Onto (Surjective) Functions

- A function $f : A \to B$ is **onto** or **surjective** if $f(A) = B$.
  - Necessarily, $|A| \geq |B|$.
  - $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^3$, is onto.

- If $|A| = m$ and $|B| = n$, then there are
  
  $$\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$$

  onto functions from $A$ to $B$.\(^a\)

- Equation (33) equals 0 for $m < n$, as desired.

\(^a\)Proofs appear on p. 294 and p. 421.
Distinct Objects into Distinct Containers with None Empty

- Distribute $m$ distinct objects into $n \leq m$ distinct containers with no containers left empty.

- There are

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

ways.

- Identify a distribution with an onto function.
- Think of the objects $a_1, a_2, \ldots$ in the container labeled $b$ as signifying

$$f(a_1) = f(a_2) = \cdots = b.$$
Application: A Combinatorial Identity

\[
\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^n = n!.
\] (35)

- By Eq. (33) on p. 269, there are

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

onto functions from \(X\) to \(X\), where \(|X| = n\).

- But the number of such onto functions is \(n!\).
An Example

- Suppose there are \( m = 6 \) distinct objects and \( n = 3 \) distinct containers.

- There are 540 ways to distribute these objects into the containers with none empty by Eq. (34) on p. 270.

- Let us verify this number with the alternative method from p. 79 (copied on the next page).
An Example (continued)

\[(x_1 + x_2 + x_3)^6 = (x_1^6 + \cdots + x_3^6) + 6 (x_1^5 x_2 + \cdots + x_2 x_3^5) + 15 (x_1^4 x_2^2 + \cdots + x_2^2 x_3^4) + 20 (x_1^3 x_2^3 + \cdots + x_2^3 x_3^3) + 30 (x_1^4 x_2 x_3 + \cdots + x_1 x_2 x_3^4) + 60 (x_1^3 x_2^2 x_3 + \cdots + x_1 x_2^2 x_3^3) + 90 x_1^2 x_2^2 x_3^2.\]
An Example (concluded)

- Only the last three groups are relevant:

\[
30 \left( x_1^4 x_2 x_3 + \cdots + x_1 x_2 x_3^4 \right) \\
+ 60 \left( x_1^3 x_2^2 x_3 + \cdots + x_1 x_2^2 x_3^3 \right) \\
+ 90 x_1^2 x_2^2 x_3^2.
\]

- The desired count is thus

\[
30 \times 3 + 60 \times 6 + 90 = 540,
\]

a match.
Distinct Objects into Identical Containers with None Empty

- Distribute $m$ distinct objects into $n$ identical containers with no containers left empty with $n \leq m$.
- Alternatively, partition $m$ objects into $n$ sets or groups.
- The number of ways is denoted by $S(m,n)$.
  - It is called the **Stirling number of the second kind**.
A Formula for the Stirling Number

• The formula is

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

(36)

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

(37)

– Copy formula (34) on p. 270.
– Then remove the container labels with division by \( n! \) (why?).
Some Boundary Conditions

• Note that

\[
S(m, 0) = 0, \quad \text{if } m > 0, \\
S(0, 0) = 1, \quad \text{if we assume } 0^0 = 1, \\
S(m, n) = 0, \quad \text{if } m < n,
\]

as they should be.

• As the left-hand side of (35) on p. 272 equals \( n! S(n, n) \),

\[
S(n, n) = 1.
\]
$S(20, n)$

Stirling number of the 2nd kind

It is unimodal in general.
A Special Case: $S(m, 2) = 2^{m-1} - 1$ for $m > 0$

- First proof: From Eq. (36) on p. 277,

$$S(m, 2) = \frac{1}{2} \left[ \binom{2}{2} 2^m - \binom{2}{1} 1^m + \binom{2}{0} 0^m \right] = 2^{m-1} - 1.$$

- Second proof:
  - Divide $m$ objects into 2 nonempty parts.
  - One of the parts contains the last object and some subset of the first $m - 1$ objects.
  - There are $2^{m-1}$ ways to choose the subset.
  - Subtract 1 from $2^{m-1}$ to rule out selecting all the $m - 1$ objects.
An Example

- Suppose there are $m = 6$ distinct objects and $n = 3$ identical containers.

