Observation 1: The injective k-tuples $\vec{s} \in S^k$ such that the set of entries of $\vec{s}$ is W are exactly the injective k-tuples $\vec{s} \in W^k$.

[Proof: Each injective k-tuple $\vec{s} \in W^k$ has the property that its set of entries is W, because it is a k-element subset of the k-element set W.]

$$= \sum_{\substack{W \subseteq S; \\ |W| = k}} \underbrace{(\# \text{ of injective } k\text{-tuples } \vec{s} \in W^k)}_{= |W^k_{dist}| = k^{\underline{k}} \text{ (by Prop. 2.22, since } |W| = k)}$$

$$= \sum_{\substack{W \subseteq S; \\ |W| = k}} \underbrace{k^{\underline{k}}}_{= k!} = \sum_{\substack{W \subseteq S; \\ |W| = k}} k! = k! \cdot (\# \text{ of } W \subseteq S \text{ such that } |W| = k).$$

Thus, $(\# \text{ of } W \subseteq S \text{ such that } |W| = k) = \underbrace{|S^k_{dist}|}_{= n^{\underline{k}}} / k!$

$$= n^{\underline{k}} / k! = \binom{n}{k}. \qquad \square$$

2.6. The polynomial identity trick revisited

4th proof of Thm. 2.18 when $x \in \mathbb{N}$ and $y \in \mathbb{N}$.

Rename x and y as a and b. So we must prove:

(8) $$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}.$$

Consider the polynomial $(1+X)^{a+b}$. Compare

$$(1+X)^{a+b} = \sum_{m=0}^{a+b} \binom{a+b}{m} X^m \quad \text{(by binom. formula)}$$

$$\overset{\circ}{=} \sum_{m} \binom{a+b}{m} X^m$$

with $$(1+X)^{a+b} = \underbrace{(1+X)^a}_{\substack{= \sum_i \binom{a}{i} X^i \\ \text{(by binom. formula)}}} \cdot \underbrace{(1+X)^b}_{\substack{= \sum_j \binom{b}{j} X^j \\ \text{(by binom. formula)}}}$$

$$= \left(\sum_i \binom{a}{i} X^i\right)\left(\sum_j \binom{b}{j} X^j\right) = \sum_{(i,j) \in \mathbb{N} \times \mathbb{N}} \binom{a}{i}\binom{b}{j} X^i X^j$$

$$= \sum_{(i,j) \in \mathbb{N} \times \mathbb{N}} \binom{a}{i} \binom{b}{j} X^{i+j}$$

$$= \sum_{k \in \mathbb{N}} \underbrace{\left(\sum_{\substack{(i,j) \in \mathbb{N} \times \mathbb{N}; \\ i+j=k}} \binom{a}{i} \binom{b}{j} \right)}_{= \sum_{i=0}^{k} \binom{a}{i} \binom{b}{k-i}} X^k$$

$$= \sum_{k \in \mathbb{N}} \left(\sum_{i=0}^{k} \binom{a}{i} \binom{b}{k-i} \right) X^k$$

$$= \sum_{m \in \mathbb{N}} \left(\sum_{k=0}^{m} \binom{a}{k} \binom{b}{m-k} \right) X^m$$

(here, we renamed k and i as m and k),

we get

$$\sum_m \binom{a+b}{m} X^m = \sum_m \left(\sum_{k=0}^{m} \binom{a}{k} \binom{b}{m-k} \right) X^m .$$

These are equal as polynomials; thus, corresponding coefficients are equal. In other words,

$$\binom{a+b}{m} = \sum_{k=0}^{m} \binom{a}{k} \binom{b}{m-k} \qquad \forall\, m \in \mathbb{N}.$$

$\square$

Apply this to $m = n$, and get (8).

