Posets Have No Loops

- If \((A, R)\) is a poset, then there do not exist distinct \(x_1, x_2, \ldots, x_n \in A, n \geq 2\), such that

\[(x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n), (x_n, x_1) \in R.\]

- Suppose \((x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n), (x_n, x_1) \in R\) instead.

- By transitivity, \((x_1, x_i), (x_i, x_1) \in R\) for \(2 \leq i \leq n\).

- By antisymmetry (p. 328),

\[x_1 = x_2 = \cdots = x_n,\]

a contradiction.
Maximal and Minimal Elements of Posets

- Let \((A, \mathcal{R})\) be a poset.

- \(x \in A\) is a **maximal element** of \(A\) if \((x, a) \notin \mathcal{R}\) for all \(a \in A\) and \(a \neq x\).\(^a\)
  - The poset \((\{1, 2, 3, 4, 5, 6, 7, 8\}, \mid)\) on p. 355 has 4 maximal elements: 5, 6, 7, 8 as none of them divides a number in \(\{1, 2, 3, 4, 5, 6, 7, 8\}\).

- \(y \in A\) is a **minimal element** of \(A\) if \((b, y) \notin \mathcal{R}\) for all \(b \in A\) and \(b \neq y\).
  - The poset \((\mathbb{Z}^+, \leq)\) has minimal element 1 but no maximal elements.

\(^a\)It does not imply \((a, x) \in \mathcal{R}\).
Maximal and Minimal Elements of Finite Posets

• Let \((A, \mathcal{R})\) be a finite poset.

• For every \(y \in A\), there exists a minimal element \(x \in A\) such that \((x, y) \in \mathcal{R}\).
  
  – If \(y\) is a minimal element, we are done as \((y, y) \in \mathcal{R}\).
  
  – Otherwise, suppose \(y\) is not a minimal element.
  
  – Then by the definition of minimality, there must be an \(x_1 \notin \{y\}\) such that \((x_1, y) \in \mathcal{R}\).
  
  – If \(x_1\) is minimal, then we are done.

\(^a\)It is possible that \(x = y\).
Maximal and Minimal Elements of Finite Posets (continued)

- (continued)
  - Otherwise, there is an $x_2$ such that $(x_2, x_1) \in R$.
  - Furthermore, $x_2 \notin \{x_1, y\}$ (p. 356).
  - If $x_2$ is minimal, then we are done by transitivity.
  - Otherwise, we continue the procedure.
Maximal and Minimal Elements of Finite Posets (concluded)

• (continued)
  – As $A$ is finite, eventually we will reach an $x_n$ such that we can no longer find an $x \not\in \{x_n, x_{n-1}, \ldots, x_1, y\}$ and $(x, x_n) \in R$.
  – This $x_n$ is minimal.

• Similarly, for every $x \in A$, there is a maximal element $y \in A$ such that $(x, y) \in R$. 
Existence of Maximal and Minimal Elements

- If $A$ is a finite poset, then $A$ has a maximal and a minimal element.
  - Pick any element and apply the procedures on pp. 358ff.

- Alternatively, the topological sorting algorithm (p. 368) returns a maximal element as $v_1$ and a minimal element as $v_n$.

- The poset ($\{1, 2, 3, 4, 5, 6, 7, 8\}$, $|$) on p. 355 have 4 maximal elements: 5, 6, 7, and 8.

- It has only 1 minimal element: 1.
Existence of Maximal and Minimal Elements (concluded)

• So a poset can have more than one maximal element and/or more than one minimal element.

• If \((A, \mathcal{R})\) is a finite poset, then \(A\) has a minimal element \(x\) and a maximal element \(y\) such that \((x, y) \in \mathcal{R}\).
  - Start with a maximal element \(y\), which exists (p. 361).
  - There exists a minimal element \(x \in A\) such that \((x, y) \in \mathcal{R}\) (p. 358).
Ranking of Finite Posets\(^a\)

- Elements of a *finite* poset \((A, R)\) can be ranked.\(^b\)
- We can output a ranking, starting with the “smallest” element, as follows.
  - Pick any minimal element \(x \in A\), which exists (361).
  - Remove \(x\) from \(A\) after outputting it and repeat.\(^c\)

\(^a\)Contributed by Mr. Asger K. Pedersen (T02202107), Mr. Johnny Lee (B02902018), and Mr. Larry Hsiang-Yu Lan (B02902123) on April 24, 2014.

