MATH 5370: COMBINATORICS

HEESUNG YANG

1. Section 3.1: Pigeonhole principle

Theorem 1.1 (Pigeonhole principle)**.** *If $n+1$ objects are distributed into n boxes, then at least one box contains two or more objects.*

Proof. Do we need one? ;) □

Remark. Note that the pigeonhole principle is non-constructive: we don't know which box has more than one object.

Example. If you have 7 green socks and 3 yellow socks in the dryer, then if you remove 3 socks you must have a pair.

Example. If there are n couples, how many of the $2n$ people must you select to guarantee you get a couple? You need to choose $n+1$.

We introduce two other related principles:

Theorem 1.2. *If n objects are placed into n boxes with no box empty, then every box contains exactly one object.*

Theorem 1.3. *If n objects are placed into n boxes with no box containing more than one, then every box contains exactly one object.*

We can also re-formulate the pigeonhole principle using functions:

Theorem 1.4. *In terms of function $f : X \to Y$ where X and Y are finite:*

- *if $|Y| < |X|$, then f is not injective (one-to-one)*
- *if $|Y| = |X|$ then f is bijective (i.e., f is one-to-one/injective iff f is onto/surjective)*

Proposition 1.1. *Given m integers $a_1, \ldots, a_m$, there exist k and l with $0 \le k \le l \le m$ such that $a_{k+1} + a_{k+2} + \cdots + a_l$ is divisible by m.*

Proof. Consider $a_1, a_1+a_2, \ldots, a_1+a_2+\cdots+a_m$. This list contains m numbers. If m divides any of these, we are done. Otherwise, this means these all leave a remainder when divided by m, in the set $\{1, \ldots, m-1\}$. By the pigeonhole principle, there are two numbers, say $a_1 + \cdots + a_k, a_1 + \cdots + a_l$ that leave the same remainder (without loss of generality, assume $k < l$). Thus $(a_1 + \cdots + a_l) - (a_1 + \cdots + a_k) = a_{k+1} + \cdots + a_l$ divides m. This completes the proof. □

Date: 2 May 2019.

Example. If we choose 101 members from $1, 2, \ldots, 200$, then we want to prove that there are two (distinct two numbers, not two same numbers) such that one divides the other. To do so, we need to be a little more creative when it comes to building the boxes. To do so, we will write each member as $2^k \cdot a$ where a is odd. By the pigeonhole principle, there must be two of the 101 members with the same odd part, say $2^k a$ and $2^l a$ for some odd a. If $k = l$ then they have to be the same, so without loss of generality assume $k < l$. Now it follows that $2^k a \mid 2^l a$, so we are done.

Theorem 1.5. *A rational number a/b has a decimal expansion that eventually repeats.*

Proof. Note that there are infinitely many pigeons (the numbers in the decimal expansion) while there are finitely many boxes (available remainders, i.e., $\{0, 1, \ldots, b-1\}$), so at some point the expansion has to repeat. □

2. Section 3.2: Pigeonhole principle (strong form)

Theorem 2.1 (Strong pigeonhole principle)**.** *Let $q_1, \ldots, q_n$ be positive integers. If $q_1 + q_2 + \cdots + q_n - (n-1)$ objects are distributed into n boxes, then either:*

- *Box 1 contains at least q_1 objects; or*
- *Box 2 contains at least q_2 objects; or*
- *...*
- *Box n contains at least q_n objects.*

Proof. Suppose that none of the statement holds. Then for each $1 \leq i \leq n$, Box i contains at most $q_i - 1$ objects. This means that we distributed $q_1 + \cdots + q_n - n$ objects, but this is a contradiction (1 fewer than what we started with). □

Corollary 2.1. *Let n, r be positive integers. If $n(r-1)+1$ objects are distributed into n boxes, at least one box has $r = \underbrace{\left\lceil \frac{n(r-1)+1}{n} \right\rceil}_{average}$ objects.*

Example. A basket of fruit is arranged out of apples, bananas, and oranges. What is the smallest number of pieces of fruit that should be put into the basket to guarantee that either there is at least 7 apples, or 9 bananas, or 12 oranges? The answer is 7+9+12-(3-1)=26.

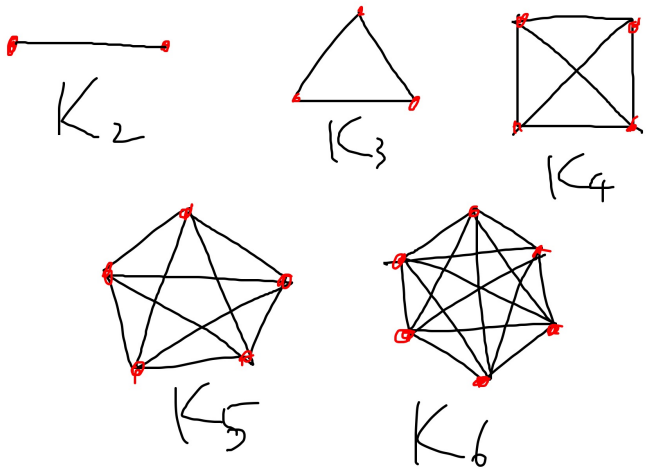
Example. Imagine a spinner with 200 divisions that has the inner wheel and the outer wheel. For the inner spinner, you can colour each red or blue. For the outer wheel, you can colour red or blue, but each must have 100. We claim that there is a rotation of the inner disc with at least 100 matches (with the outer wheel colouring).
Solution: If we fix the position of the outer disc, then there are 200 positions for the smaller disc. For each, count the number of matches. If each sector matches exactly 100 times, then the total number of matches is $200 \cdot 100 = 20000$. And there are 200 "boxes" (available positions). Thus, by Corollary 2.1 above, one of the rotations must have at least $\lceil 20000/200 \rceil = 100$ matches.

Theorem 2.2 (Erdős & Szekeres)**.** *Every sequence $a_1, \ldots, a_{n^2+1}$ of n^2 real numbers contain either an increasing subsequence of length $n+1$ or a decreasing subsequence of length $n+1$.*

Proof. For $k = 1, \ldots, n^2 + 1$, let m_k be the length of a longest increasing subsequence that begins at a_k. If any $m_k \geq n + 1$, then we're done, so assume that is not. That is, assume that $1 \leq m_k \leq n$. Now by Theorem 2.1, there must be $n + 1$ of these that have the same length, i.e., $m_{k_1} = m_{k_2} = \cdots = m_{k_{n+1}}$ (without loss of generality, assume $1 \leq k_1 < k_2 < \cdots < k_{n+1} \leq n^2 + 1$). [ugh, re-read this proof and finish writing this up] □

3. September 11: Introduction to graph theory

We start off with some examples of complete graphs:



Can we colour the edges of K_4 so that there is no triangle whose edges are of the same colour? What about K_5 and K_6? Ramsey's theorem answers this question.In fact, for any K_n where $n \geq 6$, then this cannot be done.

Theorem 3.1 (Ramsey's theorem)**.** *Of* 6 *or more people, either* 3 *mutual people are acquaintances, or* 3 *people are mutual strangers. In other words, no matter how edges of* K_n *are coloured (red or blue), there exists a red triangle or a blue triangle), for all* $n \geq 6$.

Theorem 3.2 (Ramsey's theorem, generalized)**.** *If* $m \geq 2$ *and* $n \geq 2$ *are integers, there exists a positive integer* p *such that* K_p *can be broken down into* K_m *and* K_n *(i.e.* $K_p \to K_m, K_n$*), where* K_m *(resp.* K_n*) denotes the complete graph with* m *vertices coloured all red (resp. blue) edges.*

Definition 3.1. We define *Ramsey's number* $r(m, n)$ to be the smallest integer p that satisfies $K_p \to K_m, K_n$.

Remark. Some properties of Ramsey numbers:

- $r(m, n) = r(n, m)$
- $r(m, 2) = r(2, m) = m$
- $r(3, 3) = 6$.

Proof. First we will show that $r(m, n) \leq r(m - 1, n) + r(m, n - 1)$. That is, show that $K_{r(m-1,n)+r(m,n-1)} \to K_m, K_n$. Assume that $n, m \geq 3$. Suppose we have coloured edges of

K_p where $p = r(m-1,n)+r(m,n-1)$, which we know exist by induction. Pick a vertex v_x and consider edges out of it to the rest. Put each remaining vertex into R_x if coloured red, and B_x if coloured blue. Then we have $|R_x|+|B_x| = p-1 = r(m-1,n)+r(m,n-1)-1$. By the pigeonhole principle, either $|R_x| \geq r(m-1,n)$ or $|B_x| \geq r(m,n-1)$.

(1) If $|R_x| \geq r(m-1,n)$ then in R_x either there is a red K_{m-1} or there is a blue K_n. Note that, the red K_{m-1} together with v_x is a K_m.
(2) If $|B_x| \geq r(m,n-1)$ then in B_x either there is a red K_m or there is a blue K_{n-1} (so together with v_x we have a blue K_n).

In either case we have $K_p \to K_m, K_n$, so such p exists and $p \leq r(m-1,n)+r(m,n-1)$. □

Remark. There are extensions to more than two colours (e.g., $r(3,3,3) = 1$).

Can we prove by induction that

$$r(m,n) \leq \binom{m+n-2}{m-1}?$$

What do we know about $r(m,n)$?

Theorem 3.3 (Erdős)**.** *$r(n,n) > 2^{(n-1)/2}$ for all $n \geq 3$.*

Proof. Take K_N where $N = \left\lfloor 2^{\frac{n-1}{2}} \right\rfloor$ and consider a random colouring of edges, red or blue. For $F \subseteq V(K_n)$, let E_S be event that S is either all red or all blue. Then the probability of E_s is

$$\Pr(E_s) = 2 \cdot \frac{1}{2^{\binom{n}{2}}}.$$

Thus the probability that some subset of n vertices is monochromatic is (call this event E_{mono})

$$\begin{aligned}\Pr(E_{\text{mono}}) = \Pr\left(\bigcup_S E_s\right) \leq \sum_S \Pr(E_s) &= \binom{N}{n} 2 \cdot \frac{1}{2^{\binom{n}{2}}} \\ &\leq \frac{N^n}{n!} 2 \cdot \frac{1}{2^{\binom{n}{2}}} \\ &\leq \frac{2^{n(n-1)/2}}{n!} 2 \cdot \frac{1}{2^{\binom{n}{2}}} = \frac{2}{n!} < 1.\end{aligned}$$

This implies that it is possible that all subsets of n vertices is not monochromatic. So there exists a 2-colouring of K_n with red or blue K_n. □

4. September 11: Partial ordering and equivalence relations

Definition 4.1. A relation R on a set X is a *partial ordering* or a *partial order* on X if the following three conditions are satisfied:

(i) (reflexivity) xRx for all $x \in X$
(ii) (anti-symmetry) for any $x, y \in X$, if xRy and yRx, then $x = y$
(iii) (transitivity) for all $x, y, z \in X$, if xRy and yRz, then xRz.

Definition 4.2. A relation R on X is said to be a *strict partial ordering* or a *strict partial order* if reflexivity in the above definition is replaced with irreflexivity, i.e., $x \not R x$ for all $x \in X$.

Example. $(X, \mathcal{P}(X))$ under $\subseteq$ is a partial ordering. If $\subseteq$ is replaced with $\subsetneq$, then it becomes to a strict partial ordering. $(\mathbb{N}, |)$ is a partial ordering, where $|$ denotes divisibility. $(\mathbb{R}, \leq)$ is a partial ordering, whereas $(\mathbb{R}, <)$ is a strict partial ordering.

Remark. We often denote a partial ordering (resp. a strict partial ordering) by "$\leq$" (resp. "$<$").

Remark. Given a partial order $\leq$, setting $x < y$ iff $x \leq y$ and $x \neq y$ yields a strict partial order. Similarly, given a strict partial order under $<$, setting $x \leq y$ iff $x < y$ or $x = y$ yields a partial order.

Definition 4.3. A set X on which a partial order $\leq$ is defined is called a *partially ordered set (poset)*. If R is a relation on X, then x and y are *comparable* if xRy or yRx; otherwise, they are *incomparable*. If every pair of a partial order R on set X is comparable, then R is said to be a *total ordering* or a *total order*.

Example. $(\mathbb{R}, \leq)$ is a total order, whereas $(\mathbb{N}, |)$ is not.

Theorem 4.1. *Let X be a* finite *set with n elements. Then there is a one-to-one correspondence between the total orders on X and the permutation of X. Therefore, the number of total orders on X is $n!$.*

First we prove the following lemma first.

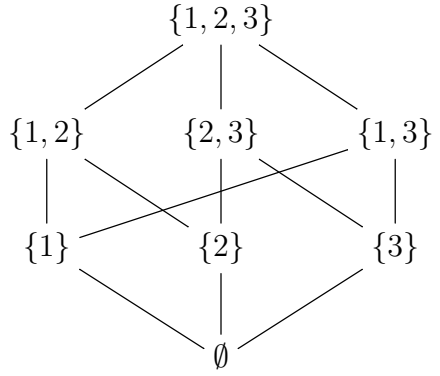
Lemma 4.1. *Given a total order on X where X is a* finite *set with n elements, there exists a permutation $a_1, a_2, \ldots, a_n$ on X such that $a_1 < a_2 < \cdots < a_n$.*

Proof of Lemma 4.1. If $n = 1$, then this is trivial. Next, show that there exists a minimal element (which we can do because X is finite – this is why the finiteness condition is crucial here) so that $a_1 < x$ for all $x \in X \setminus \{a_1\}$. Repeat this operation, and the lemma follows by induction. □

Proof of Theorem 4.1. Define $a_i \leq a_j$, provided that a_i comes before a_j in the permutation. This automatically makes $\leq$ a total order on R. This proves that we can construct a total order from the permutation. The other direction follows immediately from Lemma 4.1. □

Definition 4.4. We say that x *is covered by* y or y *covers* x if $x < y$ and there is no z such that $x < z < y$. We write this as $x <_c y$. In other words, if a finite poset is represented geometrically (with a Hasse diagram), and if $x <_c y$, then x is below y, and there is a direct line form x to y.