<u>Remark:</u> A similar argument proves the identity

(9) $$\sum_{i=0}^{m} (-1)^i \binom{n}{i} \binom{n}{m-i} = \begin{cases} (-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases}$$

for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Indeed, (9) is obtained from expanding (again using the binom. formula)

$$(1-X)^n \cdot (1+X)^n = (1-X^2)^n$$

and comparing coefficients.

In particular, if $m = n$, then (9) simplifies to

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i}^2 = \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

We'll see more of this method later.

2.7. Destructive interference & the Principle of Inclusion and Exclusion

Recall:

- For any finite sets A and B, we have $|A \cup B| = |A| + |B| - |A \cap B|$.
- For any finite sets A, B and C, we have
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Generally:

Theorem 2.23 (Principle of Inclusion & Exclusion (short PIE), or the Sylvester sieve formula). Let $n \in \mathbb{N}$. Let $A_1, A_2, \ldots, A_n$ be finite sets.

(a) We have
$$\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_n| = {} & |A_1| + |A_2| + \cdots + |A_n| \\
& - |A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{n-1} \cap A_n| \\
& + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots \\
& - \cdots \\
& + \cdots \\
& \pm \cdots \\
& + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.
\end{aligned}$$

Or, in rigorous terms:

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| .$$

Here, $\bigcap_{i \in I} A_i$ means "the intersection of all A_i with $i \in I$"

(so $\bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$ if $I = \{i_1, i_2, \ldots, i_k\}$).

(LaTeX: \bigcup, \bigcap)

(b) Let U be a finite set that contains all A_i's as subsets.
Then,

$$\left| U \setminus \bigcup_{i=1}^{n} A_i \right| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| ,$$

where we set $\bigcap_{i \in \varnothing} A_i = U$.

There are several proofs, e.g. [Galvin, §16] has two.

Thm. 2.24 ("destructive interference"). Let G be a finite set.

Then,
$$\sum_{I \subseteq G} (-1)^{|I|} = [G = \varnothing].$$

Ex: If $G = \{1,2\}$, then
$$\sum_{I \subseteq G} (-1)^{|I|} = (-1)^{|\varnothing|} + (-1)^{|\{1\}|} + (-1)^{|\{2\}|} + (-1)^{|\{1,2\}|}$$
$$= \cancel{1} + \cancel{(-1)} + \cancel{(-1)} + \cancel{1} = 0$$
$$= [\{1,2\} = \varnothing].$$

1st proof:
$$\sum_{I \subseteq G} (-1)^{|I|} = \sum_{k=0}^{|G|} \binom{|G|}{k} (-1)^k$$
(since $|I| = k$ holds for exactly $\binom{|G|}{k}$ subsets I of G)
$$= \sum_{k=0}^{|G|} (-1)^k \binom{|G|}{k} = [|G| = 0] \quad \text{(by Cor. 2.3)}$$
$$= [G = \varnothing].$$

$\square$

<u>2nd proof (outline):</u> If $G = \varnothing$, then it is obvious.

If $G \neq \varnothing$, then fix some $g \in G$.

Then, the $I \subseteq G$ that contain g are in bijection with the $I \subseteq G$ that don't $(I \mapsto I \setminus \{g\})$, and the addends from the former subsets cancel those from the latter. $\Longrightarrow$ The sum is 0. $\square$

Iverson brackets satisfy the following rules (easy):

<u>Prop. 2.25.</u> (a) If statements $\mathcal{A}$ and $\mathcal{B}$ are equivalent, then $[\mathcal{A}] = [\mathcal{B}]$.

(b) Any statement $\mathcal{A}$ satisfies $[\text{not } \mathcal{A}] = 1 - [\mathcal{A}]$.

(c) If $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k$ are k statements, then

$$[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_k] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \ldots \cdot [\mathcal{A}_k].$$

<u>Prop. 2.26 ("counting by roll-call").</u> Let U be a finite set. Let $S \subseteq U$.