\(^b\)Compare p. 327.

\(^c\)After that you still have a poset (prove it!).
Total Order

• Let \((A, \mathcal{R})\) be a poset.

• \(A\) is **totally ordered** if for all \(x, y \in A\),

  either \((x, y) \in \mathcal{R}\) or \((y, x) \in \mathcal{R}\).

  – Recall the definition of tournaments (p. 325).

• This \(\mathcal{R}\) is called a **total order** or a **linear order**.
  
  – \((\mathbb{Z}, \leq)\), \((\mathbb{Q}, \leq)\), and \((\mathbb{R}, \leq)\) are total orders.
Number of Totally Ordered Sets

**Lemma 56** If $|A| = m$, then there are $m!$ totally ordered sets on $A$.

- Every linear order of the elements of $A$ defines a distinct total order.
- So there are $m!$ relations on $A$ that are total orders.
Relation Matrices of Total Orders

• Let $\mathcal{R}$ be a total order on $A$ with $m = |A|$. 

• Its relation matrix $M(\mathcal{R})$ has $m(m + 1)/2$ 1s.
  
  – Reorder the rows and columns by increasing ranks (p. 363).
  
  – Then

  $$M(\mathcal{R})_{i,j} = 1 \quad \text{if and only if} \quad i \leq j.$$ 

  – The matrix is now an upper triangular matrix.

  – The total number of 1s is therefore

  $$m + \binom{m}{2} = \frac{m(m + 1)}{2}.$$
Topological Sort

- Given a partial order $\mathcal{R}$ represented as a Hasse diagram.
- The topological sorting algorithm produces a total order $\mathcal{T}$ for which $\mathcal{R} \subseteq \mathcal{T}$.
  - The total order needs only honor those $(x, y)$ in $\mathcal{R}$.
  - The total order may not be unique.
  - The partial order on p. 355 gives rise to one total order
    \[1, 2, 4, 3, 8, 7, 6, 5.\tag{44}\]
    - $1, 2, 4, 3, 8, 7, 5, 6$ is another total order.
    - Both honor the relations in the Hasse diagram.
The Topological Sorting Algorithm

1: $H_1$ is the input Hasse diagram; $\{|A| = n.\}$

2: for $k = 1, 2, \ldots, n$ do

3: Pick any $v_k \in H_k$ such that no edge in $H_k$ starts from $v_k$; \{A maximal element, which exists (p. 361).\}

4: if $k = n$ then

5: return $v_n, v_{n-1}, \ldots, v_1$; \{(v_i, v_{i-1}) \in \mathcal{R}, i = 2, 3, \ldots, n.\}\}

6: end if

7: Remove $v_k$ and all edges that terminate at $v_k$ to yield $H_{k+1}$; \{ $H_{k+1}$ remains a Hasse diagram (prove it!).\}

8: end for
Least and Greatest Elements of Posets

- Let $(A, \mathcal{R})$ be a poset.
- $x \in A$ is a **least element** if $(x, a) \in \mathcal{R}$ for all $a \in A$.
- $y \in A$ is a **greatest element** if $(b, y) \in \mathcal{R}$ for all $b \in A$.

- Least element and greatest element, if they exist, are unique.
  - For example, suppose $x, y$ are both greatest elements.
  - Then $(x, y) \in \mathcal{R}$ and $(y, x) \in \mathcal{R}$, which imply $x = y$ because of antisymmetry (p. 328).

- $(A, \mathcal{R})$ is **well-ordered** if $\mathcal{R}$ is a total order and every nonempty subset of $A$ has a least element.\(^a\)

\(^a\)Recall the well-ordering principle (p. 201).
Maximal vs. Greatest Elements of Posets

- A poset may have multiple maximal elements (p. 357).
- It is possible for a poset to have maximal elements but no greatest elements (p. 357).
- But the greatest element, if it exists, must be a maximal element.
- In fact, the greatest element, if it exists, must be the only maximal element (why?).
- So when a poset has more than 1 maximal element (such as p. 357), it has no greatest element.