Example. $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{3,1\}, \{1,2,3\}\}$ with a partial order $\subseteq$. Then its Hasse diagram is



Definition 4.5. A *linear extension* $(X, \leq_2)$ of a poset $(X, \leq_1)$ is a poset such that $\leq_2 \supseteq \leq_1$ and $\leq_2$ is a total order.

Theorem 4.2. *Let $(X, \leq)$ be a finite poset. Then there is a linear extension of $(X, \leq)$.*

Example. $(\{1, \ldots, n\}, \leq)$ is a linear extension of $(\{1, \ldots, n\}, |)$.

5. September 13: Equivalence relation

Definition 5.1. Let X be a set. A relation R on X is an *equivalence relation* provided that it is:

- reflexive;
- symmetric: for all x and y, if xRy, then yRx; and
- transitive.

Equivalence relations are often written as $\sim$. We denote the equivalence class of a as $[a] = \{x : x \sim a\}$.

Remark. $\sim$ is the generalization of $=$.

Theorem 5.1. *Let $\sim$ be an equivalence relation on X. Then the distinct equivalence classes partition R into non-empty parts. Conversely, given any partition of X into nonempty parts, there is an equivalence relation on X whose equivalence classes are the parts of the partition.*

Proof. Suppose that $c \in [a] \cap [b]$. Then since $c \sim a$, via symmetry we have $a \sim c$. Thus we have $a \sim c$ and $c \sim b$, by transitivity $a \sim b$. Therefore $[a] = [b]$. Conversely, suppose that there is a partition of X. Then let $\sim$ be a relation such that $x \sim y$ whenever x and y belong to the same partition. It is a standard exercise to verify that $\sim$ is an equivalence relation. □

Remark. Therefore, equivalence relations and partitions are two different ways of talking about the same concept.

Example. Let S_n be the set of all $n!$ permutations of $1, 2, \ldots, n$. Define R by $i_1, \ldots, i_n R j_1, \ldots, j_n$ whenever there is an integer k such that $j_1 \ldots j_n = i_k \cdots i_n i_1 \cdots i_{k-1}$. So we have $23451R45123$. Similarly we have $45123R34512$ and $23451R34512$. Thus $[23451] = \{34512, 45123, 51234, 12345\}$. In general, every class contains exactly n objects. So there are $n!/n = (n-1)!$ equivalence classes.

Example. Take all permutations of $1, 2, \ldots, n$. Define $i_1 \ldots i_k \sim j_1 \ldots j_k$ iff $\{i_1, \ldots, i_k\} = \{j_1, \ldots, j_k\}$. Then $[i_1 i_2 \ldots i_k] = \{$all permutation with the same elements $i_1, \ldots, i_k\}$. Note that the size of each equivalence class is $k!$. What about the number of equivalence classes? This is equal to the number of ways to choose k elements from $1, \ldots, n$. Thus there are $P(n,k)/k! = n!/((n-k)!k!) = \binom{n}{k}$ equivalence classes.

Example (Row reduction on $n \times m$ matrices). Let $A \sim B$ iff A is row-equivalent to B.

Example. On $\mathbb{Z}$, let $a \, R_n \, b$ if and only if $n \mid (a-b)$. The equivalent way of putting aR_nb in this case is $a \equiv b \pmod{n}$ (the classes mod n).

6. September 13: Chapter V - Binomial Coefficients

Definition 6.1. Define the *binomial coefficient* $\binom{n}{k}$ as

$$\binom{n}{k} := \begin{cases} 0 & \text{if } n < k; \\ 1 & \text{if } k = 0; \\ C(n,k) = \frac{n!}{k!(n-k)!} & \text{otherwise.} \end{cases}$$

Proposition 6.1. $\binom{n}{k} = \binom{n}{n-k}$ *for any* $0 \le k \le n$.

Proposition 6.2 (Pascal's formula)**.** $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

n \ k	0	1	2	3	4	$\cdots$
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	

The above is called Pascal's triangle, which illustrates Pascal's formula.

Proposition 6.3. $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

Proof. The left-hand side denotes the number of ways to choose objects from n objects (how many ways can you choose 0 objects? what about 1? and so forth). On the other hand, the right-hand side denotes how many ways to choose objects from n objects also (For each object, you can choose or not choose - two options. There are n objects, so we have 2^n). $\square$

Definition 6.2. $\binom{n}{2} = \dfrac{n(n-1)}{2}$ is called a *triangular number.*

Theorem 6.1 (Binomial theorem)**.** $(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1}y^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$.

Corollary 6.1. $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k=0}^{n} \binom{n}{n-k} x^k$.

7. September 18

Proposition 7.1. $k\binom{n}{k} = n\binom{n-1}{k-1}$.

Proof. Both describe how many ways one can choose a committee of k members with one president amongst n people. The LHS describes how many ways one can choose k committee members, and then pick a president from that. As for the RHS, this is equivalent to choosing a president first, and then choosing the remaining $k-1$ members from the remaining $n-1$ people. □

Proposition 7.2. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0$ *for all* $n \geq 1$.

Proof. Let $x = -1$ where x is as it appears in Corollary 6.1. □

Proof. $\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n \cdot 2^{n-1}$ for all $n \geq 1$. □

Proof. Differentiate both sides of Corollary 6.1, and then let $x = 1$. Another way of looking at this is as follows: the RHS depicts the total number of ways to pick a committee (choose a chairman from n people; now pick the remaining member of the committee from $n-1$ people); the same goes for LHS also (sum up how many ways you can choose a committee of 1 members, 2 members, etc). Note that there are $\binom{n}{k}$ ways to choose a committee of k members, and there are therefore k ways of picking a chairman. □

Proposition 7.3. $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Proof. Each individual term of the LHS describes the following situation: choosing k people from the n people from the first den, and $n-k$ people for the n people in the second den (recall that $\binom{n}{k} = \binom{n}{n-k}$). This is equivalent to choosing how many ways you can choose n people amongst $2n$ people. □

8. September 18: Extended definition of binomial coefficients

Definition 8.1. Let r be any real and k any integer. Then

$$\binom{r}{k} := \begin{cases} \frac{r(r-1)(r-2)\cdots(n-k+1)}{k!} & (k \geq 1) \\ 1 & (k = 0) \\ 0 & (k \leq -1). \end{cases}$$

Example. $\binom{-7}{2} = \frac{(-7)(-7-1)}{2!} = 28.$

Example. $\binom{\frac{3}{2}}{3} = \frac{(-\frac{3}{2})(-\frac{3}{2}-1)(-\frac{3}{2}-2)}{3!} = -\frac{1}{16}.$

Proposition 8.1. *The following identities hold for any integer k and any real number r:*

(i) $\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}$

(ii) $k\binom{r}{k} = r\binom{r-1}{k-1}$.

Proposition 8.2. $\binom{r+k+1}{k} = \binom{r+k}{k} + \cdots + \binom{r+1}{1} + \binom{r}{0}$.

Proof. (i) can be proven via induction:

$$\begin{aligned}\binom{r}{k} &= \binom{r-1}{k} + \binom{r-1}{k-1} \\ &= \binom{r-1}{k} + \binom{r-2}{k-1} + \binom{r-2}{k-2} \\ &\vdots \\ &= \binom{r-1}{k} + \binom{r-2}{k-1} + \binom{r-3}{k-2} + \cdots + \binom{r-k}{1} + \binom{r-k-1}{0}.\end{aligned}$$

Substituting $r+k+1$ for r yields the claim. □

Proposition 8.3. *For all positive integers n and k,*

$$\binom{n+1}{k+1} = \binom{0}{k} + \binom{1}{k} + \cdots + \binom{n-1}{k} + \binom{n}{k}.$$

Corollary 8.1. $\dfrac{n(n+1)}{2} = \binom{n+1}{2} = \binom{0}{1} + \cdots + \binom{n}{1} = 1 + 2 + \cdots + n.$

9. September 18: Unimodality of binomial coefficients

Definition 9.1. The sequence $s_0, \ldots, s_n$ is *unimodal* if there is an integer t with $0 \le t \le n$ such that $s_0 \le s_1 \le \cdots \le s_t \ge s_{t+1} \ge \cdots \ge s_n$.

Example. $1, 4, 4, 2, 1$ is unimodal, but $1, 7, 8, 7, 9, 4$ is not.

Theorem 9.1. *Let n be a positive integer. Then $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ is unimodal. Moreover, if n is even, then*

$$\binom{n}{0} < \binom{n}{1} < \binom{n}{2} < \cdots < \binom{n}{n/2} > \binom{n}{n/2+1} > \cdots > \binom{n}{n-1} > \binom{n}{n}.$$

If n is odd, then there is a double peak:

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\frac{n-1}{2}} = \binom{n}{\frac{n+1}{2}} > \cdots > \binom{n}{n-1} > \binom{n}{n}.$$

Proof. Consider the following ratio:

$$\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{n!}{k!(n-k)!} \cdot \frac{(k-1)!(n-k+1)!}{n!} = \frac{n-k+1}{k}.$$

Therefore,

$$\binom{n}{k-1} < \binom{n}{k} \Leftrightarrow n-k+1 > k \Leftrightarrow k < \frac{n+1}{2}.$$

Similarly,

$$\binom{n}{k-1} = \binom{n}{k} \Leftrightarrow k = \frac{n+1}{2};$$
$$\binom{n}{k-1} > \binom{n}{k} \Leftrightarrow k > \frac{n+1}{2}.$$

So the equality (double peak) happens only when n is odd. □

Corollary 9.1. *The largest of* $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ *(where* n *is a positive integer) is* $\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$.

Definition 9.2. An *anti-chain* of a set S of size n is a collection $\mathfrak{A}$ of subsets of S such that no one is contained in another. Such collection is called a *Sperner family* or a *Sperner system*.

Remark. One can find anti-chains by choosing $k \in \{0, 1, \ldots, n\}$ and choose *all* subsets of S of size k. Then the size of this collection $\mathfrak{A}_k$ is $\binom{n}{k}$. Therefore $|\mathfrak{A}_k| \leq \max_k \binom{n}{k} = \binom{n}{\lfloor n/2 \rfloor}$.

10. September 20

Theorem 10.1. *Let* S *be a set of* n *elements. Then an anti-chain on* S *contains at most* $\binom{n}{\lfloor n/2 \rfloor}$ *sets.*

Definition 10.1. Define a *chain* $\mathfrak{C}$ of subsets: $A_1, A_2 \in \mathfrak{C} \Rightarrow A_1 \subset A_2$ or $A_2 \subset A$. A *maximal chain* is the one that cannot be made bigger.

Example. For $S = \{a, b, c, d, e\}$ and $\mathfrak{C} = \{\emptyset, \{a\}, \{a, c\}, \{a, c, d, e\}\}$, we see that $\mathfrak{C}$ is not maximal. However,

$$\{\emptyset, \{a\}, \{a, c\}, \{a, c, d\}, \{a, c, d, e\}, \{a, b, c, d, e\}\}$$

is maximal.

Remark. To construct a maximal chain $\mathfrak{C}$ of a set S (with $|S| = n$), order each element of S, and build a chain of subsets such that there is a one-to-one correspondence between $\mathfrak{C}$ and S. Therefore there are $n!$ maximal chains of S. Furthermore, any chain intersects any anti-chain in *at most* one set.

Proof of Theorem 10.1. Let $\mathfrak{A}$ be any anti-chain of S. Then define

$$\beta := \#\{(A, \mathfrak{C}) : A \in \mathfrak{A}, A \in \mathfrak{C}, \text{ and } \mathfrak{C} \text{ is a maximal chain of } S.\}.$$

We can count in two ways:

(1) $\beta \leq n!$ (At most one $A \in \mathfrak{A}$ is in an ordered pairs with a maximal chain $\mathfrak{C}$.)

(2) Define $\alpha_k := \#\{A \in \mathfrak{A} : \#A = k\}$. Then $\sum \alpha_k = |\mathfrak{A}|$. For a given $A \in \mathfrak{A}$ of size k, there are $k!(n-k)!$ maximal chains containing A.

Putting the two together, we see

$$\sum_{k=0}^{n} \alpha_k k!(n-k)! = \beta \leq n!$$

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

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

But then by unimodality, $\alpha_k/\binom{n}{k}$ becomes the smallest when $k = \lfloor n/2 \rfloor$. Hence it follows from the last inequality that

$$\sum_{k=0}^{n} \frac{\alpha_k}{\binom{n}{\lfloor n/2 \rfloor}} \leq 1.$$

Multiplying both sides by $\binom{n}{\lfloor n/2 \rfloor}$, and recognizing that $|\mathfrak{A}| = \sum_{k=0}^{n} \alpha_k$ yields the result. □

Definition 10.2. If $n_1, \ldots, n_t$ are non-negative integers with $n = n_1 + \cdots + n_t$, then

$$\binom{n}{n_1, \ldots, n_t} := \frac{n!}{n_1! n_2! \ldots n_t!}$$

is called a *generalized binomial coefficient*, or a *multinomial coefficient*.

