest* and *least* elements, i.e., $\exists 0, 1$, such that $\forall x, 0 \leq x \leq 1$.

Proof. Put $0 = \bigvee \emptyset, 1 = \bigwedge \emptyset$. Consider the meaning of $\bigvee \emptyset$, it means that $\forall s \in \emptyset, s \leq 0$ holds vacuously, and for any element $y \in P$, $\forall s \in \emptyset, s \leq y$ also holds vacuously, so $0 \leq y$. So it is the least element. Similar for $\bigwedge \emptyset$. □

Remark 12.8. If greatest/least elements exist, to check whether $(P, \leq)$ is a lattice, it suffices to check $\bigvee S, \bigwedge S$ exist for $|S| = 2$.

Some notation: if $S = \{x, y\}$, we abbreviate $\bigvee S$ by $x \vee y$, $\bigwedge S$ by $x \wedge y$.

Example 12.9. (a) If $(L, \leq)$ is a finite linear order then it's a lattice, with $\bigvee S = \max(S), \bigwedge S = \min(S)$.

(b) If X is a set, $(\mathcal{P}(X), \subseteq)$ is a lattice, with $A \vee B = A \cup B, A \wedge B = A \cap B$.

(c) Fix $n > 0$, put $L = \{\text{divisors of } n\}$, then $(L, |)$, i.e., $m \mid n \Leftrightarrow \exists k, n = km$, is a lattice, with $j \vee k = \text{lcm}(j, k), j \wedge k = \gcd(j, k)$.

(d) Subspaces of a finite-dimensional vector space V, ordered by containment. Then least element is $\{\vec{0}\}$, greatest is V, $w_0 \wedge w_1 = w_0 \cap w_1$, $w_0 \vee w_1 = \text{span}(w_0 \cup w_1)$.

Some facts about $\vee, \wedge$: as binary operations on a lattice, they satisfy:

- Commutativity: $x \wedge y = y \wedge x$.
- Associativity: $(x \wedge y) \wedge z = x \wedge (y \wedge z)$.
- Idempotence: $x \wedge x = x$.

12.2 Zeta function & Möbius function

Let $(P, \leq)$ be a poset with $|P| = n < \infty$.

Definition 12.10. The ($\mathbb{C}$-)*incidence algebra* of P, denoted by $\mathbb{A}(P)$, is the set of all functions $f : P \times P \to \mathbb{C}$ such that $x \not\leq y \Rightarrow f(x, y) = 0$, or equivalently, $f(x, y) \neq 0 \Rightarrow x \leq y$.

A more reasonable way to think about $\mathbb{A}(P)$ is to fix a linearization $\leq_L$ of $\leq$ and view $\mathbb{A}(P)$ as a subset of $n \times n$ matrices.

Example 12.11. Consider $(\mathcal{P}(\{a, b\}), \subseteq)$, we have $\emptyset \leq \{a\}, \{b\} \leq \{a, b\}$, so view it in a matrix form with $\emptyset = 1, \{a\} = 2, \{b\} = 3, \{a, b\} = 4$:

$$\begin{bmatrix} * & * & * & * \\ 0 & * & 0 & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{bmatrix}$$

Proposition 12.12. *Suppose $\alpha, \beta \in \mathbb{A}(P)$ and $c \in \mathbb{C}$, then*

(1) $c\alpha \in \mathbb{A}(P)$

(2) $\alpha + \beta \in \mathbb{A}(P)$

(3) $\alpha\beta \in \mathbb{A}(P)$

We prove (3), since (1) and (2) hold trivially: multiplying by a scalar won't turn 0 into other numbers, and adding two 0's yields 0.

Proof of (3). Recall $(\alpha\beta)(i, k) = (\alpha\beta)_{ik} = \sum_j \alpha(i, j)\beta(j, k)$. If $(\alpha\beta)(i, k) \neq 0$, then $\exists j$ such that $\alpha(i, j) \neq 0, \beta(j, k) \neq 0$, which means $i \leq j$ and $j \leq k$. By transitivity of $\leq$, we have $i \leq k$, as desired. □

Remark 12.13. The identity matrix I and zero matrix $\mathbf{0}$ are both in $\mathbb{A}(P)$.

Definition 12.14. The *zeta function* of P is $\zeta \in \mathbb{A}(P)$ with

$$\zeta(x, y) = \begin{cases} 1, & \text{if } x \leq y \\ 0, & \text{otherwise} \end{cases}$$

Example 12.15. Consider $(\mathcal{P}(\{a, b\}), \subseteq)$, then

$$\zeta = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \zeta^{-1} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Notice $\zeta^{-1} \in \mathbb{A}(P)$.

Recall that given a polynomial $p = \sum_{i \leq d} a_i x^i \in \mathbb{C}[x]$ and a square matrix A, we have $p(A) = \sum_{i \leq d} a_i A^i$.

Proposition 12.16. *Given any finite poset P,*

- $\zeta^{-1} \in \mathbb{A}(P)$
- ζ^{-1} *takes integer values.*

Definition 12.17. The *Möbius function* is $\mu = \zeta^{-1}$.

Proof. First, notice $\det(\zeta) = 1$, since ζ is an upper triangular matrix with 1's on the main diagonal, so ζ^{-1} exists.

Consider $\zeta - I$, it's a matrix with main diagonal all 0's. $(\zeta - I)^2$ has more 0's. Notice the (i, j) entry of $(\zeta - I)^k$ is 0 unless $j - i \geq k$, so $(\zeta - I)^n = \mathbf{0}$, which we can rewrite using the binomial theorem (Theorem 7.14) as

$$\begin{aligned} \sum_{0 \leq k \leq n} (-1)^{n-k} \binom{n}{k} \zeta^k &= 0 \\ (-1)^n I + \sum_{1 \leq k \leq n} (-1)^{n-k} \binom{n}{k} \zeta^k &= 0 \\ \sum_{1 \leq k \leq n} (-1)^{k+1} \binom{n}{k} \zeta^k &= I \end{aligned}$$

So we set $p(x) = \sum_{1 \leq k \leq n} (-1)^{k+1} \binom{n}{k} x^{k-1}$, we have an integer coefficients polynomial such that $\zeta \cdot p(\zeta) = I, \zeta^{-1} = p(\zeta)$. So $\zeta^{-1} \in \mathbb{A}(P)$, since $\mathbb{A}(P)$ contains I, ζ and is closed under sums, scalar multiples and products, and ζ^{-1} takes integer values, since ζ and the coefficients of p are integers, as desired. □

We focus on $(\mathcal{P}(X), \subseteq)$ for X being a finite set, we will see that

$$\mu(A, B) = \begin{cases} 0, & \text{if } A \not\subseteq B \\ (-1)^{|B \setminus A|}, & \text{if } A \subseteq B \end{cases}$$

We remind reader that this is actually P.I.E in disguise.

Given a function $f : P \to \mathbb{C}$, we may regard f as a *vector* in $\mathbb{C}^n$, after linearizing P. If two functions $f, g : P \to \mathbb{C}$ happen to satisfy $\zeta f = g$, then they satisfy $f = \mu g$.

Let $A_1, \ldots, A_m$ be subsets of a finite set U, and consider index sets $I \subseteq [m]$, where an intersection over the empty index set means U. Given an index set I, let $g(I) = |\bigcap_{i \in I} A_i|$, $f(I) = |\bigcap_{i \in I} A_i \setminus \bigcup_{i \notin I} A_i|$. Intuitively, $g(I)$ computes the size of all intersections in the index set I, and $f(I)$ computes the size of all intersections, discarding the part that is not in the index set.

Proposition 12.18. $g(I) = \sum_{I \subseteq J} f(J)$.