\[a\]Contributed by Ms. Li-Yin Wu (B91902051) on October 20, 2003.
Lattices\textsuperscript{a}

- Let \((A, \mathcal{R})\) be a poset with \(B \subseteq A\).
- \(x \in A\) is a \textbf{lower bound} of \(B\) if \((x, b) \in \mathcal{R}\) for all \(b \in B\).
- \(y \in A\) is an \textbf{upper bound} of \(B\) if \((a, y) \in \mathcal{R}\) for all \(a \in B\).
- \(x' \in A\) is a \textbf{greatest lower bound} (\text{glb}) of \(B\) if it is a lower bound of \(B\) and if for all lower bounds \(x''\) of \(B\), \((x'', x') \in \mathcal{R}\).
- \(y' \in A\) is a \textbf{least upper bound} (\text{lub}) of \(B\) if it is an upper bound of \(B\) and if for all upper bounds \(y''\) of \(B\), \((y', y'') \in \mathcal{R}\).
- \((A, \mathcal{R})\) is called a \textbf{lattice} if for all \(x, y \in A\), the elements \(\text{lub}\{x, y\}\) and \(\text{glb}\{x, y\}\) both exist in \(A\).

\textsuperscript{a}Friedrich Schröder (1841–1902).
Examples of Lattices

• $(\mathbb{N}, \leq)$.
  - $\text{lub}\{x, y\} = \max(x, y)$.
  - $\text{glb}\{x, y\} = \min(x, y)$.

• $(2^A, \subseteq)$.\(^a\)
  - $\text{lub}\{S, T\} = S \cup T$.
  - $\text{glb}\{S, T\} = S \cap T$.

\(^a\)Recall that $2^A$ denotes $A$’s power set: $\{B : B \subseteq A\}$ (p. 226).
Partitions

- Let $\emptyset \neq A_i \subseteq A$ for $i \in I$.
- $\{A_i\}_{i \in I}$ is a partition of $A$ if
  - $A = \bigcup_{i \in I} A_i$, and
  - $A_i \cap A_j = \emptyset$ for $i \neq j$.
- $A_i$’s are called blocks.
A Partition

• Let

\[ A_i = \{ x \in \mathbb{Z} : x \equiv i \mod n \} . \]

• Then

\[ \{ A_0, A_1, \ldots, A_{n-1} \} \]

is a partition of \( \mathbb{Z} \).

– Every integer \( x \) is a member of the block \( A_r \), where

\[ r = x \mod n . \]

– Two distinct blocks \( A_i \) and \( A_j \), \( 0 \leq i < j < n \), are disjoint.
Number of Partitions

- The number of ways to partition a set of size $n$ into $k$ blocks is $S(n, k)$, a Stirling number.
  - See p. 267.
  - See Eq. (39) on p. 275 and Eq. (40) on p. 277 for easy-to-use recurrence relations.

- The number of ways to partition a set of size $n$ is $P_n$, the $n$th Bell number (p. 281).
Equivalence Relations

- A relation \( R \) on \( A \) is called an \textbf{equivalence relation} if it is
  1. Reflexive.
  2. Symmetric.
  3. Transitive.
- “=” is an equivalence relation.
- “\( \equiv \) mod \( m \)” is an equivalence relation (p. 375).
- “<” is not an equivalence relation.
Equivalence Classes

• Let $R$ be an equivalence relation on $A$.

• For each $x \in A$, the **equivalence class** of $x$, denoted by $\left[ x \right]$, is defined by

\[
\left[ x \right] = \{ y \in A : (y, x) \in R \}.
\]

  • Anything that is related to $x$ is in $\left[ x \right]$. 

\[\copyright 2017 \text{ Prof. Yuh-Dauh Lyuu, National Taiwan University}\]
Equivalence Classes (concluded)

• Consider the equivalence relation $\equiv \mod n$ on $\mathbb{Z}$ (same remainder after division by $n$).

• Then $[i] = \{ x \in \mathbb{Z} : x \equiv i \mod n \}$.

• $\{[i]\}_{i=0,1,\ldots,n-1}$ is a partition of $\mathbb{Z}$ (p. 375).
Equivalence Classes as Partitions

- Let $\mathcal{R}$ be an equivalence relation on $A$ and $x, y \in A$.