Theorem 10.2. $(x_1 + \cdots + x_t)^n = \sum_{n_1 + \cdots + n_t = n} \binom{n}{n_1, \ldots, n_t} x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$.

11. September 20: More on posets (Section 5.6)

Definition 11.1. In a poset $(X, \preceq)$, an *anti-chain* A is a subset of X such that no pair of A are comparable (i.e., $x, y \in A, x \neq y \Rightarrow x \not\preceq y, y \not\preceq x$) A *chain* is a subset of X such that any pair of elements are comparable (i.e., $x, y \in C \Rightarrow x \preceq y$ and $y \preceq x$).

Remark. If A is an anti-chain, and C is a chain, then $\#(A \cap C) \leq 1$.

Theorem 11.1. *Let $(X, \preceq)$ be a finite poset, and let r be the largest size of a chain. Then X can be partitioned into r, but no fewer anti-chains.*

Proof. Suppose $X_1 \preceq X_2 \preceq \cdots \preceq X_r$ is a chain of the largest size, and suppose that there are fewer than r anti-chains. But if this is the case, by the pigeonhole principle, there exists at least one anti-chain containing two or more chains, which is a contradiction. Thus there has to be at least r anti-chains.

Look at the maximal elements M_1 (those that have no element above them, i.e., $x \in M_1, y \neq x \Rightarrow x \not\preceq y$). Then M_1 is an anti-chain. Now, consider $(X - M_1, \preceq)$. The size of the largest chain in $(X - M_1, \preceq)$ is $r - 1$. Then let M_2 be the maximal elements in $(X - M_1, \preceq)$. Continue on and on until you reach M_r, which consists of the remaining elements after repeating this operation. □

Theorem 11.2 (Dilworth's theorem)**.** *Let $(X, \preceq)$ be a finite poset, and let m be the largest size of an anti-chain. Then X can be partitioned into m but no fewer chains.*

Proof. Read up on the proof! (Possibly a midterm question!) □

12. September 25: Inclusion-exclusion principle (Chapter 6.1)

Theorem 12.1. *Let $P_1, \ldots, P_m$ be m properties referring to objects in S, and let*

$$A_i = \{x \mid x \in S \text{ has property } P_i\} \text{ for } i = 1, \ldots, m.$$

Then $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_m}| = |S| - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \cdots + (-1)^m |A_1 \cap A_2 \cap \cdots \cap A_m|$. *The alternate formulation is* $|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum |A_i| - \sum |A_i \cap A_j| + \sum |A_i \cap A_j \cap A_k| + \cdots + (-1)^{m-1} |A_1 \cap A_2 \cap \cdots \cap A_m|$.

Example. How many numbers between 1 and 1000 (inclusive) are *not* divisible by $5, 6$, and 8?
Solution: Let

$$A_1 := \{x \in \mathbb{N}_{1000} : 5 \,|\, x\} A_2 \qquad := \{x \in \mathbb{N}_{1000} : 6 \,|\, x\} A_3 := \{x \in \mathbb{N}_{1000} : 8 \,|\, x\}.$$

Note that $|A_1| = \lfloor 1000/5 \rfloor = 200, |A_2| = \lfloor 1000/6 \rfloor = 166, |A_3| = \lfloor 1000/8 \rfloor = 125, |A_1 \cap A_2| = \lfloor 1000/30 \rfloor = 33, |A_1 \cap A_3| = 25, |A_2 \cap A_3| = 41, |A_1 \cap A_2 \cap A_3| = \lfloor 1000/120 \rfloor = 8$. Therefore

$$|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| = 1000 - (200 + 166 + 126) + (33 + 25 + 41) - 8 = 600$$

out of 1000 numbers in $\{1, 2, \ldots, 1000\}$ are not divisible by 5, 6, and 8.

Example. How many permutations of $M, A, T, H, I, S, F, U, N$ are there so that none of the words MATH, IS, FUN appears?
Solution: There are total of 9! permutations. Now group each of the words, and treat it as one element. So there are 6! permutations containing MATH (permute MATH, I, S, F, U, N), 8! permutations containing IS, and 7! permutations containing FUN. Now, there are 5! permutations containing MATH and IS (MATH, IS, F, U, N); there are 4! permutations containing both MATH and FUN, and 6! permutations containing both IS and FUN. Finally, there are 3! ways to permute MATH, IS, FUN. Thus by inclusion-exclusion, we have

$$9! - (6! + 8! + 7!) + (5! + 4! + 6!) - 6 = 317658$$

permutations satisfying the desire property.

Example. How many integers between 0 and $99,999$ (inclusive) have $2, 5$, and 8 amongst their digits?
Solution: Let

$$\begin{aligned} S &:= \{0, 1, \ldots, 99999\} \\ A_1 &:= \{x \in S : 2 \text{ does not appear as a digit in } X\} \\ A_2 &:= \{x \in S : 5 \text{ does not appear as a digit in } X\} \\ A_3 &:= \{x \in S : 8 \text{ does not appear as a digit in } X\}. \end{aligned}$$

Then

$$\begin{aligned}|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| &= |S| - \sum |A_i| + \sum |A_i \cap A_j| - |A_1 \cap A_2 \cap A_3| \\ &= 100000 - \binom{3}{1}9^5 + \binom{3}{2}8^5 - 7^5 = 4350,\end{aligned}$$

so there are 4350 numbers that have 2, 5, and 8 amongst their digits.

13. September 25: Combinations with repetitions (Chapter 6.2

Read this section yourself.

Example. How many 10-combinations of the multiset $T := \{3 \cdot a, 4 \cdot b, 5 \cdot c\}$?

Example (Derangement). How many ways can you arrange n objects (say $1, 2, \ldots, n$) so that no object is in their correct/natural place? The following theorem answers this question.

Theorem 13.1. *Let D_n be the number of derangements of n objects. Then*

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n\frac{1}{n!}\right).$$

Proof. Let S be the set of all permutations of $\{1, \ldots, n\}$. Let P_j be the property such that j is in its natural position. Let $A_j := \{x \in S : x \text{ has property } P_j\}$. Then

$$\begin{aligned}D_n = |\overline{A_1} \cap \cdots \overline{A_n}| &= n! - \binom{n}{1}(n-1) + \binom{n}{2}(n-2)! + \cdots + (-1)^n\binom{n}{n} \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots + (-1)^n\frac{1}{n!} \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n\frac{1}{n!}\right).\end{aligned}$$

□

Recall from calculus that

$$e^{-x} = 1 - \frac{x}{1!} + \frac{x^2}{2!} - \cdots,$$

so

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots.$$

Therefore $e^{-1} \sim D_n/n!$, i.e., D_n is an integer closest to $n!/e$.

Proposition 13.1. *$D_n = (n-1)(D_{n-2} + D_{n-1})$ and $D_n = nD^{n-1} + (-1)^n$.*

Example. n men and n women bring coats to a dance. How many ways can the coats be returned with men getting men's coats, women getting women's coats, but no one gets the right coat?
Solution: No restrictions: $(2n)!$; men get men's coats, women get women's coats: $n! \times n!$; dearrangements: $D_n \times D_n$.

14. September 25 & 27: Recurrence relations and generating functions (Chapter 7)

Definition 14.1. A *recurrence relation* is one where current term (indexed by natural number n) is a function of the previous terms.

Example (Fibonacci sequence). Consider the sequence $(f_0, f_1, f_2, f_3, \dots) = (0, 1, 1, 2, 3, 5, \dots)$, i.e., $f_n = f_{n-1} + f_{n-2}$. Some interesting facts about Fibonacci:

(1) $s_n := f_0 + f_1 + \cdots + f_n = f_{n+2} - 1$
(2) f_n is even if and only if $3 \mid n$.

Can we solve for f_n explicitly? We can try solution of the form $f_n = q^n$ for some non-zero q. Then $f_n = f_{n-1} + f_{n-2}$ becomes $q^n = q^{n-1} + q^{n-2}$, so $q^{n-2}(q^2 - q - 1) = 0$. But since $q^{n-2} \neq 0$, indeed $q^2 - q - 1 = 0$. So $q = \frac{1 \pm \sqrt{5}}{2}$. So

$$f_n = \left(\frac{1 \pm \sqrt{5}}{2}\right)^n$$

are both solutions. As recurrence is linear and homogeneous,

$$f_n = c_1 + \left(\frac{1 + \sqrt{5}}{2}\right)^n + c_2 \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

is also a solution, for some c_1 and c_2 – note that they are determined by base conditions. Then you will get $(c_1, c_2) = (\sqrt{5}^{-1}, -\sqrt{5}^{-1})$. Thus the generating function for f_n is

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2}\right)^n \qquad (n \geq 0).$$

Fibonacci numbers shows up pretty often in mathematics. More examples:

Example. Let h_n be the number of ways to perfectly cover a $2 \times n$ board with dominoes. Then $h_1 = 1, h_2 = 2, h_3 = 3$, and $h_n = h_{n-1} + h_{n-2}$.

Definition 14.2. Given a sequence $h_0, h_1, \dots, h_n, \dots$, of numbers, its *generating function* is the infinite series

$$g(x) := h_0 + h_1 x + h_2 x^2 + \cdots .$$

So the coefficient of x^n in $g(x)$ is h_n.

Remark. If we have a finite sequence, then $g(x)$ is a polynomial.

Example. The generating function for $1, 1, 1, \dots$ is

$$g(x) = 1 + x + x^2 + \cdots = \frac{1}{1 - x}.$$

Example. The generating function for $\binom{m}{0}, \binom{m}{1}, \dots, \binom{m}{m}$ is

$$g(x) = \binom{m}{0} + \binom{m}{1} x + \cdots + \binom{m}{m} x^m = (1 + x)^m.$$

Example. Let K be an integer, and define sequence $h_0, \ldots, h_n, \ldots$ where

$$h_n := \binom{n+k-1}{k-1},$$

i.e., the number of non-negative integral solutions to $e_1 + \cdots + e_k = n$. Then the generating function is

$$g(x) = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^n = \frac{1}{(1-x)^k} = (1 + x + x^2 + \cdots)^k = \sum x^{e_1} \sum x^{e_2} \cdots \sum x^{e_k}.$$

Example. Determine the generating function for the number of n-combinations of apples, bananas, oranges, and pears where, in each n-combination, the number of apples is even, the number of bananas is odd, the number of oranges is between 0 and 4, and there is at least one pear.
Solution: The generating function is

$$\begin{aligned} g(x) &= \underbrace{(1 + x^2 + x^4 + x^6 + \cdots)}_{\text{even number of apples}} \underbrace{(x + x^3 + x^5 + \cdots)}_{\text{odd number of bananas}} \underbrace{(1 + x + x^2 + x^3 + x^4)}_{\text{between 0 and 4 oranges}} \underbrace{(x + x^2 + x^3 + \cdots)}_{\text{at least one pear}} \\ &= \frac{1}{1-x^2} \cdot \frac{x}{1-x^2} \cdot \frac{1-x^5}{1-x} \cdot \frac{x}{1-x} = \frac{x^2(1-x^5)}{(1-x)^2(1-x^2)^2}. \end{aligned}$$

Can someone use generating functions to solve a counting problem?

Example. Find the number h_n of bags of fruits that can be made out of apples, bananas, oranges, and pears, where, in each bag, the number of apples is even, the number of bananas is a multiple of 5, the number of oranges is at most 4, and the number of pears is 0 or 1.
Solution: Let $h(x)$ be the generating function, where

$$\begin{aligned} h(x) &= h_0 + h_1 x + h_2 x^2 + \cdots \\ &= (1 + x^2 + x^4 + \cdots)(1 + x^5 + x^{10} + \cdots)(1 + x + x^2 + x^3 + x^4)(1 + x) \\ &= \frac{1}{1-x^2} \cdot \frac{1}{1-x^5} \cdot \frac{1-x^5}{1-x} \cdot (1+x) = \frac{1}{1-x^2} = 1 + 2x + 3x^2 + \cdots + (n+1)x^n + \cdots. \end{aligned}$$

Thus $h_n = n + 1$.

Example. Let g_n be the number of non-negative integral solutions to

$$3e_1 + 4e_2 + 2e_3 + 5e_4 = n.$$

Find a generating function $g(x)$ for $g_0, g_1, g_2, \ldots, g_n, \ldots$.
Solution: $g(x) = (1 + x^3 + x^6 + \cdots)(1 + x^4 + x^8 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^5 + x^{10} + \cdots) = (1-x^3)^{-1}(1-x^4)^{-1}(1-x^2)^{-1}(1-x^5)^{-1}$.

Example. If you have an unlimited supply of pennies, nickels, dimes, quarters, and half-dollar coins, the generating function for f_n, the number of ways to make n cents with these coins, is $(1-x)^{-1}(1-x^5)^{-1}(1-x^{10})^{-1}(1-x^{25})^{-1}(1-x^{50})^{-1}$.

15. September 27: Solving linear homogeneous recurrence relations (Chapter 7.4; skip Chapter 7.3)

Definition 15.1. Let $h_0, h_1, \ldots, h_n, \ldots$ be a sequence of members. We say that the sequence *satisfies a linear recurrence relations of order k* if there exist scalars $a_1, \ldots, a_k, b_n$ such that

$$h_n = a_1 h_{n-1} + \cdots + a_k h_{n-k} + b_n \qquad (n \geq k). \tag{1}$$

Particularly, if $b_n = 0$, then the given linear recurrence relations is *homogeneous*.

Example. Let D_n be the number of derangements of n objects. Then $D_n = (n-1)D_n + (n-1)D_{n-2}$, which is a homogeneous linear recurrence relation of order 2.