Proof. We will prove that for distinct J, $f(J)$ computes the size of a distinct part, i.e., there is no other $J' \supseteq I$ such that the parts computed by $f(J)$ and $f(J')$ have intersection.

Let J, J' be two different index sets with $I \subseteq J, J'$. Since they are different, let X be the set of elements that are in J but not J', and Y be the set of elements that are in J' but not J. So

$$\begin{aligned}
\bigcap_{i\in J} A_i \setminus \bigcup_{i\notin J} A_i &= \bigcap_{i\in (J'\setminus Y)\cup X} A_i \setminus \bigcup_{i\in (\overline{J'}\cup Y)\cap \overline{X}} A_i \\
&= \bigcap_{i\in (J'\setminus Y)\cup X} A_i \cap \overline{\bigcup_{i\notin J} A_i} \\
&= \bigcap_{i\in (J'\setminus Y)\cup X} A_i \cap \bigcap_{i\notin J} \overline{A}_i \\
&= \bigcap_{i\in (J'\setminus Y)\cup X} A_i \cap \bigcap_{i\in (\overline{J'}\cup Y)\cap \overline{X}} \overline{A}_i
\end{aligned}$$

We wish to compute its intersection with the part computed by $f(J')$. Since $J \neq J'$, $X \cup Y \neq \emptyset$. If $i \in Y$, then by the last line, the part computed by $f(J)$ lies inside $\overline{A_i}$, while the part computed by $f(J')$ lies inside A_i. If $i \in X$, it is the other way around. Thus, their intersection is empty. Finally, these parts cover $\bigcap_{i\in I} A_i$: each x in it lies in the part computed by $f(J)$ for $J = \{i : x \in A_i\} \supseteq I$. So $g(I) = \sum_{I\subseteq J} f(J)$. □

So we can write $g(I)$ as

$$\begin{aligned}
g(I) &= \sum_{I\subseteq J} f(J) \\
&= \sum_{J} \zeta(I,J) f(J)
\end{aligned}$$

So $g = \zeta f \Rightarrow f = \mu g$, in particular,

$$\begin{aligned}
f(\emptyset) &= \sum_{J} \mu(\emptyset, J) g(J) \\
&= \sum_{J} (-1)^{|J|} g(J) \\
&= \sum_{J} (-1)^{|J|} |\bigcap_{j\in J} A_j|
\end{aligned}$$

This is exactly the PIE formula.

Next we introduce two useful "tricks" to compute μ.

Trick 1 $\mu(x, z)$ only depends upon the *interval* between x and z.

Definition 12.19. $[x, z] = \{y \in P : x \leq y \leq z\}$.

Proposition 12.20. *For fixed $x, z \in P$:*

(a)

$$\sum_{y\in[x,z]} \mu(x,y) = \begin{cases} 1, & \text{if } x = z \\ 0, & \text{else} \end{cases}$$

(b)

$$\sum_{y\in[x,z]} \mu(y,z) = \begin{cases} 1, & \text{if } x = z \\ 0, & \text{else} \end{cases}$$

Proof. (a) We know $\mu\zeta = I$, so

$$\begin{aligned}(\mu\zeta)(x,z) &= \sum_y \mu(x,y)\zeta(y,z) \\ &= \sum_{y\in[x,z]} \mu(x,y) \\ &= \begin{cases} 1, & \text{if } x = z \\ 0, & \text{else} \end{cases}\end{aligned}$$

where the last equality comes from definition of identity matrix I.

(b) Similarly, we have $\zeta\mu = I$, so

$$\begin{aligned}(\zeta\mu)(x,z) &= \sum_y \zeta(x,y)\mu(y,z) \\ &= \sum_{y\in[x,z]} \mu(y,z) \\ &= \begin{cases} 1, & \text{if } x = z \\ 0, & \text{else} \end{cases}\end{aligned}$$

□

We finally lay out the proof for Trick 1.

Proof of Trick 1. By induction on $|[x,z]|$.

Base case: $|[x,z]| = 1$, i.e., $x = z$, so $\mu(x,z) = \mu(x,x) = 1$.

Inductive step: we know $\mu(x,y)$ only depends on $[x,y]$, $\forall x \le y < z$, by induction hypothesis, this is because for $y < z$, we have $|[x,y]| < |[x,z]|$, so by Proposition 12.20(a), $\sum_{y\in[x,z]} \mu(x,y) = 0$ since $x \neq z$, we therefore have $\mu(x,z) = -\sum_{x\le y<z} \mu(x,y)$, which only depends on $[x,z]$. □

Definition 12.21. We say y *covers* x or y is a *successor* of x if $x < y$ and $\nexists z, x < z < y$. Equivalently, $[x,y] = \{x,y\}$ and $x \neq y$. We denote this by $x \lessdot y$.

Corollary 12.22. *In any poset P, if y is a successor of x, then $\mu(x,y) = -1$.*

Proof. By Trick 1, we know if $x \lessdot y$, then $\mu(x,y)$ only depends on $[x,y]$, i.e., $\{x,y\}$. Zoom into the ζ matrix for only x and y, we have $\zeta = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ So $\mu = \zeta^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, as desired. □

Corollary 12.23. *In $(\mathcal{P}(X), \subseteq)$, if $A \subseteq B$, then $\mu(A, B) = \mu(\emptyset, B \setminus A)$.*

Proof. Examine $[A, B]$, we have

$$\begin{aligned}[A, B] &\cong \mathcal{P}(B \setminus A) \\ &\cong [\emptyset, B \setminus A]\end{aligned}$$

via $C \mapsto C \setminus A$, so the claim follows from Trick 1. □

Trick 2

Theorem 12.24 (Weisner)**.** *In a lattice with $0 < a$, we have $\sum_{x \vee a = 1} \mu(0, x) = 0$.*

Proof. We want to analyze $\sum_{x \vee a = 1} \mu(0, x)$, where

$$\begin{aligned}\sum_{x \vee a = 1} \mu(0, x) &= \sum_{x} [\mu(0, x) \sum_{y \in [x \vee a, 1]} \mu(y, 1)] \\ &= \sum_{x} [\mu(0, x) \sum_{y \geq x \vee a} \mu(y, 1)] \\ &= \sum_{x} \sum_{y \geq x \vee a} \mu(0, x) \mu(y, 1) \\ &= \sum_{x, y} \mu(0, x) \underbrace{\zeta(x, y) \zeta(a, y)}_{y \geq x \vee a} \mu(y, 1) \\ &= \sum_{y \geq a} \mu(y, 1) \sum_{x} \mu(0, x) \zeta(x, y) \\ &= \sum_{y \geq a} \mu(y, 1) \sum_{x \in [0, y]} \mu(0, x) \\ &= \sum_{y \geq a} \mu(y, 1) \cdot 0 \qquad \text{by Proposition 12.20(a) and } y > 0 \\ &= 0\end{aligned}$$

Where the first equality holds since by Proposition 12.20(b), we have $\sum_{y \in [x \vee a, 1]} \mu(y, 1) = \begin{cases} 1, & \text{if } x \vee a = 1 \\ 0, & \text{else} \end{cases}$ □

With Weisner's Theorem in hand, we are finally ready to compute μ in $(\mathcal{P}(X), \subseteq)$.

Proposition 12.25.

$$\mu(A, B) = \begin{cases} 0, & \text{if } A \not\subseteq B \\ (-1)^{|B \setminus A|}, & \text{if } A \subseteq B \end{cases}$$

Proof. If $A \not\subseteq B$, then trivially $\mu(A, B) = 0$. If $A = B$, then $\mu(A, B) = \mu(A, A) = 1$, since $\mu = \zeta^{-1}$ has 1's on the main diagonal. So the interesting case is $A \subsetneq B$. By Corollary 12.23, we know $\mu(A, B) = \mu(\emptyset, B \setminus A)$, so it suffices to show $\mu(\emptyset, C) = (-1)^{|C|}$.