- $x \in [x]$ (so $[x] \neq \emptyset$).

- $(x, y) \in \mathcal{R}$ if and only if $[x] = [y]$.
  
  - Suppose $(x, y) \in \mathcal{R}$.
    
    * Pick any $w \in [x]$.
    * $(w, y) \in \mathcal{R}$ by symmetry and transitivity.
    * Hence, $w \in [y]$.
    * We conclude $[x] \subseteq [y]$.
    * Similarly, $[y] \subseteq [x]$.
  
  - $[x] = [y] \Rightarrow x \in [y] \Rightarrow (x, y) \in \mathcal{R}$.
The Proof (continued)

- \([x] = [y]\) or \([x] \cap [y] = \emptyset\).
  - Suppose \([x] \neq [y]\) but \([x] \cap [y] \neq \emptyset\).
  - Then there is a \(v \in A\) such that \(v \in [x] \cap [y]\).
  - But then \((x, v) \in \mathcal{R}\) and \((v, y) \in \mathcal{R}\).
  - Hence \((x, y) \in \mathcal{R}\) by transitivity.
  - Therefore \([x] = [y]\) by p. 380, a contradiction.
The Proof (concluded)

- As $x \in [x]$, we have

$$\bigcup_{x \in A} [x] = A.$$ 

- Furthermore, distinct equivalence classes are disjoint.

**Corollary 57** *Equivalence classes partition* $A$. 
Equivalence Relations and Partitions

Theorem 58 There is a one-to-one correspondence between the set of equivalence relations on \( A \) and \( A \)'s set of partitions.

- Let \( A \) be a set.
- Any equivalence relation \( \mathcal{R} \) on \( A \) induces a natural partition of \( A \):
  \[
  \{ [a] : a \in A \}.
  \]
  - This partition, written as \( A/\mathcal{R} \), is called the quotient.
The Proof (concluded)

• Conversely, any partition of $A$ gives rise to an equivalence relation on $A$.

  – Define $\mathcal{R}$ by $(x, y) \in \mathcal{R}$ if $x$ and $y$ are in the same block (why?).

• It is not hard to see that our mapping is a one-to-one correspondence.
The Principle of Inclusion and Exclusion
If I am I because you are you,
and if you are you because I am I,
then I am not I,
and you are not you.
— Hassidic rabbi
The First Example

Count the number of 8-bit strings that start with 1 or end with 00.

• The number of 8-bit strings that start with 1 is $2^7 = 128$.
• The number of 8-bit strings that end with 00 is $2^6 = 64$.
• The number of 8-bit strings that start with 1 and end with 00 is $2^5 = 32$.
• Finally, the desired number is

$$128 + 64 - 32 = 160.$$
The Example on P. 27 Revisited

How many ways are there to arrange TALLAHASSEE with no adjacent As?

• Rearrange the characters as AAAEEHLLSST.

• AAAEEHLLSST has 11 characters, among which there are 3 As.

• There are \(\frac{11!}{3!2!1!2!2!1!} = 831,600\) ways to arrange the 11 characters by Eq. (2) on p. 16.

• But some of them are invalid.
The Example on P. 27 Revisited (continued)

- First, treat AA as a single, new character.

- The 10-character string (AA)AEEHLLSST can be arranged in

\[
\frac{10!}{1! \cdot 1! \cdot 2! \cdot 1! \cdot 2! \cdot 2! \cdot 1!} = 453,600
\]

ways.

- But some arrangements of (AA)AEEHLLSST may contain 3 consecutive As, which are counted twice.
  - Such as (AA)AEEHLLSST and A(AA)EEHLLSST.
The Example on P. 27 Revisited (concluded)

- To count them, as before, treat AAA as a single, new character.

- The 9-character string (AAA)EEHLLSST can be arranged in

\[
\frac{9!}{1! 2! 1! 2! 2! 1!} = 45,360
\]

ways.