We will learn how to solve linear homogeneous recurrence relations (LHRR) with constant coefficients. Rewrite (1) as

$$h_n - a_1 h_{n-1} - a_2 h_{n-2} - \cdots - a_k h_{n-k} = 0.$$

We start by looking at solutions ignoring the initial conditions.

Theorem 15.1. *Let q be a non-zero number. Then $h_n = q^n$ is a solution of the LHRR*

$$h_n - a_1 h_{n-1} - a_2 h_{n-2} - \cdots - a_k h_{n-k} = 0 (a_k \neq 0, n \geq k)$$

with constant coefficients if and only if q is a root of the polynomial equation

$$x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - a_k = 0.$$

If the polynomial equation has k distinct roots $q_1, \ldots, q_k$ (which we shall call characteristic roots*), then*

$$h_n = c_1 q_1^n + c_2 q_2^n + \cdots + c_k q_k^n \tag{2}$$

is the general solution of (1)*. Furthermore, no matter what initial values of $h_0, \ldots, h_{k-1}$ are given, there are $c_1, \ldots, c_k$ so that* (2) *is the* unique *sequence that satisfies both the recurrence relation and the initial values.*

Proof. This is Theorem 7.4.1 of the text. □

Example. Solve $h_n = 2h_{n-1} + h_{h-2} - 2h_{h-3} (n \geq 3)$ with initial values $h_0 = 1, h_1 = 2, h_2 = 0$.
Solution: Characteristic equation is $x^3 - 2x^2 - x + 2 = 0$, and its roots are $q_1 = 1, q_2 = -1, q_3 = 2$. Thus the general solution is

$$h_n = c_1(1)^n + c_2(-1)^n + c_3(2)^n = c_1 + c_2(-1)^n + c_3 2^n.$$

Now solve for initial values, i.e.,

$$\begin{aligned} c_1 + c_2 + c_3 &= 1 \quad (n = 0) \\ c_1 - c_2 + 2c_3 &= 2 \quad (n = 1) \\ c_1 + c_2 + 4c_3 &= 0 \quad (n = 2). \end{aligned}$$

Solving this will yield the solution $(c_1, c_2, c_3) = (2, -\frac{2}{3}, -\frac{1}{3})$. So the solution is

$$h_n = 2 - \frac{2}{3}(-1)^n - \frac{1}{3}2^n.$$

Example. Words of length n using only the letters a, b, and c are to be transmitted with the condition that no word with two consecutive a's are to be transmitted. Determine the number of all words allowed.
Solution: Let h_n be the number of words allowed of length n. Then $h_0 = 1, h_1 = 3$ for $n \geq 2$. Then the LHRR is

$$h_n = 2h_{n-1} + 2h_{n-2}.$$

The first 2 comes covers the case when a word starts with a b or a c. The second 2 covers any words starting with a (since the second letter must be b or c). So the characteristic equation is $x^2 - 2x - 2 = 0$, so $x = 1 \pm \sqrt{3}$. Now we need to solve for c_1 and c_2, where

$$h_n = c_1(1 + \sqrt{3})^n + c_2(1 - \sqrt{3})^n.$$

Find c_1 and c_2 so that initial values $h_0 = 1$ and $h_1 = 3$ hold. In other words,

$$c_1 + c_2 = 1 \quad (n = 0)$$
$$c_1(1 + \sqrt{3}) + c_2(1 - \sqrt{3}) = 3 \quad (n = 1).$$

Solving this gives

$$(c_1, c_2) = \left(\frac{2 + \sqrt{3}}{2\sqrt{3}}, \frac{-2 + \sqrt{3}}{2\sqrt{3}} \right).$$

So the linear recurrence we are looking for is

$$h_n = \frac{2 + \sqrt{3}}{2\sqrt{3}}(1 + \sqrt{3})^n + \frac{-2 + \sqrt{3}}{2\sqrt{3}}(1 - \sqrt{3})^n.$$

In fact, it is possible to use generating functions to solve LHRR with constant coefficients.

Example. Solve $h_n = 5h_{n-1} - 6h_{n-2}$ where $n \geq 2$, with the initial values $h_0 = 1, h_1 = -2$.
Solution: Consider $g(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_n x^n + \cdots$. Then

$$g(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_n x^n + \cdots$$
$$-5xg(x) = -5h_0 x - 5h_1 x^2 - \cdots - 5h_{n-1} x^n - \cdots$$
$$6x^2 g(x) = 6h_0 x^2 + \cdots + 6h_{n-2} x^n + \cdots .$$

Adding all three, we have

$$(1 - 5x + 6x^2)g(x) = h_0 + (h_1 - 5h_0)x + (h_2 - 5h_1 + 6h_0)x^2 + \cdots + (h_n - 5h_{n-1} + 6h_{n-2})x^n + \cdots .$$

Note $h_n - 5h_{n-1} + 6h_{n-2} = 0$ for all $n \geq 2$, and also $h_0 = 1$ and $h_1 = -2$, so

$$(1 - 5x + 6x^2)g(x) = h_0 + (h_1 - 5h_0)x = 1 - 7x.$$

Now use the partial fraction to get c_1 and c_2:

$$g(x) = \frac{1 - 7x}{1 - 5x + 6x^2} = \frac{1 - 7x}{(1 - 2x)(1 - 3x)} = \frac{c_1}{1 - 2x} + \frac{c_2}{1 - 3x}$$
$$1 - 7x = c_1(1 - 3x) + c_2(1 - 2x) = (c_1 + c_2) + (-3c_1 - 2c_2)x.$$

This gives us the system of equations: $c_1 + c_2 = 1, -3c_1 - 2c_2 = -7$. Thus $(c_1, c_2) = (5, -4)$. Hence,

$$g(x) = \frac{5}{1 - 2x} - \frac{4}{1 - 3x}.$$

Recall that

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

Thus

$$g(x) = 1 + (-2)x + (-16)x^2 + \cdots + (5 \cdot 2^n - 4 \cdot 3^n)x^n + \cdots .$$

Thus $h_n = 5 \cdot 2^n - 4 \cdot 3^n$ for $n \geq 0$.

It is possible for some recurrences to have no general solution.

Example. The recurrence $h_n = 4h_{n-1} - 4h_{n-2} (n \geq 2)$ with $h_0 = 1, h_1 = 3$ has the characteristic equation $x^2 - 4x + 4 = (x-2)^2 = 0$, which has roots 2 and 2. Thus $h_n = c_1 2^n + c_2 2^n = C2^n$ for some C. Now, note that $h_0 = C = 1$ but $h_1 = 2C = 3$, but this is a contradiction.

15.1. **More on the generating function method**

Example. Let $h_0, h_1, \ldots, h_n$ be a sequence of numbers satisfying the recurrence

$$h_n + h_{n-1} - 16h_{n-2} + 20h_{n-3} = 0 \quad (n \geq 3)$$

where $h_0 = 0, h_1 = 1, h_2 = -1$. Solve this recurrence.
Solution: Let $g(x) = h_0 + h_1 x + h_2 x^2 + \cdots$. Then

$$\begin{aligned} g(x) &= h_0 + h_1 x + h_2 x^2 + h_3 x^3 + \cdots + h_n x^n + \cdots \\ xg(x) &= h_0 x + h_1 x^2 + h_2 x^3 + \cdots + h_{h-1} x^n + \cdots \\ -16x^2 g(x) &= -16h_0 x^2 - 16h_1 x^3 - \cdots - 16h_{n-2} x^n - \cdots \\ 20x^3 g(x) &= 20h_0 x^3 + \cdots + 20h_{n-3} x^n + \cdots . \end{aligned}$$

Adding all four gives

$$(1 + x - 16x^2 + 20x^3)g(x) = h_0 + (h_1 + h_0)x^2 + (h_2 + h_1 - 16h_0)x^2 = x,$$

since $h_3 + h_2 - 16h_1 + 20h_0 = h_4 + h_3 - 16h_2 + 20h_1 = \cdots = h_n + h_{n-1} - 16h_{n-2} + 20h_{n-3} = 0$. Hence,

$$\begin{aligned} g(x) = \frac{x}{1 + x - 16x^2 + 20x^3} &= \frac{x}{(1-2x)^2(1+5x)} = \frac{c_1}{1-2x} + \frac{c_2}{(1-2x)^2} + \frac{c_3}{1+5x} \\ x &= c_1(1-2x)(1+5x) + c_2(1+5x) + c_3(1-2x)^2 \\ &= (c_1 + c_2 + c_3) + (3c_1 + 5c_2 - 4c_3)x + (-10c_1 + 4c_3)x^2. \end{aligned}$$

Hence we have the system of equations

$$\begin{aligned} c_1 + c_2 + c_3 &= 0 \\ 3c_1 + 5c_2 - 4c_3 &= 1 \\ -10c_1 + 4c_3 &= 0, \end{aligned}$$

which yields $(c_1, c_2, c_3) = (-\frac{2}{49}, \frac{7}{49}, -\frac{5}{49})$. Hence

$$\begin{aligned} g(x) &= -\frac{2}{49(1-2x)} + \frac{7}{49(1-2x)^2} - \frac{5}{49(1+5x)} \\ &= -\frac{2}{49}\sum_{k=0}^{\infty} 2^k x^k + \frac{7}{49}\sum_{k=0}^{\infty}(k+1)2^k x^k - \frac{5}{49}\sum_{k=0}^{\infty}(-5)^k x^k \\ &= \sum_{k=0}^{\infty}\left(\left(-\frac{2}{49}\right)2^k + \frac{7}{49}(k+1)2^k - \frac{5}{49}(-5)^k\right)x^k. \end{aligned}$$

Therefore,

$$h_n = \frac{-2\cdot 2^n + 7(n+1)2^n - 5(-5)^n}{49}$$

for all $n \geq 0$.

The general solution suggests that the roots of the characteristic equation are $2, 2, -5$. Let's see if this is the case. Recall that the characteristic equation is $r(x) = 0$ where $r(x) = x^3 + x^2 - 16x + 20$. Replacing x by x^{-1} and then multiplying by x^3 we get

$$x^3 r(x^{-1}) = 1 + x - 16x^2 + 20x^3 =: q(x),$$

which is the same as in $h_n + h_{n-1} - 16h_{n-2} + 20h_{n-3} = 0$. And indeed, the roots of $r(x)$ are $2, 2, -5$. Since $r(x) = (x-2)^2(x+5)$ and $q(x) = x^3(x^{-1}-2)^2(x^{-1}+5) = (1-2x)^2(1+5x)$, which is the same as before.

Indeed, this can be done in general.

Theorem 15.2. *Let $h_0, h_1, \ldots, h_n, \ldots$ be a sequence of numbers that satisfy the LHRR*

$$h_n + c_1 h_{n-1} + c_2 h_{n-2} + \cdots + c_k h_{n-k} = 0 \quad (c_n \neq 0, n \geq k) \tag{3}$$

of order k with constant coefficients. Then its generating function $g(x)$ is of the form

$$g(x) = \frac{p(x)}{q(x)}, \tag{4}$$

where $\deg g = k$ and $\deg p < k$. Conversely, given such polynomials $p(x)$ and $q(x)$, there is a sequence $h_0, h_1, \ldots, h_n, \ldots$ satisfying a LHRR with constant coefficients of order k of the type (3) *whose generating function is given by* (4).

16. October 4

For repeated roots for the characteristic equation for a homogeneous linear recurrence, say q of multiplicity s, then

$$a^n, nq^n, \ldots, n^{s-1}q^n$$

will all be solutions, so we can take any linear combination of them.

Theorem 16.1. *Let $q_1, \ldots, q_n$ be the* distinct *roots of the characteristic equation of the LHRR $h_n = a_1 h_{n-1} + a_2 h_{n-2} + \cdots + a_k h_{n-k} \quad (a_k \neq 0, n \geq k)$. If q_i is an s_i-fold root of the characteristic equation, then the part of the general solution of this recurrence relation corresponding to q_i is $H_n^{(i)} = c_1 q_i^n + c_2 n q_i^n + \cdots + c_{s_i} n^{s_i - 1} q^n$. Then the general solution of the recurrence is*

$$h_n = H_n^{(1)} + \cdots + H_n^{(t)}.$$

Example. Solve the recurrence relation

$$h_n = -h_{n-1} + 3h_{n-2} + 5h_{n-3} + 2h_{n-4} \quad (n \geq 4),$$

subject to $h_0 = 1, h_1 = 0, h_2 = 1, h_3 = 2$. Then $x^n = -x^{n-1} + 3x^{n-2} + 5x^n - 3 + 2x^{n-4}$, so the characteristic equation is $x^4 + x^3 - 3x^2 - 5x - 2 = 0$. By the rational root theorem, we see that $\pm 1, \pm 2$ are possible roots. Out of these four, we see that -1 is a root. Long division gives us the factorization $(x+1)(x+1)(x^2 - x - 2) = (x+1)^3(x-2) = 0$, so the roots are $-1, -1, -1, 2$. The general solution is

$$h_n = c_1(-1)^n + c_2 n(-1)^n + c_3 n^2(-1)^n + c_4 2^n.$$

Solve for c_1, c_2, c_3, c_4 with the given initial values:

$$\begin{aligned} c_1 + c_4 &= 1 \\ -c_1 - c_2 - c_3 + 2c_4 &= 0 \\ c_1 + 2c_2 + 4c_3 + 4c_4 &= 1 \\ -c_1 - 3c_2 - 9c_+ 8c_4 &= 2. \end{aligned}$$

This gives $(c_1, c_2, c_3, c_4) = (\frac{7}{9}, -\frac{1}{3}, 0, \frac{2}{9})$, so the general solution is

$$h_n = \frac{7}{9}(-1)^n - \frac{1}{3}n(-1)^n + \frac{2}{9}2^n.$$

So far we only have covered solving homogeneous ones. Now we will think about how to solve the non-homogeneous ones as well. First, we outline the steps to solve non-homogeneous recurrences.