- There are $S(6, 3) = 90$ ways to distribute these objects into the containers with none empty.

- Let us again verify this number with the method on p. 273.
An Example (continued)

• Recall

\[(x_1 + x_2 + x_3)^6 = (x_1^6 + \cdots + x_3^6)\]
\[+ 6 (x_1^5 x_2 + \cdots + x_2 x_3^5)\]
\[+ 15 (x_1^4 x_2^2 + \cdots + x_2^2 x_3^4)\]
\[+ 20 (x_1^3 x_2^3 + \cdots + x_2^3 x_3^3)\]
\[+ 30 (x_1^4 x_2 x_3 + \cdots + x_1 x_2 x_3^4)\]
\[+ 60 (x_1^3 x_2^2 x_3 + \cdots + x_1 x_2^2 x_3^3)\]
\[+ 90 x_1^2 x_2^2 x_3.\]
An Example (continued)

• As before, only the last three groups are relevant:

\[
30 \left( x_1^4 x_2 x_3 + \cdots + x_1 x_2 x_3^4 \right) \\
+60 \left( x_1^3 x_2^2 x_3 + \cdots + x_1 x_2 x_3^3 \right) \\
+90 x_1^2 x_2^2 x_3^2.
\]

• In each group, how many distributions will look the same after labels are removed?
An Example (continued)

- Consider the case where the containers contain 4 objects, 1 object, and 1 object.

- We look at the coefficient of
  \[ x_1^4 x_2 x_3 + \cdots + x_1 x_2 x_3^4. \]

- It is 30.

- So there are 30 distributions if, say, container \( x_1 \) holds 4 objects, container \( x_2 \) 1 object, and container \( x_3 \) 1.

- Concentrate on \( x_1^4 x_2 x_3 \) as the other terms look the same after the labels are removed.
An Example (continued)

- Containers $x_2$ and $x_3$ can have their objects swapped to yield a new distribution.
- But this pair of distributions become identical after the labels are removed.
- So the desired count is $30/2 = 15$. 
An Example (continued)

- Consider the case where the containers contain 3 objects, 2 objects, and 1 object.
- We look at the coefficient of
  \[ x_1^3x_2^2x_3 + \cdots + x_1x_2^2x_3^3. \]
- It is 60.
- So there are 60 distributions if, say, container \( x_1 \) holds 3 objects, container \( x_2 \) 2 objects, and container \( x_3 \) 1.
- Concentrate on \( x_1^3x_2^2x_3 \) as the other terms look the same after the labels are removed.
An Example (continued)

- Because 3, 2, and 1 are distinct, label removal will not change the count.

- So the desired count is 60.
An Example (continued)

• Consider the case where the containers contain 2 objects, 2 objects, and 2 objects.

• We look at the coefficient of

\[
x_1^2x_2^2x_3^2.
\]

• It is 90.

• So there are 90 distributions if, say, container \( x_1 \) holds 2 objects, container \( x_2 \) 2 objects, and container \( x_3 \) 2.
An Example (concluded)

- Because 2, 2, and 2 are identical, label removal will reduce the count by a factor of 3!.
- So the desired count is \( 90/3! = 15 \).
- In conclusion, the total count is

\[
15 + 60 + 15 = 90,
\]

a match with \( S(6, 3) = 90 \).
Functions with a Given Range Size

- There are $n!S(m, n)$ onto functions from a domain of size $m$ to a codomain of size $n$.