- The desired number is hence

\[
831,600 - 453,600 + 45,360 = 423,360,
\]

matching the earlier result.
The Setup

- Let $S$ be a set with $|S| = N$.
- Let $c_1, c_2, \ldots, c_t$ be conditions on the elements of $S$.
- $N(a \land b \land c \land \cdots)$ denotes the number of elements of $S$ that satisfy $a \land b \land c \land \cdots$.
- So $N(\overline{c_1} \overline{c_2} \cdots \overline{c_t})$ denotes the number of elements of $S$ that satisfy *none* of the conditions $c_i$. 
The Principle of Inclusion and Exclusion

\[ N(\overline{c_1 c_2 \cdots c_t}) = N - \sum_{1 \leq i \leq t} N(c_i) \]
\[ + \sum_{1 \leq i < j \leq t} N(c_i c_j) \]
\[ - \sum_{1 \leq i < j < k \leq t} N(c_i c_j c_k) + \cdots \]
\[ + (-1)^t N(c_1 c_2 \cdots c_t) \]
\[ = \sum_{k=0}^{t} (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq t} N(c_{i_1} c_{i_2} \cdots c_{i_k}). \]

\(^a\)Da Silva (1814–1878) in 1854 and James Joseph Sylvester (1814–1897) in 1883.
The Proof

- If \( x \in S \) satisfies none of the conditions \( c_i \), then \( x \) should contribute one to \( N(\overline{c_1} \overline{c_2} \cdots \overline{c_t}) \).
  - Indeed, it is counted once, in \( N \).

- If \( x \in S \) satisfies \( 1 \leq r \leq t \) of the conditions \( c_i \), then \( x \) should contribute zero to \( N(\overline{c_1} \overline{c_2} \cdots \overline{c_t}) \).
  - It is counted once in \( N \), \( r \) times in \( \sum_{1 \leq i \leq t} N(c_i) \), \( \binom{r}{2} \) times in \( \sum_{1 \leq i < j \leq t} N(c_i c_j) \), \ldots, and \( \binom{r}{r} \) times in \( N(c_{i_1} c_{i_2} \cdots c_{i_r}) \).
  - By the binomial theorem (p. 53), the total is
    \[
    1 - r + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = (1 - 1)^r = 0,
    \]
    as desired.
The Proof (concluded)

- We have exhausted all cases for $x$.\(^a\)

\(^a\)Contributed by Mr. Cheng-Chang Liu (B01902009) on April 18, 2013.
Simplification of the Notation

• Define

\[ S_0 = N, \]
\[ S_1 = N(c_1) + N(c_2) + \cdots + N(c_t), \]
\[ S_2 = N(c_1c_2) + N(c_1c_3) + \cdots + N(c_{t-1}c_t), \]
\[ \vdots \]
\[ S_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq t} N(c_{i_1}c_{i_2} \cdots c_{i_k}). \] (45)

– Observe that \( S_k \) has \( \binom{t}{k} \) terms.

• The principle of inclusion and exclusion becomes

\[ N(\overline{c_1c_2\cdots c_t}) = S_0 - S_1 + S_2 - \cdots + (-1)^t S_t. \] (46)
A Corollary

• By DeMorgan’s law,

\[ c_1 \lor c_2 \lor \cdots \lor c_t = \neg (\neg c_1 \land \neg c_2 \land \cdots \land \neg c_t). \]

• Hence the number of elements in \( S \) that satisfy at least one of the conditions \( c_i \) equals

\[ N(c_1 \lor c_2 \lor \cdots \lor c_t) = N - N(\overline{c_1} \overline{c_2} \cdots \overline{c_t}). \]
A Corollary (concluded)

• By the inclusion-exclusion principle (46) on p. 395,

\[
N(c_1 \lor c_2 \lor \cdots \lor c_t) = \sum_{1 \leq i \leq t} N(c_i) - \sum_{1 \leq i < j \leq t} N(c_i c_j) + \sum_{1 \leq i < j < k \leq t} N(c_i c_j c_k) - \cdots + (-1)^{t-1} N(c_1 c_2 \cdots c_t) = S_1 - S_2 + \cdots + (-1)^{t-1} S_t.
\]
A Further Simplification

• Often, $N(c_{i_1} c_{i_2} \cdots c_{i_k})$ depends on $k$ only and not on the specific choice of the conditions $c_{i_1}, c_{i_2}, \ldots, c_{i_k}$.

