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

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

$$= \sum_{\substack{\text{WSS;} \ 1W1=k}} \binom{\# \text{of injective } k \text{-tuples } s^k \in W^k}{k}$$

$$= |W^k_{\text{dist}}| = k^k \quad \text{(by Prop. 2.22, since } |1W1|=k)$$

$$= \sum_{\substack{\text{WSS;} \ 1W1=k}} k^k = \sum_{\substack{\text{WSS;} \ 1W1=k}} k! = k!(\# \text{of WSS such that } |1W1|=k).$$

Thus, \(\binom{\# \text{of WSS such that } |1W1|=k}{k} = |S^k_{\text{dist}}| / k!\)

$$= n^k / k! = \binom{n}{k}. \quad \square$$
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:

\[
\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k},
\]

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

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

with

\[
(1+X)^a = \sum_{i} \binom{a}{i} X^i \quad \text{(by binom. formula)}
\]

\[
(1+X)^b = \sum_{j} \binom{b}{j} X^j \quad \text{(by binom. formula)}
\]

\[
= \left( \sum_{i} \binom{a}{i} X^i \right) \left( \sum_{j} \binom{b}{j} X^j \right) = \sum_{(i,j) \in \mathbb{N} \times \mathbb{N}} \binom{a}{i} \binom{b}{j} X^i X^j
\]
\[
\sum_{(i,j) \in \mathbb{N} \times \mathbb{N}} (a_i)(b_j) \times i + j
\]

\[
= \sum_{k=0}^{\infty} \left( \sum_{(i,j) \in \mathbb{N} \times \mathbb{N}, \ i + j = k} (a_i)(b_j) \right) \times k
\]

\[
= \sum_{i=0}^{k} (a_i)(b_{k-i})
\]

\[
= \sum_{k=0}^{\infty} \left( \sum_{i=0}^{k} (a_i)(b_{k-i}) \right) \times k
\]

\[
= \sum_{m=0}^{\infty} \left( \sum_{k=0}^{m} \binom{m}{k} \binom{b}{m-k} \right) \times m
\]

(Here, we renamed \( k \) and \( i \) as \( m \) and \( k \)),

we get
\[
\sum_{m} \left( a + b \right) X^m = \sum_{m} \left( \sum_{k=0}^{m} \binom{a}{k} \binom{b}{m-k} \right) X^m.
\]

These are equal as polynomials; thus, corresponding coefficients are equal. In other words,
\[
\binom{a+b}{m} = \sum_{k=0}^{m} \binom{a}{k} \binom{b}{m-k} \quad \forall \ m \in \mathbb{N}.
\]

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

Remark: A similar argument proves the identity
\[
\sum_{i=0}^{m} (-1)^i \binom{n}{i} \binom{n-i}{m-i} = \begin{cases} 
(-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\
0, & \text{if } m \text{ is odd}
\end{cases}
\]
for all \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Indeed, (9) is obtained from expanding \((1-x)^n \cdot (1+x)^n = (1-x^2)^n\) (again using the binomial formula) 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

\[
|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|
- |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots - |A_{n-1} \cap A_n|
+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots
- \ldots
+ \ldots
+ (-1)^{n-2} |A_1 \cap A_2 \cap \ldots \cap A_n|.
\]
or, in rigorous terms:

\[ \left| \bigcup_{i=1}^{n} A_i \right| = \sum_{I \subseteq [n], |I| \neq 0} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \]

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

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

(LaTeX: \texttt{\bigcap}, \texttt{\bigcup})

(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 \( \bigcap_{i \in \emptyset} A_i = U \).
There are several proofs, e.g. [Galvin, §16] has two. \[\text{Thm. 2.24 ("destructive interference")}.\] Let $G$ be a finite set.

Then,

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

Ex: 1f $G = \{1, 2\}$, then

$$\sum_{I \subseteq G} (-1)^{|I|} = (-1)^{|\emptyset|} + (-1)^{|\{1\}|} + (-1)^{|\{2\}|} + (-1)^{|\{1, 2\}|}
= 1 + (-1) + (-1) + 1 = 0
= [\{1, 2\} = \emptyset].$$

1st proof:

$$\sum_{I \subseteq G} (-1)^{|I|} = \sum_{k=0}^{16} \binom{16}{k} (-1)^k
= \sum_{k=0}^{16} (-1)^k \binom{16}{k} = \sum_{k=0}^{16} (-1)^k \binom{16}{k} = [16! = 0] \quad (\text{by Gr. 2.3})$$

$$= [G = \emptyset].$$
2nd proof (outline): If \( G = \emptyset \), then it is obvious. If \( G \neq \emptyset \), 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 (\( I \rightarrow I \setminus \{g\} \)), and the addends from the former subsets cancel those from the latter. \( \Rightarrow \) The sum is 0. \( \square \)

Inverson brackets satisfy the following rules: (easy):

Prop. 2.25. (2) If statements \( \alpha \) and \( \beta \) are equivalent, then \( [\alpha] = [\beta] \).