(1) Find the general solution to the corresponding homogeneous recurrence relation.
(2) Find a particular solution of the non-homogeneous relation. This part is an art rather than a science. However, certain types of non-homogeneous part (say b_n) suggest trying certain particular solutions. For instance, if b_N is a polynomial of degree k in n, then try a polynomial of degree k in n. If b_n is an exponential of degree k in n, then try some exponential (e.g., if $b_n = d^n$ then try pd^n for some p).
(3) Sum up what you get in the first step and the second step, and then determine values of constants to satisfy the initial condition.

Example. Solve for $h_n = 2_{n-1} + 3^n$ for all $n \geq 1$ and $h_0 = 2$.
Solution: First, consider the corresponding homogeneous relation $h_n = 2h_{n-1}$ has the general solution $h_n = c_1 2^n$. Try $p \cdot 3^n$ as a particular solution (and search for p). Then $p \cdot 3^n = 2(p \cdot 3^{n-1}) + 3^n = (2p+1)3^n$, so $3p = 2p + 3$. Thus $p = 3$. So 3^{n+1} is a particular solution. Thus all solutions to the original recurrence are of the form $h_n = c_1 2^n + 3^{n+1}$. Plugging in $h = 0$ gives $c_1 = -1$. Verify that $h_n = -2^n + 3^{n+1}$ works by checking the recurrence relation and the initial condition – you will see this works.

Alternately, we can use the generating function to solve this.
Solution: Let $g(x) = h_0 + h_1 x + \cdots + h_n x^n + \cdots$. Then $(1-2x)g(x) = h_0 + (h_1 - 2h_0)x + (h_2 - 2h_1)x^2 + \cdots + (h_n - 2h_{n-1})x^n + \cdots$. Then $h_0 = 2$ and $h_n - 2h_{n-1} = 3^n$ for any $n \geq 1$. So we see that $(1-2x)g(x) = 2 + 3x + 3^2x^2 + \cdots + 3^n x^n = 1 + 1 + (3x) + (3x)^2 + \cdots = 1 + (1-3x)^{-1}$. So $g(x) = (1-2x)^{-1} + (1-2x)^{-1}(1-3x)^{-1}$, and using the partial fraction method gives us

$$g(x) = \frac{1}{1-2x} + \frac{1}{(1-2x)(1-3x)} = \frac{1}{1-2x} - \frac{2}{1-2x} + \frac{3}{1-3x} = -\frac{1}{1-2x} + \frac{3}{1-3x}.$$

Thus

$$\begin{aligned} g(x) &= \sum_{n=0}^{\infty}(2x)^n + (-2)\sum_{n=0}^{\infty}(2x)^n + 3\sum_{n=0}^{\infty}(3x)^n \\ &= \sum 2^n x^n + \sum(-2)2^n x^n + \sum 3\cdot 3^n x^n \\ &= \sum_{n=0}^{\infty}(-2^n + 3^{n+1})x^n, \end{aligned}$$

so $h_n = -2^n + 3^{n+1}$ as required, for all $n \geq 0$.

17. October 11: Systems of Distinct Representatives (Chapter 9)

Definition 17.1. Let Y be a finite set and $\mathcal{O} = (A_1, \ldots, A_n)$ be a family of subsets of Y (some may be the same). A *system of distinct representatives (SDR)* is a collection $(e_1, \ldots, e_n)$ of distinct elements of Y such that $e_1 \in A, \ldots, e_n \in A_n$.

Example. For $Y = \{a, b, c, d, e\}, A_1 = \{a, b, c\}, A_2 = \{b, d\}, A_3 = \{a, b, d\}, A_4 = \{b, d\}$, one can choose (c, b, a, d) to form a SDR. Another possible option: (c, d, a, b). However, if you choose a for A_1, then one cannot choose any representative for A_3.

Example. Let $Y = \{x, y, z\}, A_1 = \{x, y, z\}, A_2 = \{x, z\}, A_3 = \{x, y\}, A_4 = \{y, z\}$. In this case we cannot have any SDR – we only have three elements, but there are more than three sets.

Example. We want to place non-attacking rooks in a 4 board with forbidden squares. If $A_1 = \{1, 3, 4, 5\}, A_2 = \{1, 2, 4, 5\}, A_3 = \{2, 4\}$, and $A_4 = \{2, 3, 4, 5\}$, then one can place four non-attacking rooks on board i.e., there is an SDR for A_1, A_2, A_3, A_4.

Consider the following general problem. Let $\mathcal{O} = (A_1, \ldots, A_n)$ is a family of subsets of a finite set Y. Then determine if $\mathcal{O}$ has an SDR; if not what is the largest number t of sets in a subfamily $\mathcal{O}(i_1, \cdots i_t) := (A_{i_1}, A_{i_2}, \ldots, A_{i_t})$ that does have an SDR. It is not that hard to come up with a necessary condition: $\left|\bigcup_{t=1}^{k} A_{i_t}\right| \geq k$. Note that you need to have enough elements in order to pick a representative for each of the k sets. For this, you want to have at least k distinct elements to guarantee a pick for each set. This is also known as the "marriage condition". But surprisingly, this is also a sufficient condition, as we will see in the theorem below.

Theorem 17.1. *The family $\mathcal{O} = (A_1, \ldots, A_n)$ of subsets of a finite set Y has an SDR if and only if for all $k \in \{1, 2, \ldots n\}$ and for all $A_{i_1}, \ldots, A_{i_k}$ we have $|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}| \geq k$.*

Proof. ($\Rightarrow$) already proved.

($\Leftarrow$) We will prove this by induction.

(i) Base case ($n = 1$): By the marriage condition, indeed $|A_1| \geq 1$, so just pick $x_1 \in A_1$.

(ii) Inductive hypothesis: Assume that if MC holds, then there exists an SDR for any collection containing fewer than n sets.

(iii-1) Inductive step - Case 1 ("tight case"): for some $k \in \{1, \ldots, n-1\}$, there is a subfamily $A_{i_1}, \ldots, A_{i_k}$ such that $|A_{i_1} \cup \cdots \cup A_{i_k}| = k$. Without loss of generality, re-index each of A_{i_t} with A_t. Write $E := A_1 \cup \cdots \cup A_k$. Then $|E| = k$. As $\mathcal{O}$ satisfies the MC, so does $\mathcal{O}' = (A_1, \ldots, A_k)$. So by inductive hypothesis $\mathcal{O}'$ has an SDR (say $(e_1, \ldots, e_k)$). Now set $\mathcal{O}^* := \{A_{k+1} \setminus E, \ldots, A_n \setminus E\}$. Clearly $\mathcal{O}^*$ has fewer than n sets. We want $\mathcal{O}^*$ to have the marriage condition. Pick any l sets, say $A_{j_1} \setminus E, A_{j_2} \setminus E, \ldots, A_{j_l} \setminus E$. Now consider the $k + l$ sets $A_1, \ldots, A_k, A_{j_1}, \ldots, A_{j_l}$. Then $|A_1 \cup \cdots \cup A_k \cup A_{j_1} \cup \cdots \cup A_{j_l}| \geq k + l$. Then $|E \cup A_{j_1} \cup \cdots \cup A_{j_l}| \geq k + l$. But since E is already in the union, it follows

$$|E \cup (A_{j_1} \setminus E) \cup \cdots \cup (A_{j_l} \setminus E)| \geq k + l.$$

But $E \cap (A_{j_t} \setminus E) = \emptyset$ for each t, so indeed

$$\underbrace{|E|}_{k} + |(A_{j_1} \setminus E) \cup \cdots \cup (A_{j_l} \setminus E)| \geq k + l,$$

or equivalently

$$|(A_{j_1} \setminus E) \cup \cdots \cup (A_{j_l} \setminus E)| \geq l.$$

Hence $\mathcal{O}^*$ satisfies the marriage condition, so by induction it has an SDR $(e_{k+1}, \ldots, e_n)$. Putting the two pieces together, we see that $(e_1, \ldots, e_n)$ is an SDR for $\mathcal{O}$.

(iii-2) Inductive step - Case 2: For all $k \in \{1, \ldots, n-1\}$ and all indices $i_1, \ldots, i_k$, we have $|A_{i_1} \cup \cdots \cup A_{i_k}| > k$. So $|A_1| \geq 2$, so pick $e_1 \in A_1$. And now consider $\mathcal{O}' = (A_2 \setminus \{e_1\}, \ldots, A_n \setminus \{e_1\})$. Note that $\mathcal{O}'$ contains fewer than n sets, so we are home free if $\mathcal{O}'$ has the marriage condition. Choose some k sets from $\mathcal{O}'$, say $|(A_{i_1} \setminus \{e_1\}) \cup \cdots \cup (A_{i_k} \setminus \{e_1\})| = |(A_{i_1} \cup \cdots \cup A_{i_k}) \setminus \{e_1\}|$. Since $|(A_{i_1} \cup \cdots \cup A_{i_k}) \setminus \{e_1\}| \geq |A_{i_1} \cup \cdots \cup A_{i_k}| - 1 \geq k$, by induction $\mathcal{O}'$ has an SDR $(e_2, \ldots, e_n)$. Then $(e_1, \ldots, e_n)$ is an SDR for $\mathcal{O}$. □

Corollary 17.1. *Let $\mathcal{O} = (A_1, \ldots, A_n)$ be a family of subsets of a finite set Y. Then the largest number of sets in a subfamily of $\mathcal{O}$ with an SDR equals the smallest value of*

$$|A_{i_1} \cup \cdots \cup A_{i_k}| + n - k$$

over all choices of $k = 1, \ldots, n$ and all choices of k indices $i_1, \ldots, i_k$.

Example. Let $A_1 = \{a, b, c\}, A_2 = \{b, c\}, A_3 = \{b, c\}, A_4 = \{b, c\}, A_5 = \{c\}, A_6 = \{a, b, c, d\}$. Clearly we cannot find an SDR for all six sets. However, note that $|A_2 \cup A_3 \cup A_4 \cup A_5| = |\{b, c\}| = 2$. So by Corollary 17.1, at most $2 + 6 - 4 = 4$ of the sets can be chosen to have an SDR. But then (A_1, A_2, A_5, A_6) has (a, b, c, d) as an SDR, so 4 is the best you can do.

18. October 16: Combinatorial Designs (Chapter 10)

First, we do some quick review of modular arithmetic $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$. First, $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is a group with identity 0. On the other hand, $(\mathbb{Z}/n\mathbb{Z}, \odot)$ is a semigroup, not a group. But $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \odot)$ is a group if and only if n is a prime. In general, $(\mathbb{Z}/n\mathbb{Z}, \odot)$ is a semigroup as not every element has an inverse. For instance, if $n = 10$, then only the integers that are relatively prime to 10 have inverses.

Theorem 18.1. *Let $n \geq 2$ be an integer. Then for any $a \in \{1, \ldots, n-1\}$, a has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if* $\gcd(a, n) = 1$.

Corollary 18.1. *Let N be a prime number. Then every non-zero integer in $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse.*

Corollary 18.2 (Wilson's theorem)**.** $(p-1)! \equiv -1 \pmod{p}$ *if and only if p is a prime.*

Remark. In particular, $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ is a *field* when n is a prime. Moreover, in a field, we have cancellation rules – that is,

$$a \odot b = 0 \Rightarrow a = 0 \text{ or } b = 0$$
$$a \odot b = a \odot c, a \neq 0 \Rightarrow b = c.$$

Also, provided $a \neq 0$, the linear equation $a \odot x = b$ has the unique solution $x = a^{-1} \odot b$.

In fact, finite fields have p^k elements for $k \geq 1$ and p prime. But how do we construct them? Take an irreducible polynomial $s(x)$ of degree k over $\mathbb{Z}/p\mathbb{Z}$. Then $a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ are the elements of a field of order p^k (of course, $a_i \in \mathbb{Z}/p\mathbb{Z}$ for all i).

Example. We will try to construct the finite field of 4 elements. Note that $f(x) := x^2 + x + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$ since $f(0) = f(1) = 1$. Note that

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1),$$

where the RHS denotes a set of equivalence relations $\sim$ defined as $q_1(x) \sim q_2(x)$ if and only if $q_1 - q_2 \in (x^2 + x + 1)$. So for instance, we have $[0] = [x^2 + x + 1]$, so $[x^2] = [x + 1]$. Similarly, $[x^3] = [x][x^2] = [x][x + 1] = [x^2 + x] = [1]$.