Then,
$$|S| = \sum_{x \in U} [x \in S].$$

Proof: LTTR. $\square$

Proof of Thm. 2.23. (b) Let $x \in U$. Let $G = \{i \in [n] \mid x \in A_i\} \subseteq [n]$.

Now,
$$\sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{\left[x \in \bigcap_{i \in I} A_i\right]}_{\substack{= [x \in A_i \text{ for all } i \in I] \\ = [i \in G \text{ for all } i \in I] \\ = [I \subseteq G]}}$$

$$= \sum_{I \subseteq [n]} (-1)^{|I|} [I \subseteq G]$$

$$= \sum_{\substack{I \subseteq [n]; \\ I \subseteq G}} (-1)^{|I|} \underbrace{[I \subseteq G]}_{=1} + \sum_{\substack{I \subseteq [n]; \\ I \not\subseteq G}} (-1)^{|I|} \underbrace{[I \subseteq G]}_{\substack{=0 \\ (\text{since } I \not\subseteq G)}}$$

$$= \sum_{\substack{I \subseteq [n]; \\ I \subseteq G}} (-1)^{|I|} \underset{(\text{since } G \subseteq [n])}{=} \sum_{I \subseteq G} (-1)^{|I|} \underset{(\text{by Thm 2.24})}{=} [G = \varnothing]$$

$= [\text{there exist no } i \in [n] \text{ such that } x \in A_i]$

$= [x \notin A_i \text{ for all } i \in [n]] = [x \notin \bigcup_{i=1}^{n} A_i]$

(10) $= [x \in U \setminus \bigcup_{i=1}^{n} A_i]$.

This holds for every $x \in U$. Now,

$$\sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{\left| \bigcap_{i \in I} A_i \right|}_{\substack{= \sum_{x \in U} [x \in \bigcap_{i \in I} A_i] \\ \text{(by Prop. 2.26)}}}$$

$$= \sum_{I \subseteq [n]} (-1)^{|I|} \sum_{x \in U} [x \in \bigcap_{i \in I} A_i]$$

$$= \sum_{x \in U} \underbrace{\sum_{I \subseteq [n]} (-1)^{|I|} [x \in \bigcap_{i \in I} A_i]}_{\overset{(10)}{=} [x \in U \setminus \bigcup_{i=1}^{n} A_i]}$$

$$= \sum_{x \in U} [x \in U \setminus \bigcup_{i=1}^{n} A_i] = \left| U \setminus \bigcup_{i=1}^{n} A_i \right| \quad \text{(by Prop. 2.26).}$$

This proves Thm. 2.23 (b).

(a) Let $U = \bigcup_{i=1}^{n} A_i$. Then, $U \setminus \bigcup_{i=1}^{n} A_i = \emptyset$, so that

$$0 = \left| U \setminus \bigcup_{i=1}^{n} A_i \right| \overset{\text{part (b)}}{=\!=\!=} \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|$$

$$= \underbrace{(-1)^{|\emptyset|}}_{=1} \underbrace{\left| \bigcap_{i \in \emptyset} A_i \right|}_{=U} + \sum_{\substack{I \subseteq [n]; \\ I \neq \emptyset}} \underbrace{(-1)^{|I|}}_{= -(-1)^{|I|-1}} \left| \bigcap_{i \in I} A_i \right|$$

$$= |U| - \sum_{\substack{I \subseteq [n]; \\ I \neq \emptyset}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

Thus, $\sum_{\substack{I \subseteq [n]; \\ I \neq \emptyset}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| = |U| = \left| \bigcup_{i=1}^{n} A_i \right|$.

But this proves Thm. 2.23 (a). $\square$

Applications:

Example 1: Recall: A <u>derangement</u> of a set X means a permutation f of X that has no fixed points (i.e., $\nexists\, x \in X$ such that $f(x) = x$).

Let D_n be the # of derangements of $[n]$. What is D_n?

Let $U = \{\text{all permutations of } [n]\}$. Note $|U| = n!$.