(b) Any statement \( \alpha \) satisfies \( [\neg \alpha] = 1 - [\alpha] \).

(c) If \( \alpha_1, \alpha_2, \ldots, \alpha_k \) are \( k \) statements, then
\[
[\alpha_1 \land \alpha_2 \land \ldots \land \alpha_k] = [\alpha_1] \cdot [\alpha_2] \cdot \ldots \cdot [\alpha_k].
\]

Prop. 2.26 ("counting by roll-cell"). Let \( U \) be a finite set. Let \( S \subseteq U \).

Then, \( |S| = \sum_{x \in U} [x \in S] \).
Proof of Thm. 2.23, (b) let $x \in U$, let $G = \{ i \in [n] \mid x \in A_i \} \subseteq [n]$.

Now, $\sum_{i \in [n]} (-1)^{|I|} \left[ x \in \bigcap_{i \in I} A_i \right]$

= $\left[ x \in A_i \text{ for all } i \in I \right]$

= $\left[ i \in G \text{ for all } i \in I \right]$

= $\left[ I \subseteq G \right]$

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

= $\sum_{I \subseteq [n]; I \subseteq G} (-1)^{|I|} \left[ I \subseteq G \right] + \sum_{I \subseteq [n]; I \notin G} (-1)^{|I|} \left[ I \subseteq G \right]$

= $1$ (since $I \subseteq G$)

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

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

= $\left[ G = \emptyset \right]$ (by Thm 2.24)
there exist no \( i \in [n] \) such that \( x \in A_i \) \]
\[
= [x \notin A_i \text{ for all } i \in [n]] = [x \notin \bigcup_{i=1}^{n} A_i]
\]
\[(10) \quad = [x \in U \setminus \bigcup_{i=1}^{n} A_i].
\]

This holds for every \( x \in U \). Now,
\[
\sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|
\]
\[
= \sum_{x \in U} \left[ x \in \bigcap_{i \in I} A_i \right]
\]
(by Prop. 2.26)
\[
= \sum_{x \in U} \left[ x \in \bigcap_{i \in I} A_i \right]
\]
\[
= \sum_{x \in U} \sum_{I \subseteq [n]} (-1)^{|I|} \left[ x \in \bigcap_{i \in I} A_i \right]
\]
\[
\overset{(10)}{=} [x \in U \setminus \bigcup_{i=1}^{n} A_i].
\]
\[
\sum_{x \in \bigcup_{i=1}^{n} A_i} = |\bigcup_{i=1}^{n} A_i| \quad \text{(by Prop. 2.26)}.
\]

This proves Thm. 2.23 (b).

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

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

\[
= (-1)^0 \cdot \left( \bigcap_{i \in \emptyset} A_i \right) + \sum_{I \supseteq \{n\}, I \neq \emptyset} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|
\]

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

Thus,

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

But this proves Thm. 2.23 (2). \( \square \)
Example 1: Recall: A **derangement** of a set $X$ means a permutation $f$ of $X$ that has no fixed points (i.e., $\forall x \in X$ such that $f(x) = x$).

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

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

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

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

so this becomes

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

\[
= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!
\]

Thus;

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

\[
D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = n! e^{-1}
\]

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

It can be shown that \( D_n = \text{round}(n!/e) \) when \( n > 0 \).
Example 2: surjections, again.