In other words, $\mathbb{F}_4$ can be viewed as a two-dimensional vector space over $\mathbb{F}_2$; $(0, 0)$ corresponds to 0; $(0, 1)$ corresponds to 1. Also, $(1, 0)$ corresponds to x, and $(1, 1)$ corresponds to $(x + 1)$. Addition and multiplication work as follows:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

19. October 18: Block Designs (Chapter 10.2)

Seven varieties of a product are to be tested. We can ask each consumer to test all seven, but can we ask each person to test 3, such that every *pair* of varieties are tested?
Solution: Let $\{0, 1, 2, 3, 4, 5, 6\}$ be varieties. There are $\binom{7}{2} = 21$ varieties. Each tester makes $\binom{3}{2} = 3$ comparisons of pairs. Thus the number of testers needed is $21/3 = 7$. One possible block: $B_1 = \{0, 1, 3\}, B_2 = \{1, 2, 4\}, B_3 = \{2, 3, 5\}, B_4 = \{3, 4, 6\}, B_5 = \{0, 4, 5\}, B_6 = \{1, 5, 6\}, B_7 = \{0, 2, 6\}$. Another way to represent this block is the incidence matrix:

	0	1	2	3	4	5	6
B_1	1	1	0	1	0	0	0
B_2	0	1	1	0	1	0	0
B_3	0	0	1	1	0	1	0
B_4	0	0	0	1	1	0	1
B_5	1	0	0	0	1	1	0
B_6	0	1	0	0	0	1	1
B_7	1	0	1	0	0	0	1

Definition 19.1. Let k, λ, and v be positive integers with $2 \leq k \leq v$. Let X be a set of v elements ("varieties"). Let $\mathscr{B}$ be the collections $B_1, B_2, \ldots, B_b$ of k-element subsets of X ("blocks"). Then $\mathscr{B}$ is a *balanced block design* on X if every pair of elements of X occurs in exactly λ blocks, and λ is called the *index* of the design $\mathscr{B}$. If $k = v$, then the design is called a *complete block design*; if $k < v$, then $\mathscr{B}$ is a *balanced incomplete block design* (BIBD).

We shall assume from now on we are dealing with a BIBD (i.e., $k < v$), as nothing much interesting can be said of a complete block design.

If B is a BIBD on X, then we can associate an *incidence matrix* or an *incidence array*. Say $M = (m_{ij})$ be a $b \times r$ matrix, and define $m_{ij} := 1$ if $x_j \in B_i$ and 0 otherwise.

Lemma 19.1. *In a BIBD, each variety is contained in* $r = \dfrac{\lambda(v-1)}{k-1}$ *blocks.*

Proof. Fix a variety y. Let's consider the set $\{(x, B) : x \neq y, \text{ both } x, y \in B\}$. Now let's count the size of this set. We can count in two ways. First, note that there are $v - 1$ choices (exactly $v - 1$ varieties – everything except for y itself) to choose from, for x. There are λ blocks containing each of the pair, so there are $(v-1)\lambda$ elements. Second, we first count the number of blocks containing y first – suppose that there are r_y of those. Now, note that any arbitrary block has k elements, so for each block, we have $k - 1$ choices of x (again, everything in that block except for y itself). Thus, the same set also has $r_y(k-1)$ elements. Thus, since $r_y(k-1) = (v-1)\lambda$, the claim follows. □

Lemma 19.2. *$bk = vr$ in a BIBD.*

Proof. Look at the incidence matrix of a BIBD, and count the number of 1's in that matrix in two different ways. □

Corollary 19.1. *$\lambda < r$ in a BIBD.*

For a BIBD, there are some parameters (not all independent), namely:

- b: number of blocks
- v: number of varieties
- k: number of varieties in each block
- r: number of blocks containing each variety
- λ: number of blocks containing each pair of varieties

Example. Is there a BIBD with parameters $(b, k, v, r) = (12, 4, 16, 3)$? First, we have $bk = vr = 48$, so we cannot conclusively say yet if there is a BIBD. However, note that

$$r = \frac{\lambda(v-1)}{k-1} \Rightarrow \lambda = \frac{(k-1)r}{v-1} = \frac{3 \cdot 3}{16-1} = \frac{9}{15} = \frac{3}{5} \notin \mathbb{N}.$$

Since r is not a positive integer, there cannot be any design with these parameters.

Example. Is there a BIBD with parameters $(b,k,v,r) = (12,3,9,4)$? Yes, there is (the incidence matrix displayed below):

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Theorem 19.1 (Fisher's inequality)**.** *$b \geq v$ in a BIBD.*

Proof. Let A be the $b \times v$ incidence matrix (remember $r > \lambda$). Then

$$A^T A = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \vdots & \vdots & r & \vdots & \vdots \\ \lambda & \vdots & \vdots & \ddots & \lambda \\ \lambda & \lambda & \cdots & \lambda & r \end{pmatrix}$$

(i.e., r on diagonal entries, λ otherwise).Now we claim that $A^T A$ has rank v (equivalently, $A^T A$ is invertible). To show this, it suffices to show that the determinant of $A^T A$ is non-zero.

$$\begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \vdots & \vdots & r & \vdots & \vdots \\ \lambda & \vdots & \vdots & \ddots & \lambda \\ \lambda & \lambda & \cdots & \lambda & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \vdots & \vdots & r & \vdots & \vdots \\ \lambda & \vdots & \vdots & \ddots & \lambda \\ r+(v-1)\lambda & r+(v-1)\lambda & r+(v-1)\lambda & \cdots & r+(v-1)\lambda \end{vmatrix}$$

$$= (r+(v-1)\lambda) \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \vdots & \vdots & r & \vdots & \vdots \\ \lambda & \vdots & \vdots & \ddots & \lambda \\ 1 & 1 & 1 & \cdots & 1 \end{vmatrix}$$

$$= (r+(v-1)\lambda) \begin{vmatrix} r-\lambda & 0 & 0 & \cdots & 0 \\ 0 & r-\lambda & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & r-\lambda & 0 \\ 1 & 1 & 1 & \cdots & 1 \end{vmatrix}$$

$$= (r+(v-1)\lambda)(r-\lambda)^{v-1} \cdot 1.$$

But recall that $r - \lambda > 0$ since $r > \lambda$. Also, both r and λ are all positive, and $v - 1 \geq 1$. Thus the determinant of $A^T A$ is non-zero. But from linear algebra, recall that $\text{rank}(BC) \leq \text{rank}(C)$ for any matrices B and C. So we have $v = \text{rank}(A^T A) \leq \text{rank}\, A \leq b$ (cannot be greater than the number of rows of A). The claim now follows. □

20. October 23: Construction of a block design

Definition 20.1. A BIBD for which $b = v$ is called *symmetric* (an SBIBD). Therefore, in this case, we have $k = r$.

To build these, we use the integers mod v. Start with a *starter block* $B \in \mathbb{Z}/v\mathbb{Z} = \{0, 1, \ldots, v-1\}$ and take the translates of it: $B = B + 0, B + 1, \ldots, B + (v-1)$ where $B + j = \{x + j : x \in B\}$. Now we need to introduce the following definition to discuss how to choose B appropriately to get an SBIBD.

Definition 20.2. B is a *difference set mod* v provided that every nonzero integer in $\mathbb{Z}/v\mathbb{Z}$ occurs the same number λ of times amongst the $k(k-1)$ differences amongst the distinct elements of B (in both orders): $x - y$ for distinct $x, y \in B$.

Since there are $v - 1$ non-zero integers in $\mathbb{Z}/v\mathbb{Z}$, each non-zero integer in $\mathbb{Z}/v\mathbb{Z}$ must occur

$$\lambda = \frac{k(k-1)}{v-1}$$

times as a difference.

Example. $v = 7, k = 3, B = \{0, 1, 3\}$

$-$	0	1	3
0	0	6	4
1	1	0	5
2	3	2	0

Theorem 20.1. *Let B be a subset of $k < v$ elements of $\mathbb{Z}/v\mathbb{Z}$ that forms a difference set mod v. Then the blocks developed from B as a starter block form an SBIBD with $\lambda = \frac{k(k-1)}{v-1}$.*

Proof. This is Theorem 10.2.5 of the text. □

Example. Find a difference set of size 5 in $\mathbb{Z}/11\mathbb{Z}$ and use it as a starter block for SBIBD.
Solution: Try $B = \{0, 2, 3, 4, 8\}$. Then

$-$	0	2	3	4	8
0	0	9	8	7	3
2	2	0	10	9	5
3	3	1	0	10	6
4	4	2	1	0	7
8	8	6	5	4	0

Other than 0, every element in $\mathbb{Z}/11\mathbb{Z}$ appears twice, so this an SBIBD.

21. October 23: Steiner Triple Systems (STS) (Chapter 10.3)

For a BIBD with $k = 2$, every pair is a block λ times. But if $k = 3$, then things become more complex and interesting.

Definition 21.1. A *Steiner triple system (STS)* is a BIBD with $k = 3$.

Example. The set $\{0, 1, 2\}$ is a STS with $v = 3, b = 1, \lambda = 1$.

Example. $\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}$ is a STS (and a SBIBD), with $(b, v, \lambda) = (7, 1, 1)$. In fact, this is the only STS that is a SBIBD.

Example. $\{0, 1, 2\}, \{0, 2, 3\}, \{1, 2, 3\}, \{0, 2, 3\}$ is a STS on 4 varieties but with $\lambda = 2$.

Example. See text p363 for an example with $(v, b, \lambda) = (9, 12, 1)$.

Theorem 21.1. *Let B be a STS with parameters $b, v, k = 3, r, \lambda$. Then $r = \dfrac{\lambda(v-1)}{2}$ and $b = \dfrac{\lambda v(v-1)}{6}$. Is $\lambda = 1$, then there exists $n \in \mathbb{Z}$ such that $v = bn + 1$ or $bn + 3$ (i.e., $v \equiv 1$ or $3 \pmod b$).*

Proof. $k = 3$ so $r = \frac{\lambda(v-1)}{k-1} = \frac{\lambda(v-1)}{2}$. $bk = vr$, so $3b = \frac{\lambda v(v-1)}{2}$. Thus $b = \frac{\lambda v(v-1)}{6}$. If $\lambda = 1$, then $b = \frac{v(v-1)}{6}$ and $r = \frac{v-1}{2}$. Then v is odd, and $v(v-1) \equiv 0 \pmod 6$. The claim follows upon noting that $v(v-1) \not\equiv 0 \pmod 6$ if $v \equiv 5 \pmod 6$ but $v(v-1) \equiv 0 \pmod 6$ if $v \equiv 1, 3 \pmod 6$. □

Remark. In fact, it can be shown that for all $n \geq 1$, there are STS with $\lambda = 1$ and $v = 6n+1$ or $6n + 3$.

Theorem 21.2 (Constructing a larger STS from smaller ones)**.** *If there are STS of index $\lambda = 1$ with v and w varieties respectively, then there is a STS of index $\lambda = 1$ with vw varieties.*

Proof. Let B_1 (resp. B_2) be a STS of index 1 with varieties $a_1, \ldots, a_v$ (resp. $b_1, \ldots, b_w$). Consider $X = \{(a_i, b_j) : 1 \leq i \leq v, 1 \leq j \leq w\}$. Let B be triples $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\}$ where:

(i) $r = s = t$ and $\{a_i, a_j, a_k\} \in B_1$; or
(ii) $i = j = k$ an $\{b_r, b_s, b_t\} \in B_2$; or
(iii) all i, j, k are different, all r, s, t are different, $\{a_i, a_j, a_k\} \in B_1$ and $\{b_r, b_s, b_t\} \in B_2$.

Now we show that for any $(a_i, b_r) \neq (a_j, b_s)$, there exists a unique (a_k, b_t) such that $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\} \in B$.

(1) Case 1: $r = s$.
Then $a_i \neq a_j$, so there exists a unique a_k such that $\{a_i, a_j, a_k\} \in B_1$. Then $\{(a_i, b_r), (a_j, b_r), (a_k, b_r)\} \in B$. And it is the only possible block of B containing (a_i, b_r) and (a_j, b_r).
(2) Case 2: $i = j$.
This case works similarly as Case 1.
(3) Case 3: $r \neq s$ and $i \neq j$.
In this case, there exist unique a_k and b_t such that $\{a_i, a_j, a_k\} \in B_1$ and $\{b_r, b_s, b_t\} \in B_2$, so $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\} \in B$ and there is no other choice. □

Example. Start with $B_1 = \{\{0,1,2\}\} = B_2$. Then

$$\begin{aligned} B = \{&\{(0,0),(1,0),(2,0)\},\{(0,1),(1,1),(2,1)\},\{(0,2),(1,2),(2,2)\},\\ &\{(0,0),(0,1),(0,2)\},\{(1,0),(1,1),(1,2)\},\{(2,0),(2,1),(2,2)\},\\ &\{(0,0),(1,1),(2,2)\},\{(0,0),(1,2),(2,1)\},\{(0,1),(1,0),(2,2)\},\\ &\{(0,1),(1,2),(2,0)\},\{(0,2),(1,0),(2,1)\},\{(0,2),(1,1),(2,0)\}\} \end{aligned}$$

gives a STS.

22. October 25: Latin Squares (Chapter 10.4)

Definition 22.1. A *Latin square (LS) of order* n, based on a set S of n elements, is an $n \times n$ array, each of whose entries are in S such that each of the n elements of S occurs exactly once in each row and column.

Example. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are Latin squares of order 2. Similarly, $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ is a LS of order 3.

If A is a LS of order n and $A(k)$ is the set of positions occupied by the k's, then $A(0), \ldots, A(n-1)$ is a partition of the n^2 positions of the $n \times n$ board into sets of n non-attacking rook positions. We can also interchange any permutation of symbols to get a new LS. So $n!$ Latin squares arise from one Latin square as a result.

Example.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 3 & 1 & 0 \\ 3 & 1 & 0 & 2 \\ 1 & 0 & 2 & 3 \end{pmatrix}$$

One can ways bring a LS into the *standard form*, where the first row is $0, 1, \ldots, n-1$ in order.