We proceed by induction on $|[\emptyset, C]|$.

Base case: $|[\emptyset, C]| = 1$, i.e., $C = \emptyset$, so $\mu(\emptyset, C) = 1 = (-1)^0$.

Inductive step: pick any $c \in C$, put $a = \{c\}$, notice $a > 0 = \emptyset$, so by Trick 2 (in the lattice $[\emptyset, C]$, whose greatest element is C), we have $\sum_{x \vee \{c\} = C} \mu(0, x) = 0$. There are only 2 x's that contribute to this sum: $x = C, x = C \setminus \{c\}$, so

$$\begin{aligned} \mu(\emptyset, C) + \mu(\emptyset, C \setminus \{c\}) &= 0 \\ \mu(\emptyset, C) &= -\mu(\emptyset, C \setminus \{c\}) \\ &= -(-1)^{|C|-1} && \text{by inductive hypothesis} \\ &= (-1)^{|C|} \end{aligned}$$

This completes the proof. □

12.3 Applications of zeta and Möbius functions

In this section, we present more examples with applications of ζ and μ functions.

Example 12.26. Let P be a chain of n elements, and a_i be the ith element in P.

Proposition 12.27.

$$\mu(a_0, a_{n-1}) = \begin{cases} 1, & n = 1 \\ -1, & n = 2 \\ 0, & n > 2 \end{cases}$$

Proof. $n = 1$ and $n = 2$ cases are trivial, the only interesting one is $n > 2$. We use Trick 2: choose $a_1 > 0$, consider which x's satisfy $x \vee a_1 = a_{n-1}$? The only solution is $x = a_{n-1}$, so $\mu(a_0, a_{n-1}) = 0$. □

The matrix version is even more interesting. ζ is an upper triangular matrix whose non-zero entries are filled with 1's, its inverse μ is a matrix with main diagonal all 1's, and one diagonal above the main diagonal all -1's, all other entries 0.

Example 12.28. Let P be a lattice such that there are $n + 2$ elements in total, except for 0 and 1, all other elements form an antichain. We call elements in antichain $a_1, a_2, \ldots, a_n$.

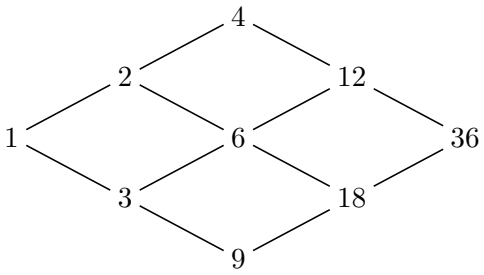
Proposition 12.29. *Suppose $n \geq 2$, then*

$$\mu(0, 1) = n - 1$$

Proof. We know that $\mu(0, a_i) = -1$ for any i, then we apply Trick 2 at $a_1 > 0$, again we ask: what x's satisfy $x \vee a_1 = 1$? This time $x \in \{1, a_2, a_3, \ldots, a_n\}$, so $\mu(0, 1) + \sum_{i \geq 2} \mu(0, a_i) = 0$, we have $\mu(0, 1) = n - 1$ □

We again examine the ζ and μ matrices. ζ matrix has all 1's on main diagonal, the first row all 1's, and the last column all 1's. Its inverse μ is an upper triangular matrix with main diagonal all 1's, the upper right corner being $n - 1$, and all other entries in first row and last column being all -1's.

Example 12.30. Consider the divisor lattice, $\mathcal{L}_n = (\{\text{divisors of } n\}, |)$.
For example, $\mathcal{L}_{36}$:



Proposition 12.31. *Let c be a divisor of n, then*

$$\mu(1, c) = \begin{cases} (-1)^{\textit{number of prime divisors}}, & \textit{if } c \textit{ is square-free} \\ 0, & \textit{else} \end{cases}$$

Proof. First by Trick 1, when $a \mid b$, we have $\mu(a,b) = \mu(1, \frac{b}{a})$ (the map $d \mapsto d/a$ is an isomorphism $[a,b] \cong [1, \frac{b}{a}]$), so the above proposition is useful, in the sense we can generalize arbitrary $\mu(a,b)$ by reducing to $\mu(1, \frac{b}{a})$.

We start with some simple cases. If $c = 1$, then $\mu(1,c) = 1$; if c is a prime, then $\mu(1,c) = -1$. So the interesting case is when c is a composite, we pick a prime divisor p of c.

To use Trick 2, we ask: for what $x \in \mathcal{L}_c$ is $x \vee p = c$? Notice $x = c$ always works.

Case 1 $p^2 \nmid c$. Then $\frac{c}{p}$ works, since $\operatorname{lcm}(\frac{c}{p}, p) = c$, so $x \in \{c, \frac{c}{p}\}$ are the only solutions.

Case 2 $p^2 \mid c$, now $\frac{c}{p}$ also fails, since $c = kp^2$ for some $k \in \mathbb{N}^+$, and $\frac{c}{p} = kp$, $\operatorname{lcm}(\frac{c}{p}, p) = kp = \frac{c}{p}$. In this case, $x = c$ is the only solution.

Notice there are no other solutions: if $\operatorname{lcm}(x,p) = c$ with $x \mid c$, then x has the same exponent as c at every prime other than p, and in Case 2 also at p, since that exponent is at least 2. By Trick 2,

$$\mu(1,c) = \begin{cases} -\mu(1, \frac{c}{p}), & \text{if } p^2 \nmid c \\ 0, & \text{if } p^2 \mid c \end{cases}$$

The final result follows by applying Trick 1, and using a similar inductive argument as we do in the proof of Proposition 12.25. □

Notice we have essentially recovered the Möbius inversion that is introduced in Definition 7.12, if

$$g(n) = \sum_{d \mid n} f(d) = \sum_d f(d)\zeta(d,n)$$

then

$$f(n) = \sum_{d \mid n} g(d)\mu(d,n) = \sum_{d \mid n} g(d)\mu(\frac{n}{d})$$

Example 12.32. This example is in a greater abstract level, compared to others.

Consider $\mathbb{N}$ with the usual order $\leq$, it still makes sense to say $\zeta(m,n) = 1$ if and only if $m \leq n$, so

$$\mu(m,n) = \begin{cases} 1, & \text{if } m = n \\ -1, & \text{if } m+1 = n \\ 0, & \text{else} \end{cases}$$

This is because essentially, $[m,n]$ is a chain.

Consider $\alpha \in \mathbb{A}(\mathbb{N}, \leq)$ with the bonus property that $\alpha(m,n) = \alpha(0, n-m)$, when $m \leq n$. We call it the *reduced incidence algebra*. So α is determined by the sequence $a_n = \alpha(0,n)$, consider the OGF $f(x) = \sum_n a_n x^n$, fix another β also in reduced incidence algebra, with $b_n = \beta(0,n)$ and OGF $g(x) = \sum_n b_n x^n$.

Proposition 12.33. *The OGF for $\gamma = \alpha\beta$ is fg.*

Notice this shows that reduced incidence algebra is *isomorphic* to the formal OGF ring.