• In this case, define

$$N_k \equiv N(c_{i_1} c_{i_2} \cdots c_{i_k}).$$

• Then

$$S_k = \binom{t}{k} N_k.$$

• The above is much simpler than Eq. (45) on p. 395.
Number of Onto Functions Revisited

- Let $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$.
- Let $c_i$ be the condition that $b_i$ is not in the range of $f : A \rightarrow B$.
- $N(\overline{c_1 c_2 \cdots c_n})$ is the number of onto $f : A \rightarrow B$.
- $N(c_{i_1} c_{i_2} \cdots c_{i_k})$ is the number of

$$f : A \rightarrow B - \{b_{i_1}, b_{i_2}, \ldots, b_{i_k}\}.$$  

- Clearly

$$N(c_{i_1} c_{i_2} \cdots c_{i_k}) = (n - k)^m$$

for distinct $i_1, i_2, \ldots, i_k$. 
Number of Onto Functions Revisited (concluded)

- By the principle of inclusion and exclusion,

\[
N(\overline{c_1} \overline{c_2} \cdots \overline{c_n})
= \sum_{k=0}^{n} (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} N(c_{i_1} c_{i_2} \cdots c_{i_k})
= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n - k)^m
= n! S(m, n),
\]

confirming again Eq. (32) on p. 262.
A Useful Combinatorial Identity

Lemma 59 For $m \leq r \leq n$,
\[
\binom{n-m}{r-m} = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{n-k}{r}.
\]

- In how many ways can we pick $r$ numbers out of $\{1, 2, \ldots, n\}$ and $1, 2, \ldots, m$ must be picked?

- The number is clearly
\[
\binom{n-m}{r-m}.
\]
The Proof (continued)

• Alternatively, let $c_i$ denote the condition that $i$ is not picked, $1 \leq i \leq m$.

• Clearly, $N(\overline{c_1 c_2 \cdots c_m})$ is our goal.

• Now,

$$N(c_i) = \binom{n-1}{r},$$

$$N(c_i c_j) = \binom{n-2}{r}, \quad i \neq j,$$

$$\vdots$$
The Proof (concluded)

• By the inclusion-exclusion principle (46) on p. 395, the desired number equals

\[
N(c_1 c_2 \cdots c_m) = \sum_{k=0}^{n} (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} N(c_{i_1} c_{i_2} \cdots c_{i_k})
\]

\[
= \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{n - k}{r}.
\]
Euler’s Phi Function

- Let \( \phi(n) \) denote the number of positive integers \( m \in \{1, 2, \ldots, n\} \) such that \( \gcd(m, n) = 1 \), where \( n \geq 2 \).
  - \( \phi(p) = p - 1 \) for prime \( p \).
  - \( \phi(1) = 1 \) by convention.

- It is a computationally hard problem without the knowledge of \( n \)’s factorization.
  - Related to the security of some cryptographical systems such as RSA.
Euler’s Phi Function: The Formula

**Theorem 60** Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be the prime factorization of $n$. Then

$$\phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).$$

• Let $c_i$ be the condition that a number from $\{1, 2, \ldots, n\}$ is divisible by $p_i$.

• The desired number is

$$\phi(n) = N(\overline{c_1 \overline{c_2} \cdots \overline{c_t}}).$$

• For distinct $i_1, i_2, \ldots, i_k$,

$$N(c_{i_1} c_{i_2} \cdots c_{i_k}) = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.$$
The Proof (concluded)

• By the principle of inclusion and exclusion,

\[
\phi(n) = N(\overline{c_1 c_2 \cdots c_t})
\]

\[
= \sum_{k=0}^{t} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq t} \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}
\]

\[
= n \sum_{k=0}^{t} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq t} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_k}}
\]

\[
= n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).
\]

(48)
An Example

• Suppose \( n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \).

• Then

\[
\phi(n) = \frac{n}{1 - \frac{1}{p_1}} \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right)
\]

\[
= n \left[1 - \left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}\right) + \left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \frac{1}{p_2 p_3}\right) - \frac{1}{p_1 p_2 p_3}\right].
\]

• This may help convince you that Eq. (48) on 406 is correct.
Application: \( \phi(2^n) \)

\[
\phi(2^n) = 2^n \prod_{p \mid 2^n, p \text{ prime}} \left(1 - \frac{1}{p}\right)
\]

\[
= 2^n \left(1 - \frac{1}{2}\right)
\]

\[
= 2^{n-1}.
\]