For each $i \in [n]$, let $A_i = \{f \in U \mid f(i) = i\}$.

Then, $D_n = \left| U \setminus \bigcup_{i=1}^{n} A_i \right|$ (since the set of derangements of $[n]$ is $U \setminus \bigcup_{i=1}^{n} A_i$)

$$\overset{\text{Thm. 2.23(b)}}{=} \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

But for any $I \subseteq [n]$, we have

$$\left| \bigcap_{i \in I} A_i \right| = \left| \{ f \in U \mid f(i) = i \text{ for all } i \in I \} \right|$$
$$= \left| \{ \text{permutations of } [n] \setminus I \} \right|$$

$$= \underbrace{|[n] \setminus I|}_{=n-|I|}! = (n-|I|)!,$$

so this becomes

$$D_n = \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)! = \sum_{k=0}^{n} (-1)^k (n-k)! \binom{n}{k}$$

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

Thus:

Thm. 2.27: For any $n \in \mathbb{N}$, we have

$$D_n = \sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k} (n-k)!}_{= \frac{n!}{k!}} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Rmk: Thus, $D_n / n! = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx e^{-1}$ for $e = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2.718\ldots$.

It can be shown that $D_n = \operatorname{round}(n!/e)$ when $n > 0$.

Example 2: surjections, again.

Fix $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Compute $\operatorname{sur}(m,n) = (\#$ of surjective maps $[m] \to [n])$.

Set $U = \{\text{maps } [m] \to [n]\}$.

For each $i \in [n]$, let $A_i = \{\text{maps } [m] \to [n] \text{ that miss } i\}$.

(We say that a map f misses i if i is not a value of f.)

Then, $\{\text{surjective maps } [m] \to [n]\} = U \setminus \bigcup_{i=1}^{n} A_i$.

Thus, $\operatorname{sur}(m,n) = \left| U \setminus \bigcup_{i=1}^{n} A_i \right|$

$$\overset{\text{Thm. 2.23(b)}}{=} \sum_{I \subseteq [n]} (-1)^{|I|} \Big| \underbrace{\bigcap_{i \in I} A_i}_{\substack{= \{\text{maps } [m] \to [n] \\ \text{missing all } i \in I\} \\ \cong \{\text{maps } [m] \to [n] \setminus I\}}} \Big|$$

$$= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{\left| \{\text{maps } [m] \to [n] \setminus I\} \right|}_{= |[n]\setminus I|^{|[m]|} = (n-|I|)^m}$$

$$= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)^m = \sum_{i=0}^{n} (-1)^i (n-i)^m \binom{n}{i}$$

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

Thus;

Thm 2.28. For all $m \in \mathbb{N}$ and $n \in \mathbb{N}$, we have

$$\operatorname{sur}(m,n) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m = \sum_{i=0}^{n} (-1)^{n-i} \underbrace{\binom{n}{n-i}}_{=\binom{n}{i}} i^m$$

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

Rmk. HW3 exercise 6(a) (applied to $A_i = 1$) gives

$$\sum_{I \subseteq [n]} (-1)^{n-|I|} |I|^m = \sum_{\substack{(i_1, i_2, \ldots, i_m) \in [n]^m \\ \{i_1, \ldots, i_m\} = [n]}} 1 = sur(m,n).$$

This is equivalent to Thm. 2.28.

Example 3: Euler's ϕ-function.

Recall: Two integers a and b are coprime (aka relatively prime) if $\gcd(a,b)=1$.