Proof. Recall: $fg = \sum_n c_n x^n$, where $c_n = \sum_{i \le n} a_i b_{n-i}$, we check

$$\begin{aligned}
\gamma(0,n) &= \sum_{m \in [0,n]} \alpha(0,m)\beta(m,n) \\
&= \sum_{m \in [0,n]} \alpha(0,m)\beta(0,n-m) \\
&= \sum_{m \le n} a_m b_{n-m} \\
&= c_n
\end{aligned}$$

□

Consider $\zeta, \mu \in \mathbb{A}(\mathbb{N}, \le)$. Indeed, they are in reduced incidence algebra, so

- $$\zeta \to a_n = 1 \to f = \sum_n x^n = \frac{1}{1-x}$$
- $$\mu \to b_n = \begin{cases} 1, & n = 0 \\ -1, & n = 1 \\ 0, & n > 1 \end{cases} \to g = 1 - x$$

Similarly, reduced incidence algebra of $\mathbb{A}(\mathcal{P}_{\text{fin}}(\mathbb{N}), \subseteq) \cong EGF$, $f = \sum_n a_n \frac{x^n}{n!}$:

- $$\zeta \to a_n = 1 \to f = e^x$$
- $$\mu \to b_n = (-1)^n \to g = e^{-x}$$

And the ring of Dirichlet series, $\sum_{n \ge 1} \frac{a_n}{n^s}$, is isomorphic to reduced incidence algebra of $\mathbb{A}(\mathbb{N}^+, |)$, with

- $$\zeta \to a_n = 1 \to \sum_n \frac{1}{n^s} = \zeta(s)$$
- $$\mu \to \frac{1}{\zeta(s)}$$

Where the last two ζ's are the *Riemann zeta function.*

12.4 Advanced countings with lattices

Definition 12.34. Suppose G is a graph on $n \geq 1$ vertices and $x \in \mathbb{N}$, then

$$\chi_G(x) = |\{\text{proper colorings } c : V \to x\}|$$

Example 12.35. G has no edges, then every $c : n \to x$ is a proper coloring, so $\chi_G(x) = x^n$.

Example 12.36. $G = K_n$, then

$$\chi_G(x) = x(x-1)(x-2)\cdots(x-n+1) = (x)_n = \sum_{k=1}^{n} s(n,k)x^k$$

Definition 12.37. *The (ordered) partition lattice* is defined as follows: we consider partitions of an n-element set $[n]$, where elements are distinguishable, then

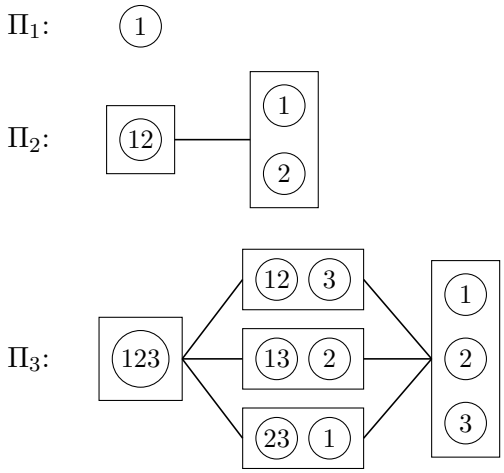
$$\Pi_n = \{\text{all partitions of } [n] \text{ with non-empty parts}\}$$

Given partitions $\mathcal{P}, \mathcal{Q} \in \Pi_n$, we say $\mathcal{P} \leq \mathcal{Q}$ if $\mathcal{P}$ is a *refinement* of $\mathcal{Q}$, or equivalently, $\mathcal{Q}$ is a *coarsening* of $\mathcal{P}$. Via the equivalence relation definition, we say $E \leq F$ if and only if $E \subseteq F$, as sets of pairs.

Suppose $\mathcal{P} \in \Pi_n$, let $|\mathcal{P}|$ denote number of parts in $\mathcal{P}$.

Definition 12.38. The *base partition*, denoted by Δ, is the partition that divides each element into a unique part, and no two elements share a part.

Example 12.39. The following demonstrates Π_1, Π_2, Π_3:



Proposition 12.40. *Each Π_n is a lattice.*

Proof. $E \wedge F = E \cap F, E \vee F = \text{transitive closure}(E \cup F)$. □

Example 12.41. Let $E = \{\{1,2\},\{3,4\}\}, F = \{\{1\},\{2,3\},\{4\}\}$ (as lists of parts), then

$$E \wedge F = \{\{1\},\{2\},\{3\},\{4\}\} = \Delta, \quad E \vee F = \{\{1,2,3,4\}\}$$

Intuitively, we can think of partitions as gathering objects, so transitive closure serves to maintain that, if two objects are originally in the same part, then they remain in the same part after the operation.

Definition 12.42. Suppose $x \in \mathbb{N}$ is fixed. For each $\mathcal{P} \in \Pi_n$, define $g(\mathcal{P})$ = number of functions $n \to x$ which are constant on each part $= x^{|\mathcal{P}|}$, and $f(\mathcal{P})$ = number of functions $n \to x$ which are constant on each part and distinct parts get different colors.

A quick observation: for each function $c : n \to x$ counted by $g(\mathcal{P})$, there is a unique $\mathcal{Q} \in \Pi_n$ with $\mathcal{Q} \geq \mathcal{P}$ such that c is also counted by $f(\mathcal{Q})$. The idea is we group parts that got the same color of $\mathcal{P}$, then find a coarsening $\mathcal{Q}$ of $\mathcal{P}$ such that parts that got the same color are in the same part of $\mathcal{Q}$.

So we have

$$\begin{aligned} g(\mathcal{P}) &= \sum_{\mathcal{Q} \geq \mathcal{P}} f(\mathcal{Q}) \\ &= \sum_{\mathcal{Q}} \zeta(\mathcal{P}, \mathcal{Q}) f(\mathcal{Q}) \\ &\Rightarrow g = \zeta f \end{aligned}$$

Thus, $f = \mu g$, in particular,

$$\begin{aligned} \chi_{K_n}(x) &= f(\Delta) \\ &= \sum_{\mathcal{Q}} \mu(\Delta, \mathcal{Q}) g(\mathcal{Q}) \\ &= \sum_{k=1}^{n} [\sum_{|\mathcal{Q}|=k} \mu(\Delta, \mathcal{Q})] x^k \end{aligned}$$

We therefore have, for $n \geq 1$ in Π_n, $\sum_{|\mathcal{Q}|=k} \mu(\Delta, \mathcal{Q}) = s(n,k)$, by comparing coefficients with $\chi_{K_n}(x) = \sum_k s(n,k) x^k$, since both sides are polynomials in x that agree at every $x \in \mathbb{N}$.

What about the main combinatorial object we are concerned with, namely, finite graphs?

Definition 12.43. Given a graph G on n vertices, we define a subset $L(G) \subseteq \Pi_n$ like so: $\mathcal{P} \in L(G)$ if and only if each part is G-connected. Notice $L(G)$ contains Δ and is closed under the join of Π_n, so it is a lattice, but it need not be closed under the meet of Π_n.

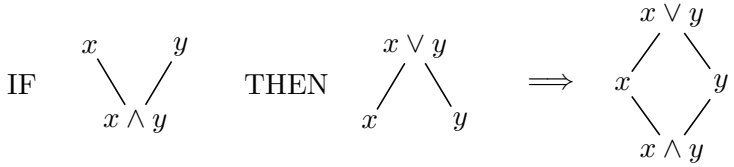
The idea is, each part is "generated" by G-edges.

Recall Definition 12.42 used in partition lattice, we modify f a bit by $f(\mathcal{P})$ = number of functions $n \to x$ constant on each $\mathcal{P}$-part **and** parts connected by a G-edge get different colors.

Notice everything we have discussed on the partition lattice (Definition 12.37) still applies on $L(G)$. In particular, $\chi_G(x) = f(\Delta) = \sum_{\mathcal{Q} \in L(G)} \mu(\Delta, \mathcal{Q}) x^{|\mathcal{Q}|}$.