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

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, $\text{sur}(m, n) = |U \setminus \bigcup_{i=1}^{n} A_i|$

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

\[ = \{ \text{maps } [m] \to [n] \text{ missing all } i \in I \} \]

\[ = \{ \text{maps } [m] \to [n \setminus I] \} \]
\[
= \sum_{I \subseteq [n]} (-1)^{|I|} \left| \{ \text{maps } [m] \to [n] \setminus I \} \right|
\]
\[
= |[n] \setminus I|^{|m|} = (n-|I|)^m
\]
\[
= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)^m = \sum_{i=0}^{n} (-1)^i (n-i)^m \binom{n}{i}
\]
\[
= \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m.
\]

Thus,

\[\text{Thm 2.28.} \quad \text{For all } m \in \mathbb{N} \text{ and } n \in \mathbb{N}, \text{ we have}
\]

\[
\text{sur}(m,n) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{n-i} i^m
\]
\[
= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m.
\]
Rmk. HW3 exercise 6(2) (applied to $A_c=1$) gives

$$\sum_{I \subseteq \{n\}} (-1)^{|I|-1} |I|^m = \sum_{(i_1, i_2, \ldots, i_m) \in \{n\}^m \atop \{i_1, i_2, \ldots, i_m\} = \{n\}} 1 = \text{sr}(m, n).$$

This is equivalent to Thm. 2.28.

Example 3: Euler's $\phi$-function.

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

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

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

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

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

$\phi(6) = \left| \{1, 2, 3, 4, 5, 6\} \right| = 2$. 
\[ \phi(12) = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 23\} = 4. \]

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

Prop. 2.29. Let \( a_1, a_2, \ldots, a_n \) be \( n \) numbers. Then:

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

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

**Proof.** (a) Proof by example: \( n = 3. \)

\[ 1 + a_1 + a_2 + a_3 + a_1a_2 + a_1a_3 + a_2a_3 + a_1a_2a_3 \]

\[ = (1 + a_1)(1 + a_2)(1 + a_3). \]

Rigorously: Induction.

(b) Apply (a) to \(-a_i\) instead of \(a_i\). \( \square \)
Let $p_1, p_2, \ldots, p_n$ be the distinct primes dividing $u$.

Let $U = \{u\}$. For each $i \in [n]$, let $A_i = \{x \in \mathbb{Z} \mid x \in p_i \mathbb{Z}\}$.

Then, \{m \in \mathbb{Z} \mid \text{coprime to } u\} = U \setminus \bigcup_{i=1}^{n} A_i.

Hence, \(\phi(u) = \left| \bigcup_{i=1}^{n} A_i \right| \geq \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|\).

Since \(\left| \bigcap_{i \in I} A_i \right| = \left(\text{# of all } m \in \mathbb{Z} \text{ that are multiples of all the } p_i \text{ for all } i \in I\right)\)

\(= \left(\text{# of all } m \in \mathbb{Z} \text{ that are multiples of } \prod_{i \in I} p_i\right)\)

\(= \frac{u}{\prod_{i \in I} p_i} \quad (\text{since } \prod_{i \in I} p_i \mid u)\)

for each $I \subseteq [n]$, we can rewrite this as
\[ \phi(u) = \sum_{I \subseteq \{\mathbb{N}\}} (-1)^{|I|} \frac{u}{\prod_{i \in I} p_i} \]

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

\[ \overset{\text{Prop. 2.29(b)}}{=} \frac{1}{\prod_{i \in \mathbb{N}} (1 - \frac{1}{p_i})} \]

Thus,

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

\[ \phi(u) = u \prod_{i \in \mathbb{N}} (1 - \frac{1}{p_i}) \]
2.8. The roots-of-unity filter (introduction).

**Def.** Given \( n \in \mathbb{N} \) and \( j \in \mathbb{Z}, \) for \( n > 0, \) we let

\[
\left( \begin{array}{c}
n \\ \equiv j \mod u \end{array} \right) = \sum_{\substack{k \in \mathbb{Z}; \\ k \equiv j \mod u}} \binom{n}{k}
\]

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

**Prop. 2.31.** Let \( n \in \mathbb{N}. \) Then,

\[
\left( \begin{array}{c}
n \\ \equiv 0 \mod 2 \end{array} \right) = \frac{2^n + [n=0]}{2} \quad \text{and} \quad \left( \begin{array}{c}
n \\ \equiv 1 \mod 2 \end{array} \right) = \frac{2^n - [n=0]}{2}.
\]

**Prop. 2.32.** Let \( n \in \mathbb{N}. \) Then,

\[
\left( \begin{array}{c}
n \\ \equiv i \mod 3 \end{array} \right) = \frac{2^n - (-1)^i}{3} + (-1)^i [n \equiv -i \mod 3].
\]

(HW2 exe 3(b))

What about \( \mod 4? \)