- In general, there are $P(n, r) S(m, r)$ functions from a domain of size $m$ to a codomain of size $n$ with a range of size $r$.\(^{a}\)
  - There are $\binom{n}{r}$ to choose the range.
  - Given a range as the codomain, there are $r!S(m, r)$ onto functions.
  - Hence the desired count is
    \[ \binom{n}{r} r!S(m, r) = P(n, r) S(m, r). \] (39)

\(^{a}\)Recall from Eq. (1) on p. 13 that $P(n, r) = n(n - 1) \cdots (n - r + 1)$. 
Functions with a Given Range Size (concluded)

- In the special case of \( r = n \), Eq. (39) reduces to

\[
P(n, n) S(m, n) = n! S(m, n),
\]

as it should be
An Identity for Stirling Numbers

\[ \sum_{k=1}^{m} S(m, k) x(x - 1) \cdots (x - k + 1) = x^m. \quad (40) \]

- The number of functions from \( A \) to \( B \) is \( x^m \), where \( |A| = m \) and \( |B| = x \) (p. 244).
- Equation (39) on p. 290 says

\[ S(m, k) x(x - 1) \cdots (x - k + 1) \]

is the number of functions whose range has size \( k \).
- This proves the identity for \( x \in \mathbb{Z}^+ \).
An Identity for Stirling Numbers (concluded)

- Hence the polynomial

\[ \sum_{k=1}^{m} S(m, k) x(x - 1) \cdots (x - k + 1) - x^m \]

has more than \( m \) roots, its degree.

- Therefore, it must be identically zero.
Finally, Proof of Eq. (33) on P. 269

It suffices to prove Eq. (37) on p. 277:

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

\[
= \sum_{j=0}^{n} \frac{(-1)^{n-j}}{(n-j)!} j! \sum_{r=0}^{j} S(m, r) j(j-1) \cdots (j-r+1) \quad \text{by Eq. (40) on p. 292}
\]

\[
= \sum_{j=0}^{n} \sum_{r=0}^{j} (-1)^{n-j} S(m, r) \frac{1}{(n-j)!(j-r)!}
\]

\[
= \sum_{r=0}^{n} \frac{S(m, r)}{(n-r)!} \sum_{j=r}^{n} (-1)^{n-j} \frac{(n-r)!}{(n-j)!(j-r)!}
\]

\[
= S(m, n) + \sum_{r=0}^{n-1} \frac{S(m, r)}{(n-r)!} (1 - 1)^{n-r} = S(m, n) \quad \text{by Eq. (11) on p. 60}
\]
A Recurrence Relation for Stirling Numbers

\[
S(m + 1, n) = \begin{cases} 
1, & \text{if } m + 1 = n, \\
1, & \text{if } n = 1, \\
S(m, n - 1) + nS(m, n), & \text{if } 2 \leq n \leq m.
\end{cases}
\] (41)

- \(S(m + 1, n)\) counts the number of ways objects
  \(a_1, a_2, \ldots, a_{m+1}\)
  are distributed among \(n\) identical containers, with no containers left empty.\(^a\)

- Object \(a_{m+1}\) can be in a container all by itself or with other objects.

\(^a\)Recall p. 276.
The Proof (concluded)

- Object $a_{m+1}$ is alone.
  - $S(m, n-1)$ is the number of ways $a_1, a_2, \ldots, a_m$ are distributed among $n - 1$ identical containers, with none left empty.

- Object $a_{m+1}$ is not alone.
  - $S(m, n)$ is the number of ways $a_1, a_2, \ldots, a_m$ are distributed among $n$ identical containers, with none left empty.
  - Now object $a_{m+1}$ has $n$ containers to choose from.
Another Recurrence Relation for Stirling Numbers

\[ S(m, n) = \sum_{k=n-1}^{m-1} \binom{m-1}{k} S(k, n-1), \quad n \leq m. \]  

(42)

- The left-hand side denotes the number of distributions of \( m \) distinct objects into \( n \) identical containers with none left empty.
- Fix an object \( O \).
- Call a container that has \( O \) the \( O \)-container.
- The \( O \)-container must contain \( r \) other objects, where \( 0 \leq r \leq m - n \).\(^a\)

\(^a\)The \( O \)-container thus has \( r + 1 \) objects.
The Proof (concluded)

• These \( r \) objects can be chosen in \( \binom{m-1}{r} \) ways.