Definition 12.44. A lattice L is *(weakly) semi-modular* if $\forall x, y \in L$, $(x \wedge y) \lessdot x$ and $(x \wedge y) \lessdot y$ implies $x \lessdot (x \vee y)$ and $y \lessdot (x \vee y)$.

Example 12.45. The following figure demonstrates the above definition. Notice this also coincides with the intuition of *lattices*.



Example 12.46. In $(\mathcal{P}(X), \subseteq)$, we notice $A \lessdot B$ if and only if $A \subseteq B$ and $|B \setminus A| = 1$, so in order for the requirement to hold, we need $A \cap B = A \setminus \{a\} = B \setminus \{b\}$, in this case, $A \cup B = A \cup \{b\} = B \cup \{a\}$, so the powerset lattice is semi-modular.

Example 12.47. In subspace lattice of a finite-dimensional vector space V, $w_1 \lessdot w_2$ if and only if $w_1 \subseteq w_2$ and $\dim(w_2) - \dim(w_1) = 1$. Observe that this case almost reduces to the powerset lattice: if $w_1 \wedge w_2 \lessdot w_1, w_2$, then $w_1 = \text{span}((w_1 \cap w_2) \cup \{a\})$ and $w_2 = \text{span}((w_1 \cap w_2) \cup \{b\})$ for some vectors a, b. Also notice $b \notin \text{span}(w_1)$ and $a \notin \text{span}(w_2)$, since otherwise, we will have $w_1 \subseteq w_2$ or $w_2 \subseteq w_1$, and their intersection is exactly one of w_1 or w_2. So $\text{span}(w_1 \cup w_2) = \text{span}(w_1 \cup \{b\}) = \text{span}(w_2 \cup \{a\})$, which has dimension one more than w_1 and w_2, and subspace lattice is semi-modular as well.

Example 12.48. Consider $L(G)$, $\mathcal{P} \lessdot \mathcal{Q}$ if and only if $\mathcal{P} \leq \mathcal{Q}$ and there is a *unique* pair of parts in $\mathcal{P}$ glued together in $\mathcal{Q}$, also these two parts must be G-adjacent. We can think of $P_1 \wedge P_2$ as $P_1 \cap P_2$, so for $P_1 \wedge P_2 \lessdot P_1, P_2$, we need two distinct pairs of parts to be glued together in P_1 and P_2, which we denote by two edges e_1, e_2. Then $P_1 \vee P_2$ is the transitive closure, which we can view as adding e_2 to P_1 and e_1 to P_2. So $L(G)$ is semi-modular as well.

Definition 12.49. a is an *atom* of L if $0_L \lessdot a$.

Lemma 12.50 (Atom Exchange Principle)**.** *Suppose L is a semi-modular lattice, a, b, c are atoms such that*

- $a \neq c$
- $a \leq b \vee c$

then $b \leq a \vee c$.

We first examine this lemma using the above examples.

Example 12.51. In powerset lattice, atoms are $\{a\}$ for any $a \in X$, notice if $a \subseteq \{b, c\}$ and $a \neq c$, then $a = b$, so trivially, $b \subseteq \{a, c\}$.

Example 12.52. In subspace lattice, atoms are spanned by single non-zero vectors, so $a \in \text{span}(b, c)$ means $a = mb + nc$ for some m, n, where $m \neq 0$, since otherwise a and c span the same atom, contradicting $a \neq c$, this implies $b = \frac{a - nc}{m}$, $b \in \text{span}(a, c)$.

Example 12.53. In $L(G)$, 0_L is Δ, so atoms correspond to single edges in G. Suppose $a \leq b \vee c$ and $a \neq c$, this means either $a = b$, or the edges a, b, c form a triangle in G, so $b \leq a \vee c$ as well.

Proof. We first notice that $b \neq c$, since if $b = c$, then $b \vee c = b$, and $a \leq c, a \neq c$ contradicts that a, b, c are atoms.

Observe that $c \leq b \vee c$ and also $a \leq b \vee c$, this means $a \vee c \leq b \vee c$.

Notice $a \wedge c = 0_L$, since $a \neq c$ are atoms, and 0_L is covered by both a and c. Similarly for b and c. By semi-modularity, we also know that $c \lessdot a \vee c, c \lessdot b \vee c$, so $c \lessdot a \vee c \leq b \vee c \Rightarrow a \vee c = b \vee c$, in particular, $b \leq b \vee c = a \vee c$, as desired. □

Definition 12.54. A lattice is *atomistic* if $\forall x \in L, \exists$ a finite set A of atoms with $x = \bigvee A$.

Definition 12.55. A lattice is *geometric* if it is atomistic and semi-modular.

Lemma 12.56 (Exchange Principle)**.** *Suppose L is a geometric lattice, a, b are atoms, $x \in L$, if*

- $a \not\leq x$
- $a \leq x \vee b$

then $b \leq x \vee a$.

Proof. Since $a \not\leq x$, we have $b \not\leq x$: otherwise $x \vee b = x$ and $a \leq x$. We claim that $x \lessdot x \vee b$. Given the claim, $x < x \vee a \leq x \vee b$, since $a \not\leq x$ and $a \leq x \vee b$, so $x \vee a = x \vee b$, in particular, $b \leq x \vee a$.

To prove the claim, we show $x \lessdot x \vee b$ for every atom $b \not\leq x$, by induction on $|[0_L, x]|$. If $x = 0_L$, it says $0_L \lessdot b$. Otherwise, pick $y \lessdot x$, then $b \not\leq y$, so $y \lessdot y \vee b$ by inductive hypothesis. Notice $y \leq x \wedge (y \vee b) \leq x$, and $x \wedge (y \vee b) = x$ is impossible: it would give $y < x \leq y \vee b$, so $x = y \vee b \geq b$. So $x \wedge (y \vee b) = y$, which is covered by both x and $y \vee b$, and semi-modularity gives $x \lessdot x \vee (y \vee b) = x \vee b$. □

Definition 12.57. A set I of atoms is *independent* if $\forall a \in I, \bigvee(I \setminus \{a\}) < \bigvee I$.

The following proposition requires algebraic knowledge that is out of the scope of this course, so we state it as fact.

Proposition 12.58. *In a geometric lattice, $\forall x \in L$, there exists an independent set I of atoms with $x = \bigvee I$. Moreover, if I, J are independent with $x = \bigvee I = \bigvee J$, then $|I| = |J|$.*

We call $|I|$ the rank of x.

Example 12.59. In powerset lattice, $A = \bigvee I$ where $I = \{\{a\} : a \in A\}$, $|I| = |A|$, $\text{rank}(A) = |A|$.

Example 12.60. In subspace lattice, $w = \bigvee I$, where $I = \{\text{span}(v_i)\}$ for a basis $\{v_i\}$ of w, thus $\text{rank}(w) = \dim(w)$.

Example 12.61. In $L(G)$, atoms correspond to edges in G, a set of edges is *independent* if and only if it is acyclic. The intuition is, when applying independence on $L(G)$, "removing an atom breaks their big join" is equivalent to "removing an edge disconnects two components", so acyclicity is what we want.

Given $\mathcal{P} \in L(G)$, $\text{rank}(\mathcal{P})$ = number of edges in a spanning forest $= n - |\mathcal{P}|$. To better understand this number, consider a tree with n vertices, it also has $n - 1$ edges. If we remove all edges and put them back one by one, each time we reduce number of connected components by one, so when there are $|\mathcal{P}|$ connected components, we have put back exactly $n - |\mathcal{P}|$ edges.