Theorem 22.1. *Let n be a positive integer, and let A be an $n \times n$ array whose (i,j)-th entry is $a_{ij} = i + j \pmod n$. Then A is a LS of order n based on $\mathbb{Z}/n\mathbb{Z}$.*

Theorem 22.2. *Let n be a positive integer where $\gcd(r,n) = 1$ and $r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$. If A is a $n \times n$ array with $a_{ij} = ri + j$, then A is a LS of order n based on $\mathbb{Z}/n\mathbb{Z}$, which we shall call L_n^r.*

Proof. Suppose that $a_{ij} = a_{ik}$. Then $ri + j \equiv ri + k \pmod n$, so $j \equiv k \pmod n$. Similarly, if $a_{ij} = a_{kj}$, then $ri + j \equiv rk + j \pmod n$, or $ri \equiv rk \pmod n$. Since $\gcd(r,n) = 1$, we can multiply both sides by r^{-1}, so $i \equiv k \pmod n$. □

Example.

$$L_5^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}.$$

Definition 22.2. Let $A_1, \ldots, A_k$ be LS's of order n based on $\mathbb{Z}/n\mathbb{Z}$. We say that A_i and A_j are *orthogonal* for $i \neq j$ if in the juxtaposed array $A_i \times A_j$, each of the ordered pairs (i, j) of integers in $\mathbb{Z}/n\mathbb{Z}$ appear exactly once. We say that $A_1, \ldots, A_k$ are *mutually orthogonal Latin squares (MOLS)* if A_i and A_j are orthogonal for $i \neq j$.

Example. $\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}$ are orthogonal, as the matrix

$$\begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{pmatrix}$$

contains each (i, j) exactly once. However, it is impossible to construct such if the order is 2.

Theorem 22.3. *Let n be a prime number. Then $L_n^1, \ldots, L_n^{n-1}$ are $n-1$ MOLS's.*

Proof. As n is prime, $L_n^1, \ldots, L_n^{n-1}$ are LS's of order n. Let $r, s \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ where $r \neq s$. We show that L_n^r and L_n^s are orthogonal. Suppose – to reach a contradiction – that tow entries, say the (i, j)-th and the (k, l)-th, are the same in the juxtaposed array. Call the (i, j)-th entry of L_n^r $a_{r,(i,j)}$. Then our assumption means $(a_{r,(i,j)}, a_{s,(i,j)}) = (a_{r,(k,l)} = a_{s,(k,l)})$. Since $a_{r,(i,j)} = ri + j$, we have $(ri + j, si + j) = (rk + l, sk + l)$. Hence $ri - rk = l - j$ and similarly $si - sk = l - j$ – so $r(i - k) = s(r - k)$. Note that $r \neq s$, so this forces $i - k = 0$. Hence $i = k$ so $j = l$. But this contradicts the fact that $(i, j) \neq (k, l)$, so L_n^r and L_n^s are orthogonal, as required. □

Example. $L_5^1, L_5^2, L_5^3, L_5^4$ are MOLS's.

We can extend these ideas into prime powers via finite fields (viewed as a vector space over the finite field of n elements for n prime). So for every prime power n, there are $n - 1$ MOLS of order n.

Theorem 22.4. *Let $n \geq 2$ be an integer, and let $A_1, \ldots, A_n$ be MOLS of order n. Then $k \leq n - 1$.*

Proof. Without loss of generality, each LS is on $\mathbb{Z}/n\mathbb{Z}$, and we can bring each LS into the standard form (note this does not affect orthogonality). Consider $A_i \times A_j$; its first row is always $(0, 0), \ldots, (n - 1, n - 1)$. If a_j is the second row, first column entry of A_j, then notice that each $a_1, \ldots, a_k$ must be distinct. But this means $k \neq n - 1$ due to the pigeonhole principle. □

23. October 30

Let $N(n)$ be the largest number of MOLS of order n. Last time we proved that $N(2) = 1$, and $N(n) = n - 1$ whenever n is a prime power. We also displayed MOLSs $L_n^1, \ldots, L_n^{n-1}$ where each L_n^r is defined $(L_n^r)_{ij} := ri + j \pmod{n}$.

Example. To see $N(4) = 3$, we first find a field of order 4. Note that $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, so $\mathbb{F}_4 \cong \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle = \{0, 1, x, 1 + x\}$. So we have $x^2 = -x - 1 = x + 1$. This allows us to construct the following Latin squares:

$$L_n^1 = \begin{pmatrix} 0 & 1 & x & 1+x \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \end{pmatrix},$$

$$L_n^x = \begin{pmatrix} 0 & 1 & x & 1+x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \\ 1 & 0 & 1+x & x \end{pmatrix}, \text{ and}$$

$$L_n^{1+x} = \begin{pmatrix} 0 & 1 & x & 1+x \\ 1+x & x & 1 & 0 \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \end{pmatrix}.$$

Re-label x and $1 + x$ with 2 and 3 respectively.

$$L_n^1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix},$$

$$L_n^x = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \text{ and}$$

$$L_n^{1+x} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}.$$

Now we have three MOLSs.

Example. It is a non-trivial exercise, but $N(6) = 1$. Note that 6 is not a prime power.

Theorem 23.1. *$N(n) \geq 2$ for each odd integer n.*

Proof. This is Theorem 10.2 from the textbook (Brualdi, Introductory Combinatorics). □

Theorem 23.2. *$N(mk) \geq \min\{N(m), N(k)\}$ for any positive integers m and k.*

Example. $N(3) \geq 2$ and $N(4) \geq 2$, so $N(12) \geq 2$. Pick two MOLSs for each integer (3 and 4 in this example):

$$A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

$$B_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}, B_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 9 \\ 1 & 0 & 3 & 2 \end{pmatrix}.$$

Now take $A_1 \otimes B_1$ and $A_2 \otimes B_2$. Then one will see that $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are orthogonal.

Corollary 23.1. *Let $n \geq 2$ be an integer that is* not twice an odd number*. Then there exists a pair of orthogonal Latin squares of order n.*

Corollary 23.2. *Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of n. Then $N(n) \geq \min\{p_i^{e_i} - 1 : 1 \leq i \leq k\}$.*

So what about the twice an odd number case (i.e., integers of the form $4k + 2$ for some $k \in \mathbb{N} \cup \{0\}$)? It actually has been shown that *except for* $n = 2, 6$, there is a pair of MOLS of order n.

Now we discuss the relationships between MOLS and BIBD. We can use $n - 1$ MOLS of order n to build a BIBD. Let $A_1, \ldots, A_{n-1}$ be $n - 1$ MOLS of order n. Set

$$R_n := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ n-1 & n-1 & \cdots & n-1 \end{pmatrix}, S_n := \begin{pmatrix} 0 & 1 & \cdots & n-1 \\ 0 & 1 & \cdots & n-1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & n-1 \end{pmatrix}.$$

We construct a block design B with $b = n^2 + n, v = n^2, k = n, r = n + 1, \lambda = 1$. Let $X = \{(i, j) : 0 \leq i, j \leq n - 1\}$ be our varieties. And for any array C, define $C(i)$ to be the set of cells with symbol i in C. Then consider the following blocks: $R_n(0), \ldots, R_n(n-1), S_n(0), \ldots, S_n(n-1), A_1(0), \ldots, A_1(n-1), A_2(0), \ldots, A_2(n-1), \ldots, A_{n-1}(0), \ldots, A_n(n-1)$. Evidently $k = n$, so we only need to show that every pair of treatments are in exactly one block. Consider two treatments (i, j) and (k, l). There are three possibilities:

(1) (i, j) and (k, l) are in the same row, i.e., $i = k$. Then (i, j) and (k, l) both belong to $R_n(i)$ *but no other*.
(2) (i, j) and (k, l) are in the same column, i.e., $j = l$. Then (i, j) and (k, l) both belong to $S_n(j)$ *but no other*.
(3) $i \neq k$ and $j \neq l$. Clearly (i, j) and (k, l) don't belong to any $R_n(\varepsilon_1)$ or $S_n(\varepsilon_2)$ blocks. If (i, j) and (k, l) were in $A_r(e)$ and $A_s(f)$, this contradicts the fact that A_r and A_s being orthogonal. Therefore (i, j) and (k, l) are in *at most* one block together. But there are n^2 varieties, and $\binom{n^2}{2} = \dfrac{n^2(n^2-1)}{2}$ pairs of them, each pair of which is in at most one block. Each block has n varieties, and so $\dfrac{n(n-1)}{2}$ pairs of varieties.

Thus we have a total of

$$(n^2+n)\frac{n(n-1)}{2} = \frac{n^2(n^2-1)}{2}$$

pairs of varieties in blocks, which is the number of pairs of varieties. It follows that every pair must be in exactly one block.

Putting all these together, we see that we have a BIBD with $\lambda = 1$, as required.

24. November 1: Building a BIBD from $n-1$ MOLS of order n

Example. Let

$$A_1 := \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}, A_2 := \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Also, let

$$R := \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{pmatrix}, S := \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

Then the varieties are $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$, and the blocks are

$$\{(0,0),(0,1),(0,2)\},\{(1,0),(1,1),(1,2)\},\{(2,0),(2,1),(2,2)\},$$
$$\{(0,0),(1,0),(2,0)\},\{(0,1),(1,1),(2,1)\},\{(0,2),(1,2),(2,2)\},$$
$$\{(0,0),(1,2),(2,1)\},\{(0,1),(1,0),(2,2)\},\{(0,2),(1,1),(2,0)\},$$
$$\{(0,0),(1,1),(2,2)\},\{(0,2),(1,0),(2,1)\},\{(0,1),(1,2),(2,0)\}.$$

Definition 24.1. We say that a BIBD is *resolvable* if blocks can be partitioned into classes such that in each class, every variety appears on *exactly one block*. To put it geometrically, given a line (a block) and a point (a variety) not on line, there exists *exactly one line* parallel to the first containing the point.

Theorem 24.1. *Let $n \geq 2$ be an integer. If there exist $n-!$ MOLSs of order n, then there exists a resolvable BIBD with $b = n^2+n, v = n^2, k = n, r = n+1, \lambda = 1$.*

Also, what about "completing" a Latin rectangle (LR) (i.e, completing a partial LS)?

Example. We want to complete the following LR:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 3 & 2 & 1 \end{pmatrix}.$$

Adding these two rows will complete the partial LS.

$$\begin{pmatrix} 1 & 2 & 4 & 0 & 3 \\ 2 & 3 & 1 & 4 & 0 \end{pmatrix}$$

But is this possible for every partial LS? The answer is yes.

Theorem 24.2. *Let L be an $m \times n$ LR based on $\mathbb{Z}/n\mathbb{Z}$ with $m < n$. Then L has a completion.*

Remark. If $m > n$, then we can just take the transpose of that LR, complete, and then transpose it back. So there is no loss of generality even though we assume $m < n$.

Proof. It suffices to show that an $m \times n$ LR can be extended to a $(m+1) \times n$ LR – note that this will produce another LR, so we can extend that LR by adding a new row, and so forth, until we reach the completion. Let $\mathfrak{A} = (A_0, \ldots, A_{n-1})$ where $A_i := \{x \in \mathbb{Z}/n\mathbb{Z} : x \text{ is missing in column } i\}$. All we need to do is find a SDR for $\mathfrak{A}$: we need to show that the marriage condition holds for $\mathfrak{A}$: Pick any subcollection $A_{i_1}, \ldots, A_{i_k}$, and show that $|A_{i_1} \cap \cdots \cap A_{i_k}| \geq k$. But then

$$k(n-m) = |A_{i_1}| + \cdots + |A_{i_k}| \leq |A_{i_1} \cup \cdots \cup A_{i_k}|(n-m),$$

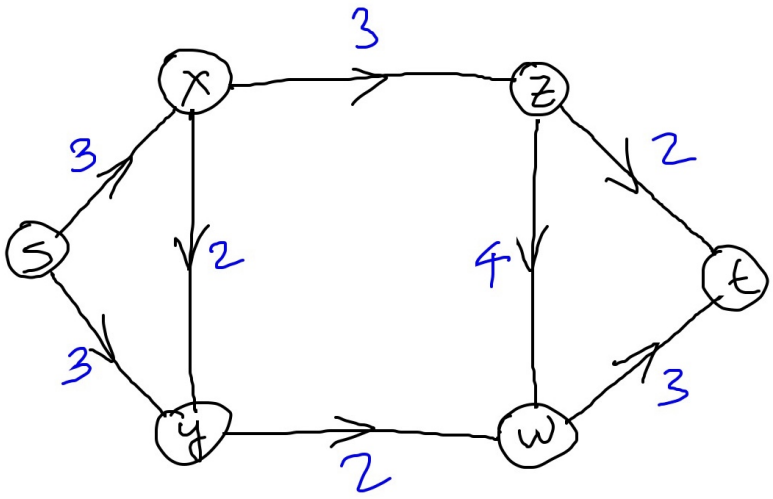
so $|A_{i_1} \cup \cdots \cup A_{i_k}| \geq k$. So there exists an SDR, so it's possible to extend LR by a row. □

How one can extend a LR, and how one can find an SDR?

25. November 1: Networks (Section 13.2)

Definition 25.1. A *network* $N = (V, A, s, t, c)$ is a directed graph (V, A), where V is a set of vertices, and A is a collection of ordered pairs ("arcs") of V, with two distinct vertices s (source) and t (target), in which each arc α has a non-negative weight $c(\alpha)$ (the *capacity* of α).

Example. Let $V = \{s, x, y, z, w, t\}$ and $A = \{(s,x), (s,y), (x,y), (x,z), (z,w), (y,w), (z,t), (w,t)\}$. Then the following graph is an example of a directed graph.