Def. The function $\phi: \{1,2,3,\ldots\} \to \mathbb{N}$ (called Euler's totient function, or Euler's ϕ-function) is defined by

$$\phi(u) = (\# \text{ of all } m \in [u] \text{ coprime to } u).$$

Ex: $\phi(2) = |\{1, \cancel{2}\}| = 1.$

$\phi(4) = |\{1, \cancel{2}, 3, \cancel{4}\}| = 2.$

$\phi(6) = |\{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}\}| = 2.$

$\phi(12) = |\{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\}| = 4.$

What is $\phi(n)$ in general? We need an auxiliary identity:

<u>Prop. 2.29.</u> Let $a_1, a_2, \ldots, a_n$ be n numbers. Then:

(a) $$\sum_{I \subseteq [n]} \prod_{i \in I} a_i = (1+a_1)(1+a_2)\cdots(1+a_n).$$

(b) $$\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} a_i = (1-a_1)(1-a_2)\cdots(1-a_n).$$

<u>Proof.</u> (a) Proof by example: $n=3$.

$$1 + a_1 + a_2 + a_3 + a_1 a_2 + a_1 a_3 + a_2 a_3 + a_1 a_2 a_3$$
$$= (1+a_1)(1+a_2)(1+a_3).$$

Rigorously: Induction.

(b) Apply (a) to $-a_i$ instead of a_i. $\square$

Let $p_1, p_2, \dots, p_n$ be the distinct primes dividing u.
Let $U = [u]$. For each $i \in [n]$, let $A_i = \{x \in [u] \mid \underbrace{x \in p_i \mathbb{Z}}_{\substack{\text{this means} \\ p_i \mid x}}\}$.

Then, $\{m \in [u] \text{ coprime to } u\} = U \setminus \bigcup_{i=1}^{n} A_i$.

Hence, $$\phi(u) = \left| U \setminus \bigcup_{i=1}^{n} A_i \right| \overset{\text{Thm. 2.23(b)}}{=\!=\!=} \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

Since $\left| \bigcap_{i \in I} A_i \right| = $ (# of all $m \in [u]$ that are multiples of all the p_i for all $i \in I$)

$= $ (# of all $m \in [u]$ that are multiples of $\prod_{i \in I} p_i$)

$$= \frac{u}{\prod_{i \in I} p_i} \qquad \left(\text{since } \prod_{i \in I} p_i \mid u\right)$$

for each $I \subseteq [n]$, we can rewrite this as

$$\phi(u) = \sum_{I \subseteq [n]} (-1)^{|I|} \frac{u}{\prod_{i \in I} p_i}$$

$$= u \sum_{I \subseteq [n]} (-1)^{|I|} \frac{1}{\prod_{i \in I} p_i} = u \underbrace{\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i}}_{\overset{\text{Prop. 2.29(b)}}{\underset{\text{for } a_i := \frac{1}{p_i}}{=}} \prod_{i \in [n]} \left(1 - \frac{1}{p_i}\right)}$$

$$= u \prod_{i \in [n]} \left(1 - \frac{1}{p_i}\right).$$

Thus:

Thm. 2.30. If u is a positive integer, and if $p_1, p_2, \dots, p_n$ are the distinct primes dividing u, then

$$\phi(u) = u \prod_{i \in [n]} \left(1 - \frac{1}{p_i}\right).$$

2.8. The roots-of-unity filter (introduction).

Def. Given $n \in \mathbb{N}$ and $j \in \mathbb{Z}$ and $u > 0$, we let

$$\binom{n}{\equiv j \bmod u} = \sum_{\substack{k \in \mathbb{Z};\\ k \equiv j \bmod u}} \binom{n}{k}$$

$$= (\text{\# of subsets of } [n] \text{ whose size is } \equiv j \bmod u).$$

Prop. 2.31. Let $n \in \mathbb{N}$. Then,

$$\binom{n}{\equiv 0 \bmod 2} = \frac{2^n + [n=0]}{2} \quad \text{and} \quad \binom{n}{\equiv 1 \bmod 2} = \frac{2^n - [n=0]}{2}.$$

Prop. 2.32. Let $n \in \mathbb{N}$. Then,

$$\binom{n}{\equiv i \bmod 3} = \frac{2^n - (-1)^n}{3} + (-1)^n [n \equiv -i \bmod 3].$$

(HW2 exe 3(b))

What about mod 4?