Proposition 12.62. *In a geometric lattice L, $\forall x \in L$,*

$$\mu(0_L, x) = \begin{cases} \geq 0, & \text{if } \text{rank}(x) \text{ even} \\ \leq 0, & \text{if } \text{rank}(x) \text{ odd} \end{cases}$$

Proof. By induction on $\text{rank}(x)$.

Base case: $\text{rank}(x) = 0$, i.e., $x = 0_L$, $\mu(0_L, 0_L) = 1$.

Inductive step: If $\text{rank}(x) > 0$, for some atom $a \leq x$, we use Trick 2 in the lattice $[0_L, x]$: $\sum_{a \vee y = x} \mu(0_L, y) = 0$. We consider what y will contribute to this sum. Obviously, $y = x$ works, otherwise, $y \neq x$ and add a to y, we get x, this implies $\text{rank}(y) = \text{rank}(x) - 1$. To see this, notice $a \not\leq y$, and if I is an independent set with $\bigvee I = y$, then $I \cup \{a\}$ is independent with join x:

removing a leaves $y < x$, and if removing some $c \in I$ still left x, then $z = \bigvee(I \setminus \{c\})$ would satisfy $c \not\leq z$ and $c \leq z \vee a$, so the Exchange Principle would give $a \leq z \vee c = y$.

So apply inductive hypothesis, we have

$$\mu(0_L, x) = -\sum_{y \neq x, a \vee y = x} \mu(0_L, y)$$

where for all such y's, they have the same sign, so $\mu(0_L, x)$ has the opposite sign. □

Corollary 12.63. *Chromatic polynomials have alternating coefficients.*

Proof. Coefficient of x^k is $\sum_{|\mathcal{Q}|=k} \mu(0_{L(G)}, \mathcal{Q})$, and every $\mathcal{Q} \in L(G)$ with $|\mathcal{Q}| = k$ has $\text{rank}(\mathcal{Q}) = n - k$, so by the previous proposition, this coefficient is ≥ 0 if $n - k$ is even and ≤ 0 if $n - k$ is odd. Here $L(G)$ is geometric: it is semi-modular, and it is atomistic since each $\mathcal{Q}$ is the join of the edges of spanning trees of its parts. □

We go back to codes, and try to use μ function to count a specific type of code.

Definition 12.64. A code $C \subseteq \Sigma^n$ with $|\Sigma| = q$ and $\text{mindist}(C) = d$ is *maximum distance separable*, abbreviated as *MDS*, if $|C| = q^{n-d+1}$, i.e., C meets the Singleton bound (Theorem 11.27).

Remark 12.65. If additionally, C is a linear $[n, k]$-code, then we have $q^k = q^{n-d+1}$, i.e., $k = n - d + 1 \Rightarrow d = n - k + 1$.

Definition 12.66. The *support* of a codeword x is $\text{supp}(x) = \{i : x_i \neq 0\}$.

Theorem 12.67. *Suppose $C \subseteq \mathbb{F}_q^n$ is an MDS $[n, k]$-code, then for each $i \geq d$, there are exactly $w_i = \binom{n}{i}(q-1)\sum_{j=0}^{i-d}(-1)^j\binom{i-1}{j}q^{i-j-d}$ codewords of weight i.*

Proof. We will invoke μ-inversion on poset $(\mathcal{P}([n]), \subseteq)$, for each $A \subseteq [n]$, we define $f(A), g(A)$ by $f(A) = |\{x \in C : \text{supp}(x) = A\}|, g(A) = |\{x \in C : \text{supp}(x) \subseteq A\}|$. Note that $g(A) = \sum_{B \subseteq A} f(B) = \sum_B f(B)\zeta(B, A)$.

Proposition 12.68.

$$g(A) = \begin{cases} 1, & \text{if } |A| < d \\ q^{|A|-d+1}, & \text{else} \end{cases}$$

Proof of Claim. Consider two cases.

Case 1 $|A| < d$, the only codeword with weight $< d$ is $\vec{0}$.

Case 2 $|A| \geq d$. Consider the subspace $D \subseteq C$, $D = \{x \in C : \text{supp}(x) \subseteq A\}$, notice D is the intersection of a k-dimensional subspace C and a $|A|$-dimensional subspace $\{x \in \mathbb{F}_q^n : \text{supp}(x) \subseteq A\}$, so $\dim(D) \geq k + |A| - n = |A| - d + 1$. However, D has $\text{mindist}(D) = d$, so $\dim(D) \leq |A| - d + 1$. This is because we can delete the coordinates outside A, where all codewords of D are 0, and apply the Singleton bound to D as a code of length $|A|$.

Thus, $g(A) = |D| = q^{|A|-d+1}$.

□

So μ-inversion says

$$\begin{aligned} f(A) &= \sum_B g(B)\mu(B,A) \\ &= \sum_{B\subseteq A} g(B)(-1)^{|A\setminus B|} \end{aligned}$$

Finally, we are ready to compute w_i. Below we use i to denote $|A|$ and j to denote $|B|$.

$$\begin{aligned} w_i &= \sum_{|A|=i} f(A) \\ &= \sum_{|A|=i}\sum_{B\subseteq A} g(B)(-1)^{|A\setminus B|} \\ &= \binom{n}{i}[\sum_{j=0}^{d-1}\binom{i}{j}(-1)^{i-j} + \sum_{j=d}^{i}\binom{i}{j}q^{j-d+1}(-1)^{i-j}] \\ &= \binom{n}{i}[-\sum_{j=d}^{i}\binom{i}{j}(-1)^{i-j} + \sum_{j=d}^{i}\binom{i}{j}q^{j-d+1}(-1)^{i-j}] \quad \text{since } 0 = \sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j} \\ &= \binom{n}{i}\sum_{j=d}^{i}(-1)^{i-j}\binom{i}{j}(q^{j-d+1}-1) \\ &= \binom{n}{i}(q-1)\sum_{j=d}^{i}(-1)^{i-j}\binom{i}{j}(\sum_{e=0}^{j-d}q^e) \quad \text{since } q^{j-d+1}-1 = (q-1)(\sum_{e=0}^{j-d}q^e) \end{aligned}$$

Then, we manipulate a bit by

- $j \leftrightarrow i-j$
- $\binom{i}{j} - \binom{i-1}{j-1} = \binom{i-1}{j}$

Then we get desired result,

$$\binom{n}{i}(q-1)\sum_{j=0}^{i-d}(-1)^j\binom{i-1}{j}q^{i-j-d}$$

□

Corollary 12.69. *If $C \subseteq \mathbb{F}_q^n$ is an MDS $[n,k]$-code and $d < n$, then $q \geq d$.*

Proof. Since $n > d$, we can examine $w_{d+1} = \binom{n}{d+1}(q-1)\sum_{j=0}^{1}(-1)^j\binom{d}{j}q^{1-j} = \binom{n}{d+1}(q-1)(q-d)$, so $q - d \geq 0 \Rightarrow q \geq d$. □

Proposition 12.70. *In the subspace lattice of $V = \mathbb{F}_q^n$, we have $\mu(0,V) = (-1)^n q^{\binom{n}{2}}$.*

Proof. By induction on $\dim(V)$.

Base case is trivial, suppose $\dim(V) = 1$, then $\mu(0, V) = -1 = (-1)^1 q^{\binom{1}{2}}$.