Definition 25.2. A *flow* f on network N is a function $f : A \to \mathbb{R}_{\geq 0}$ such that:

(i) $0 \leq f(\alpha) \leq c(\alpha)$ for all $\alpha \in A$

(ii) Let $i(\alpha)$ be an initial vertex of α and $\tau(\alpha)$ a terminal vertex of α. Then $\sum_{i(\alpha)=x} f(\alpha) = \sum_{\tau(\alpha)=x} f(\alpha)$ for all $x \neq s, t$, i.e., flow in = flow out.

Let U be a subset of vertices containing s but not t, and define

$$\overrightarrow{U} = \{\alpha : i(\alpha) \in U, \tau(\alpha) \notin U\}$$
$$\overleftarrow{U} = \{\alpha : \tau(\alpha) \in U, i(\alpha) \notin U\}.$$

Example. Using the same graph in the first example, we see that $\overrightarrow{U} = \{(s,y),(x,z),(w,t),(x,y)\}$ and $\overleftarrow{U} = \{(y,w),(z,w)\}$.

Lemma 25.1. *Let f be a flow in network $N = (V, A, s, t, c)$ and let U be a set of vertices containing s but not t. Then*

$$\sum_{\alpha \in \overrightarrow{U}} f(\alpha) - \sum_{\alpha \in \overleftarrow{U}} f(\alpha) = \underbrace{\sum_{i(\alpha)=s} f(\alpha) - \sum_{\tau(\alpha)=s} f(\alpha)}_{\text{value of the flow}}.$$

Proof. Consider

$$\sum_{x \in U} \left(\sum_{i(\alpha)=x} f(\alpha) - \sum_{\tau(\alpha)=x} f(\alpha) \right). \qquad (\star)$$

On one hand,

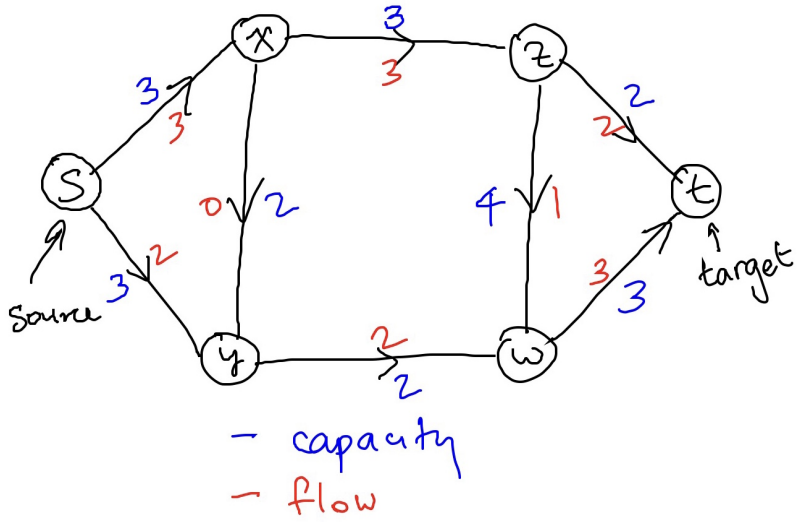
$$(??) = \sum_{i(\alpha)=s} f(\alpha) - \sum_{\tau(\alpha)=s} f(\alpha).$$

On the other hand,

$$\begin{aligned}(??) &= \sum_{x \in U} \sum_{i(\alpha)=x} f(\alpha) - \sum_{x \in U} \sum_{\tau(\alpha)=x} f(\alpha) \\ &= \sum_{i(\alpha) \in U} f(\alpha) - \sum_{\tau(\alpha) \in U} f(\alpha) \\ &= \sum_{\alpha \in \overrightarrow{U}} f(\alpha) - \sum_{\alpha \in \overleftarrow{U}} f(\alpha).\end{aligned}$$

□

Example. Flow in has to be equal to flow out for any point.



Definition 25.3. A *max flow* f is a flow that has the largest value.

In case where all capacities are integers, we find the maximum flow (it will have all integer flows on all arcs).

Definition 25.4. A *cut* in a network $N = (V, A, s, t, c)$ is a set C of arcs such that path from s to t contains at least one arc in C. The *capacity* $\text{cap}(C)$ *of cut* C is the sum of the capacities in C. A cut is a *minimum cut* provided it has the smallest capacity amongst all cuts in N.

Lemma 25.2. *Every minimal cut is of the form* $\overrightarrow{U}$ *for some set* U *of vertices containing* s *but not in* t*.*

Proof. This is Lemma 13.2.2 in the text. □

Theorem 25.1. *Let* $N = (V, A, s, t, c)$ *be a network. Then the maximum value of a flow in* N *is the maximum capacity of a cut in* N *(i.e., capacity of some minimum cut). If all capacities on all arcs are integers, then there is a maximum flow in which all values are integers.*

Proof (sketch). For each flow and each cut C, we show that $\text{val}(C) \leq \text{cap}(C)$. Without loss of generality, C is of the form $\overrightarrow{U}$.

$$\begin{aligned}\text{val}(f) &= \sum_{i(\alpha)=s} f(\alpha) - \sum_{\tau(\alpha)=s} f(\alpha) \\ &= \sum_{\alpha\in\overrightarrow{U}} f(\alpha) - \sum_{\alpha\in\overleftarrow{U}} f(\alpha) \\ &\leq \sum_{\alpha\in\overrightarrow{U}} f(\alpha) \leq \sum_{\alpha\in\overrightarrow{U}} c(\alpha) = c(\overrightarrow{U}).\end{aligned}$$

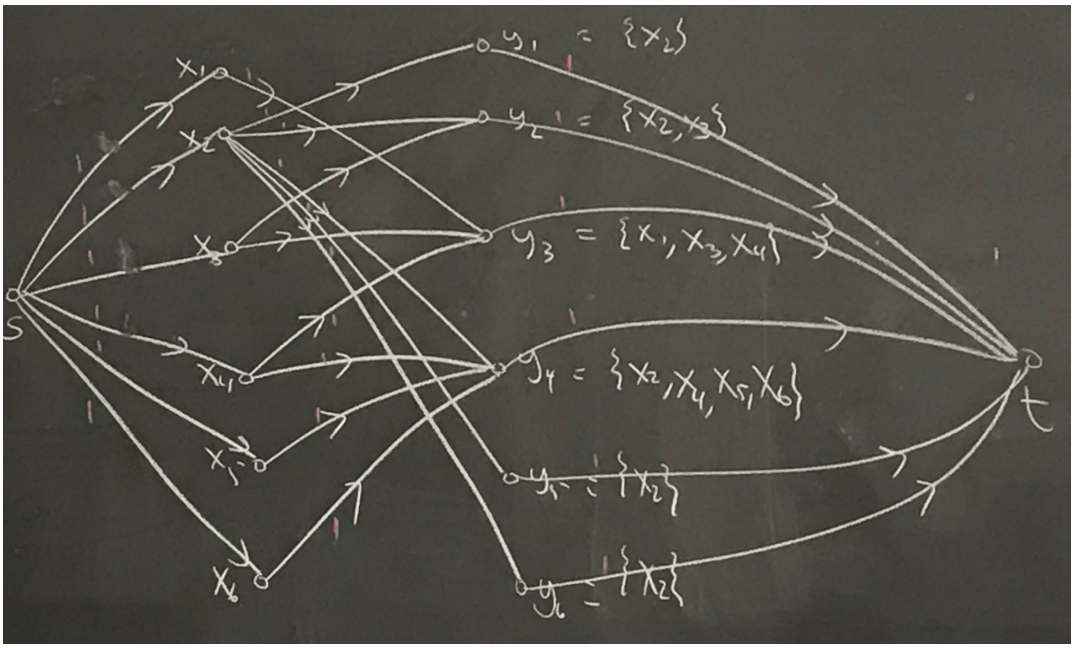
Next show, we show that there exist a flow $\hat{f}$ and a cut $\hat{C}$ such that $\text{val}(\hat{f}) = \text{cap}(\hat{C})$. It then follows that $\hat{f}$ is a maximum flow, and $\hat{C}$ is a minimum cut.. We will prove this by displaying an algorithm that gives us this output.

(1) Start with a flow (the zero flow: 0 on each arc)
(2) We either improve flow, or we stop as we have a max flow:
  (0) $U \leftarrow \{s\}$
  (1) If there exists an arc $\alpha = (x, y)$ with either:
    (i) $x \in U, y \notin U, f(\alpha) < c(\alpha)$; or
    (ii) $x \notin U, y \in U, f(\alpha) > 0$.
    For the first case, put $y \in U$; for the second case, put $x \in U$.
  In the end, output U; if $t \in U$ then we can increase the flow. If $t \notin U$, then we achieve a maximum flow. □

One interesting application of flow is finding an SDR. Consider $S_1 \cup \cdots \cup S_n = \{x_1, \ldots, x_m\}$. Construct a digraph from $S_1, \ldots, S_n$ to $x_1, \ldots, x_m$, where S_k and x_i are connected (from S_k to x_i) if and only if $x_i \in S_k$. Let s be the source (and flow out to each of S_k); and let t be the target (flow into t from x_i). Let each capacity be 1. Then there exists a maximum flow with all integer flows on all arcs. In fact, any good flow represents a SDR. Note that if that is not the case, there exists a point x_i such that more than 1 flows into x_i then to t, so this is not a good flow.

26. November 20

Consider the bipartite graph below, where $y_1 = \{x_2\}, y_2 = \{x_2, x_3\}, y_3 = \{x_1, x_3, x_4\}, y_4 = \{x_2, x_4, x_5, x_6\}, y_5 = \{x_2\}, y_6 = \{x_2\}$. We want to find an SDR or a maximum matching in the given graph. So this is the same problem but phrased differently.



We will see that we can have an SDR for up to four sets. An example would be $(y_1, y_2, y_3, y_4) = (x_2, x_3, x_1, x_4)$.

Definition 26.1. Let $D = (V, A)$ be a digraph (directed graph). Then the *indegree of* x (resp. *outdegree*) in D is

$$\text{indegree}_D\, x = |\{\alpha \in A : \tau(\alpha) = x\}|$$
$$\text{outdegree}_D\, x = |\{\alpha \in A : i(\alpha) = x\}|.$$

Remark. Loops contribute 1 to both the indegree and the outdegree.

Theorem 26.1. *In digraph* $D = (V, A)$,

$$\sum_{x \in V} \text{indegree}_D\, x = \sum_{x \in V} \text{outdegree}_D\, x.$$

Definition 26.2. D is *strongly connected* iff for all $x, y \in V$ there exists a directed path from x to y and a directed path from y to x. A *strongly connected component of* D is a maximal strongly connected subdigraph. The *condensation of digraph* D $\rho(D)$ has as its vertices the strongly connected components $c_1, c_2, \ldots, c_k$ of D with an arc from c_i to c_j if and only if there is an arc in D, say $\alpha = (x, y)$ where $x \in c_i$ and $y \in c_j$.

Definition 26.3. A *tournament* is an orientation of K_n.

Theorem 26.2. *In a tournament* $T = (V, A)$*, there is a vertex* v *such that for any other vertex* x*, either* v *"beats"* x *or there is a vertex* y *such that* v *beats* y*, and* y *beats* x*.*

Proof. Pick a vertex v that beats the most other vertices. We will prove that this v satisfies the desired properties. □

Definition 26.4. A *transitive tournament* is a tournament whose arc set is transitive (if $(x, y), (y, z) \in A$, then $(x, z) \in A$). So if a tournament is transitive, then we can list the vertices as $p_1, \ldots, p_n$ such that p_i beats all to the right of it (note that the tournament is a linear total order).

Definition 26.5. A digraph *has property* P_k if for all disjoint subsets U, W, Y, Z each of size k, there is a point $p \notin U \cup W \cup Y \cup Z$ such that there is an arc directed from p to every point in U and Y, an arc directed from every point in W to p, but no arc connecting between p and any point in Z.

Can we construct a digraph with such property? Start by forming a *random* digraph on $\{1, 2, \ldots, n\}$, choosing (x, y) with probability $1/2$. Then given any disjoint sets U, W, Y, Z, each of size k,

$$\Pr(\text{has property } P_k) = \left(\left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^k\right)^4 = \left(\frac{1}{2}\right)^{8k}$$

$$\Pr(p \text{ is not joined properly to } U, W, Y, Z) = 1 - \left(\frac{1}{2}\right)^{8k}$$

$$\Pr(\text{no point } p \text{ outside of } U, W, Y, Z \text{ is joined properly}) = \left(1 - \left(\frac{1}{2}\right)^{8k}\right)^{n-4k}.$$

Thus – let $E_{U,W,Y,Z}$ denote the event that there is no good point for U, W, Y, Z.

$$\begin{aligned}
&\Pr(\text{for some } U, W, Y, Z \text{ there is no good point}) \\
&= \Pr\left(\bigcup_{U,W,Y,Z} E_{U,W,Y,Z}\right) \\
&\leq \sum_{U,W,Y,Z} \Pr(E_{U,W,Y,Z}) \\
&= \binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k}\binom{n-3k}{k}\left(1 - \left(\frac{1}{2}\right)^{8k}\right)^{n-4k} \\
&\leq n^k n^k n^k n^k \left(1 - \left(\frac{1}{2}\right)^{8k}\right)^{n-4k}.
\end{aligned}$$

Let $t := n^{4k}(1 - 2^{-8k})^{n-4k}$, and take log on both sides. Then

$$\log t = 4k \log n + (n - 4k) \log\left(1 - \left(\frac{1}{2}\right)^{8k}\right).$$

But since $1 - 2^{-8k}$ is less than 1, $\log(1 - 2^{-8k}) < 1$. Hence $\log t \to -\infty$, so $t \to 0$. Hence, there exists a digraph with property P_k.

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2

E-mail address: hsyang@dal.ca