Indeed, the only numbers in \( \{1, 2, \ldots, 2^n\} \) relatively prime with 2 are the \( 2^n/2 = 2^{n-1} \) odd numbers.
Euler’s Phi Function Is Multiplicative

- Let $n = m_1 m_2$, where $\gcd(m_1, m_2) = 1$.
- Let $m_1 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the prime factorization of $m_1$.
- Let $m_2 = p_{s+1}^{e_{s+1}} p_{s+2}^{e_{s+2}} \cdots p_t^{e_t}$ be the prime factorization of $m_2$.
- From the formula on p. 405,

\[
\phi(m_1 m_2) = \phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = m_1 \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) m_2 \prod_{i=s+1}^{t} \left(1 - \frac{1}{p_i}\right) = \phi(m_1) \phi(m_2).
\]
A Loose Lower Bound for the Phi Function$^a$

**Theorem 61 (Hardy & Wright (1979))**

\[ \phi(n) > \frac{n}{(6 \ln \ln n)} \text{ for } n > 3. \]

---

$^a$Godfrey Harold Hardy (1877–1947) and Edward Maitland Wright (1906–2005).
Godfrey Harold Hardy (1877–1947)
Permutations without Fixed Points

- Write a permutation $f$ on $\{1, 2, \ldots, n\}$ as
  \[
  \begin{pmatrix}
  1 & 2 & \cdots & n \\
  f(1) & f(2) & \cdots & f(n)
  \end{pmatrix}
  \]

- There are $n!$ permutations.

- Permutation $f$ has a fixed point at $i$ if $f(i) = i$.
  - $i$ is invariant under $f$.

- When $i$ is a fixed point, then $f f \cdots f(i) = i$ for any $m \geq 0$. 
Number of Permutations without Fixed Points

What is the number of permutations without fixed points?

• Let \( S_X \) be the number of permutations that fix all \( i \in X \).

• By the principle of inclusion and exclusion, the desired number is

\[
\sum_{X \subseteq \{1,2,\ldots,n\}} (-1)^{|X|} S_X.
\]

• \( S_X = (n - |X|)! \) as those numbers not in \( X \) form a permutation.

---

\(^a\)Let \( c_i \) denote the condition that \( i \) is a fixed point. Then the desired number is

\[
\sum_{k=0}^{n} (-1)^k \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} N(c_1 c_2 \cdots c_n) =\]

\[
\sum_{k=0}^{n} (-1)^k \sum_{\{i_1, i_2, \ldots, i_k\} \subseteq \{1,2,\ldots,n\}} S\{i_1, i_2, \ldots, i_k\} = \sum_{X \subseteq \{1,2,\ldots,n\}} (-1)^{|X|} S_X.
\]

---

©2017 Prof. Yuh-Dauh Lyuu, National Taiwan University
The Proof (concluded)

• The desired number is

\[ \sum_{X \subseteq \{1,2,\ldots,n\}} (-1)^{|X|}(n - |X|)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n - k)! \]

\[ = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad (49) \]

\[ \approx \frac{n!}{e}, \]

where \( e = 2.71828 \ldots \).

• A constant fraction of permutations have no fixed points!

• Or, if one picks a random permutation, with roughly 40% chance, that permutation will have no fixed points!
Derangements (Also P. 413)

- A **derangement** is a permutation of 1, 2, . . . , \( n \) in which 1 is not in the first place, 2 is not in the second place, etc.\(^a\)

- How many derangements of 1, 2, . . . , \( n \) are there?

- Let \( c_i \) denote the condition that \( i \) is in the \( i \)th place.

- The desired number is \( N(\overline{c_1} \overline{c_2} \cdots \overline{c_n}) \), which equals

\[
d_n \equiv \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)! = n! \sum_{i=0}^{n} (-1)^i \frac{1}{i!} \approx \frac{n!}{e} \quad (50)
\]

by the principle of inclusion and exclusion (46) on p. 395.