For inductive step, assume $n \geq 1$, fix 1-d subspace $A \subseteq V$. By Trick 2, $\sum_{U \vee A = V} \mu(0, U) = 0$, then U is either V or U is $(n-1)$-dimensional and $A \not\subseteq U$, there are q^{n-1} such U. To see this, there are $\frac{q^n - 1}{q-1}$ subspaces of dimension $n-1$ (kernels of non-zero linear functionals, up to scalars), and $\frac{q^{n-1}-1}{q-1}$ of them contain A (from functionals vanishing on A), so the difference is q^{n-1}. Thus,

$$\begin{aligned}
\mu(0, V) &= - \sum_{\dim(U) = n-1, U \vee A = V} \mu(0, U) \\
&= -q^{n-1} \cdot (-1)^{n-1} \cdot q^{\binom{n-1}{2}} && \text{by inductive hypothesis} \\
&= (-1)^n q^{\binom{n}{2}}
\end{aligned}$$

□

13 Advanced Topics on Graphs

In this section, we demonstrate some advanced topics on graphs, especially concerning counting of graphs.

Recall Theorem 1.25, there are n^{n-2} labeled trees on $[n]$.

We ask further: how many connected labeled graphs on $[n]$? This number is between n^{n-2} and $2^{\binom{n}{2}}$. The second number is the total number of graphs on n vertices.

With each partition $\mathcal{P} \in \Pi_n$, let $f(\mathcal{P})$ count the number of graphs whose connected components are exactly $\mathcal{P}$, $g(\mathcal{P})$ count number of graphs whose connected components refine $\mathcal{P}$, so $g(\mathcal{P}) = \sum_{\mathcal{Q} \subseteq \mathcal{P}} f(\mathcal{Q}) = \sum_{\mathcal{Q}} \zeta(\mathcal{Q}, \mathcal{P}) f(\mathcal{Q})$.

We want to evaluate $f(1_{\Pi_n}) = \sum_{\mathcal{Q}} g(\mathcal{Q}) \mu(\mathcal{Q}, 1_{\Pi_n})$.

Proposition 13.1. *Suppose parts of $\mathcal{P}$ are $A_1, \dots, A_k$, and $g(\mathcal{P})$ counts graphs with no edge between $A_i, A_j, i \neq j$, then*

$$g(\mathcal{P}) = 2^{\binom{|A_1|}{2}} \cdots 2^{\binom{|A_k|}{2}} = 2^{k_2\binom{2}{2}} 2^{k_3\binom{3}{2}} \cdots 2^{k_n\binom{n}{2}}$$

where k_i = number of parts of size i. This further indicates that

$$f(1_{\Pi_n}) = \sum_{\vec{k}:\, k_1 + 2k_2 + \cdots + nk_n = n} (-1)^{m-1} \frac{n!\,(m-1)!}{(1!)^{k_1} k_1! \cdots (n!)^{k_n} k_n!} \cdot 2^{k_2\binom{2}{2} + \cdots + k_n\binom{n}{2}},$$

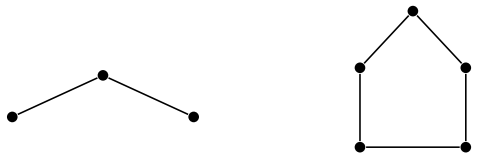
where $m = k_1 + \cdots + k_n$.

For the second formula: there are $\frac{n!}{(1!)^{k_1} k_1! \cdots (n!)^{k_n} k_n!}$ partitions $\mathcal{Q}$ with k_i parts of size i, and for each of them $\mu(\mathcal{Q}, 1_{\Pi_n}) = (-1)^{m-1}(m-1)!$, since the interval $[\mathcal{Q}, 1_{\Pi_n}]$ is isomorphic to Π_m, and in Π_m the previous section gives $\mu(\Delta, 1_{\Pi_m}) = s(m,1) = (-1)^{m-1}(m-1)!$.

Definition 13.2. A graph G with $|V| > k$ is called *k-connected* if $\forall A \subseteq V$ with $|A| < k$, $G \restriction (V \setminus A)$ is connected.

So vacuously, G is 1-connected if and only if G is connected.

Example 13.3. Consider the following two graphs:



not 2-connected 2-connected

Proposition 13.4. *G is 2-connected if and only if $|V| \geq 3$ and any two vertices lie on a cycle.*

Theorem 13.5 (Whitney)**.** *Suppose G is finite and simple, $|V| > k$, then G is k-connected if and only if $\forall x \neq y$, $\exists$ k disjoint paths $p_1, \dots, p_k$, such that $x - p_i - y$ is also a path.*

Proof Sketch. We sketch out a proof for necessity and sufficiency.

($\Leftarrow$) : Suppose $|A| < k$, we need to show that $G \restriction (V \setminus A)$ is connected. Fix $x \neq y \in V \setminus A$, by our hypothesis, there are k disjoint paths $p_1, \dots, p_k$ from x to y, so $\exists i \leq k$ such that $A \cap p_i = \emptyset$, so $x - p_i - y$ is a $G \restriction (V \setminus A)$ path, x and y are still connected.

($\Rightarrow$) : The proof is similar to Theorem 6.22 by using a maxflow-mincut argument. A hint is for each $v \in V$, build v_1, v_2 such that if $\{u, v\}$ is an edge, then in the new graph, we have edges $(u_1, u_2), (u_2, v_1), (v_1, v_2)$. By Theorem 6.22, cut is equivalent to disconnection. □

We introduce the *topological method* below. The motivation is G will be finite but not simple, in general.

Definition 13.6. Let G be a graph and e be an edge with two endpoints u, v, the *contraction* of e from G is a new graph G', with a super-vertex w that represents both u and v, all edges other than e incident to u or v are re-routed to w. We use G/e to denote contracting e from G. We also use $G - e$ to denote the graph yielded by deleting e from G.

Proposition 13.7. *Recall that $\chi_G(x)$ counts the number of proper colorings $c : V \to x$. Then*

$$\chi_G = \chi_{G-e} - \chi_{G/e}$$

Proof. It suffices to show $\chi_{G-e} = \chi_G + \chi_{G/e}$, i.e., each proper coloring of $G - e$ is either counted by G or G/e. Fix a coloring c of $G - e$, we case on whether its two endpoints u, v get the same color.

Case 1 Suppose u, v get the same color, then it corresponds to exactly one coloring of G/e: we simply view u, v as one vertex. More formally, the corresponding coloring c' on G/e is defined as

$$c'(a) = \begin{cases} c(u), & \text{if } a = w \\ c(a), & \text{else} \end{cases}$$

Case 2 Suppose u, v get different colors, then it corresponds to exactly one coloring of G, since adding back the edge e still preserves the validity of the coloring c. More formally, the corresponding coloring c' on G is exactly c.

On the other hand, each proper coloring of G is a proper coloring of $G - e$ in which u, v get different colors, and each proper coloring c' of G/e comes from the proper coloring of $G - e$ given by $c(u) = c(v) = c'(w)$ and $c(a) = c'(a)$ otherwise. So both correspondences are bijections, and $\chi_{G-e} = \chi_G + \chi_{G/e}$. □

Definition 13.8. An *orientation* of G is a digraph D such that each D-edge corresponds to exactly one G-edge, and vice versa.

Definition 13.9. An orientation is *acyclic* if and only if it has no directed cycles.

Theorem 13.10 (Stanley)**.** *If G is a graph on n vertices, let $\omega(G) := |\{\text{acyclic orientations of } G\}|$, then $\omega(G) = (-1)^n \chi_G(-1)$.*

Proof. By induction on $|E|$.

Base case: $|E| = 0$, we have $\chi_G(x) = x^n$, also,

$$\begin{aligned} \omega(G) &= 1 \\ (-1)^n \chi_G(-1) &= (-1)^n (-1)^n \\ &= (-1)^{2n} \\ &= 1 \end{aligned}$$

Inductive step: if G has a loop, both sides are 0, since a loop is a directed cycle in every orientation and no coloring is proper. So assume G has no loops. It suffices to show for each G-edge e:

$$\omega(G) = \omega(G - e) + \omega(G/e)$$

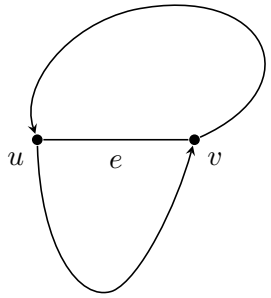
since then

$$\begin{aligned}\omega(G) &= (-1)^n \chi_{G-e}(-1) + (-1)^{n-1}\chi_{G/e}(-1) \\ &= (-1)^n(\chi_{G-e}(-1) - \chi_{G/e}(-1)) \\ &= (-1)^n \chi_G(-1)\end{aligned}$$

We need two subclaims to finish the proof.

Proposition 13.11 (Subclaim 1)**.** *Each acyclic orientation of $G - e$ extends to at least one acyclic orientation of G.*

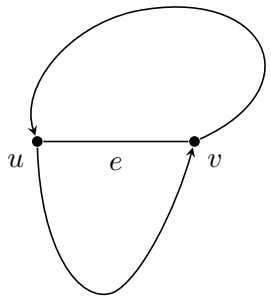
Proof of Subclaim 1. Adding back e, we claim at least one of (u, v) and (v, u) will work. Suppose otherwise, none of them work, then it must be the case that



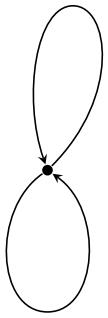
i.e., $G - e$ has a directed path from v to u and one from u to v, which together contain a directed cycle, contradicting that the original orientation is acyclic. □

Proposition 13.12 (Subclaim 2)**.** *An acyclic orientation of $G - e$ extends to two acyclic orientations of G if and only if it is an acyclic orientation of G/e.*

Proof of Subclaim 2. Notice we can extend to two acyclic orientations if and only if none of



occurs, so after contraction, none of



will occur. Thus, the orientation is acyclic on G/e, since directed cycles avoiding w are the same in $G-e$ and G/e. On the other hand, if it is acyclic on G/e, then $G-e$ has no directed path between u and v, since such a path would become a directed cycle through w in G/e. So both orientations of e work. □

Notice that by Subclaims 1 and 2, we have completed the proof, since each orientation of G can be viewed as an extension of an orientation of $G-e$, moreover, if a pair of orientations of G comes from the same orientation of $G-e$, we can assign one of them to be matched with the orientation of $G-e$, the other with the orientation of G/e. □

In the next part, we present an interesting result that corresponds to graph theory, theoretical computer science and proof theory.

Definition 13.13. Given two finite graphs G, H, we say that G is a *minor* of H if there is a finite sequence of moves:

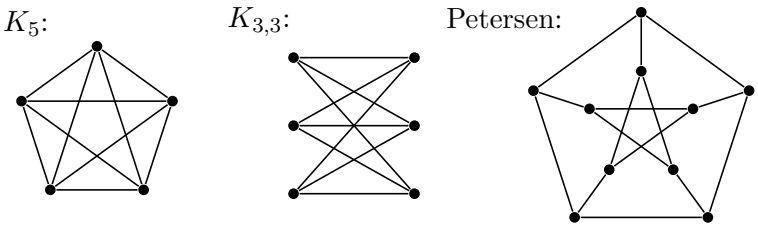
1. Delete an edge
2. Delete an (isolated) vertex
3. Contract a (non-loop) edge

applied to H, yielding a graph $G' \cong G$.

Example 13.14. Consider the following graphs:



Example 13.15. Consider the following graphs $K_5, K_{3,3}$ and the Petersen graph:

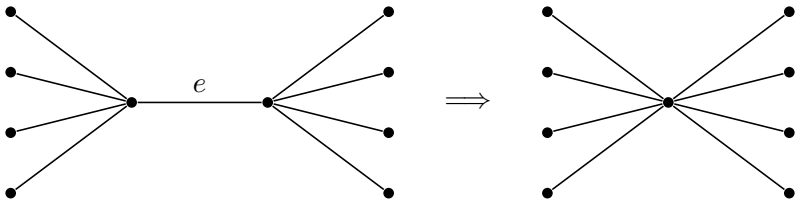


Both of K_5 and $K_{3,3}$ are minors of the Petersen graph.

Definition 13.16. A graph G is *planar* if it can be drawn on a surface with no overlapping edges.

Proposition 13.17. *If H is planar on surface S and G is a minor of H, then G is also planar on S.*

Proof. We check that planarity is stable under three moves: For deleting edge and vertex, we just don't draw it, so it does not affect planarity. For contracting an edge, it looks like:



Also does not affect planarity. □

Example 13.18. $K_{3,3}$ is not planar on the plane, but is planar on a *torus*.

Definition 13.19. A transitive relation on set X, denoted by $\leq$, is a *well-quasi-order (WQO)* if there is no infinite "decreasing or incomparable" sequence, i.e., for every sequence $x_1, x_2, x_3, \ldots \in X, \exists i < j$ with $x_i \leq x_j$.

Theorem 13.20 (Robertson–Seymour)**.** *The binary relation R on family of finite graphs $\mathcal{G}$, such that $G, H \in \mathcal{G}$ with $(G, H) \in R$ if and only if G is a minor of H, is a WQO on $\mathcal{G}$.*

Proposition 13.21. *Suppose $(X, \leq)$ is WQO and $A \subseteq X, A \neq X$ satisfying $(y \in A \wedge x \leq y) \Rightarrow x \in A$, then there is a finite set $F \subseteq X$ such that $x \notin A$ if and only if $\exists f \in F, f \leq x$.*

Proof. Suppose there is no such F. We will construct a sequence that contradicts WQO.

- At stage 0, fix some $f_0 \notin A$.
- At stage n, we have $f_0, \ldots, f_n \notin A$ such that $f_i \not\leq f_j, \forall i < j \leq n$, pick $f_{n+1} \notin A$ such that $\forall i \leq n, f_i \not\leq f_{n+1}$. Such f_{n+1} exists: since A is closed downward, every x with some $f_i \leq x$ is outside A, so if every $x \notin A$ had some $f_i \leq x$, then $F = \{f_0, \ldots, f_n\}$ would work.

The resulting sequence $(f_n)_{n \in \mathbb{N}}$ contradicts WQO. □

If we consider $A = \{\text{graphs planar on } S\}$, Theorem 13.20 and the two propositions above imply there is a finite family $\mathcal{F}$ of graphs such that H cannot be planar on S if and only if $\exists G \in \mathcal{F}$, G is a minor of H.

Example 13.22. H is not planar on the plane if and only if H has either K_5 or $K_{3,3}$ as a minor.

Example 13.23. Any finite set detecting non-planarity on the torus has at least 16000 graphs.

This leads to an infamous result on theoretical computer science: From a *Logic* perspective, Theorem 13.20 yields, for each surface S, a polynomial time algorithm for detecting planarity on S.

Problem 1: Nobody knows such an algorithm for interesting and complicated S.
Problem 2: Theorem 13.20 is hard to prove, formally.

Next, we introduce some hierarchies in *Reverse math of* $\mathbb{N}$:

- RCA_0: all decidable sets.
- WKL_0: decidable sets with some Kőnig's lemma.
- ACA_0: general arithmetic. Theorem 2.12 can be proved at this level.
- ATR_0: transfinite induction/recursion on countable ordinals.
- Π^1_1-CA: it can be described as "ATR_0+ more Kőnig's lemma".

Theorem 13.24 (H. Friedman, Robertson–Seymour)**.** *None of the above suffices to prove Theorem 13.20.*