\(^{a}\)Just a permutation without fixed points!
A Combinatorial Identity for $d_n$

- Let $d_k$ denote the number of derangements of $1, 2, \ldots, k$.
- By convention, $d_0 = 1$.
- Any permutation of $1, 2, \ldots, n$ can have $n - k$ fixed points for some $k$, with the rest being deranged.
- There are $\binom{n}{n-k} = \binom{n}{k}$ choices for the fixed points.
- Hence
  \[ n! = \sum_{k=0}^{n} \binom{n}{k} d_k. \]  \hfill (51)
- Alternatively,
  \[ 1 = \sum_{k=0}^{n} \frac{d_k}{k! (n-k)!}. \]
The Proof (concluded)

- With the help of Eq. (50) on p. 416, the following complex identity is obtained:

\[
\begin{align*}
\frac{n!}{n!} &= \sum_{k=0}^{n} \binom{n}{k} k! \sum_{i=0}^{k} (-1)^i \frac{1}{i!} \\
&= n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \sum_{i=0}^{k} (-1)^i \frac{1}{i!}.
\end{align*}
\]
An Example

One can numerically verify identity (51) on p. 417 with the following data:

\[ d_0 = 1, d_1 = 0, \]
\[ d_2 = 1, d_3 = 2, \]
\[ d_4 = 9, d_5 = 44, \]
\[ d_6 = 265, \]
\[ d_7 = 1854, \]
\[ d_8 = 14833, \]
\[ d_9 = 133496, \]
\[ d_{10} = 1334961. \]
A Variation on Derangement

• How many permutations of 1, 2, ..., n are there such that \( i \) is not in the \((i - 1)\)st place for \(2 \leq i \leq n\)?
  – For example, 12345 (but not 23451).

• Let \( c_i \) denote the condition that \( i \) is in the \((i - 1)\)st place.

• Now \( N(c_i) = (n-1)! \), \( N(c_ic_j) = (n-2)! \) with \( i \neq j \), etc.

• The desired number \( N(\overline{c_2c_3 \cdots c_n}) \) equals

\[
n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \cdots
\]

by the principle of inclusion and exclusion.
A Variation on Derangement (continued)

\[
\begin{align*}
\sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} (n-i)! &= \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{(n-1)! (n-i)}{i!} \\
&= n! + \sum_{i=1}^{n-1} (-1)^i \frac{n! (n-i)}{i!} \\
&= n! + \sum_{i=1}^{n-1} (-1)^i \frac{n!}{i!} - \sum_{i=1}^{n-1} (-1)^i \frac{(n-1)!}{(i-1)!} \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} - \sum_{i=1}^{n-1} (-1)^i \frac{(n-1)!}{(i-1)!}
\end{align*}
\]
A Variation on Derangement (concluded)

\[
\begin{align*}
A_n &= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-2} (-1)^i \frac{(n-1)!}{i!} \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-2} (-1)^i \frac{(n-1)!}{i!} \\
&\quad + \left[ (-1)^n \frac{n!}{n!} + (-1)^{n-1} \frac{(n-1)!}{(n-1)!} \right] \\
&= \sum_{i=0}^{n} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-1} (-1)^i \frac{(n-1)!}{i!} \\
&= d_n + d_{n-1} \quad (52)
\end{align*}
\]

from Eq. (50) on p. 416.
A Simpler Proof

• Again, how many permutations of 1, 2, \ldots, n are there such that \( i \) is not in the \((i - 1)\)st place for \( 2 \leq i \leq n \)?

• Consider a permutation of 1, 2, \ldots, n, where
  1. \( i \) is not in the \((i - 1)\)st place for \( 2 \leq i \leq n \).
  2. 1 is not in the \( n \)th place.

• There are \( d_n \) of such permutations as they are but derangements with the location restrictions shifted.

• The 2nd condition that 1 is not in the \( n \)th place is extra.

• So we need to add to \( d_n \) the number of permutations that satisfy condition 1 but not condition 2.
A Simpler Proof (concluded)

- So consider permutations of 1, 2, ..., n such that
  1. $i$ is not in the $(i - 1)$st place for $2 \leq i \leq n$.
  2. 1 is in the $n$th place.
- Remove 1 and rename $i$ as $i - 1$ for $2 \leq i \leq n$.
- The results are permutations of 1, 2, ..., $n - 1$ such that
  $i$ is not in the $i$th place for $1 \leq i \leq n - 1$.
- They are simply derangements of 1, 2, ..., $n - 1$.
- Their count is $d_{n-1}$, as desired.