• With each choice, the other \( n - 1 \) containers may be filled in \( S(m - r - 1, n - 1) \) ways.

• Hence

\[
S(m, n) = \sum_{r=0}^{m-n} \binom{m-1}{r} S(m-1-r, n-1)
\]

\[
= \sum_{r=0}^{m-n} \binom{m-1}{m-1-r} S(m-1-r, n-1)
\]

\[
= \sum_{k=n-1}^{m-1} \binom{m-1}{k} S(k, n-1).
\]
A Special Case: \( S(m, m - 1) = \binom{m}{2} \) for \( m > 0 \)^a

From Eq. (42) on p. 297,

\[
S(m, m - 1) = \sum_{k=m-2}^{m-1} \binom{m-1}{k} S(k, m - 2)
\]

\[
= \binom{m-1}{m-2} S(m - 2, m - 2) + \binom{m-1}{m-1} S(m - 1, m - 2)
\]

\[
= (m - 1) + S(m - 1, m - 2)
\]

\[
= (m - 1) + (m - 2) + S(m - 2, m - 3)
\]

\[
= (m - 1) + (m - 2) + \cdots + 1 = \binom{m}{2}.
\]

^aCheck that the proof works even when \( m = 1 \). Thanks to a lively discussion on March 29, 2018.
$S(m, m - 1) = \binom{m}{2}$ the Easier Way

- Consider any distribution of $m$ distinct objects into $m - 1$ identical containers with no containers left empty.
- There must be one container with 2 objects and $m - 2$ containers with 1 object (why?).
- The 2-object container can be composed in $\binom{m}{2}$ ways.
Bell\textsuperscript{a} Numbers

- The \( m \)th Bell number \( P_m \) is the number of partitions of \( m \) distinct objects.\textsuperscript{b}

- Alternatively, there are \( P_m \) ways for \( m \) distinct objects to form groups.
  
  - There are 5 ways to partition 3 distinct objects:
    
    \[
    \{
      \{1, 2, 3\}, \{1\}, \{2\}, \{3\},
      \{1, 2\}, \{3\}, \{1, 3\}, \{2\}, \{1\}, \{2, 3\}\}
    \]

\textsuperscript{a}Eric Temple Bell (1883–1960).

\textsuperscript{b}It differs from the Stirling number of the second kind in that the number of partitions is \textit{not} fixed.
A Formula for Bell Numbers

• By convention $P_0 = 1$.

• For $m > 0$,

$$P_m = \sum_{k=0}^{m} S(m, k) = \sum_{k=0}^{\infty} S(m, k).$$

– The above formula also works for $P_0$.

• Indeed, $P_3 = 5$.

---

\textsuperscript{a}Recall that $S(m, 0) = 0$ for $m > 0$ by Eq. (38) on p. 278.

\textsuperscript{b}Recall that $S(0, 0) = 1$ on p. 278.
Dobinski’s Equality

• Now,

\[ P_m = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^m \]

\[ = \sum_{j=0}^{\infty} \frac{j^m}{j!} \sum_{k=j}^{\infty} \frac{(-1)^{k-j}}{(k-j)!} \]

\[ = \frac{1}{e} \sum_{j=0}^{\infty} \frac{j^m}{j!} . \]
A Recurrence Relation for Bell Numbers

\[ P_n = \begin{cases} 
1, & \text{if } n = 0, \\
\sum_{k=0}^{n-1} \binom{n-1}{k} P_k, & \text{if } n \geq 1.
\end{cases} \] (43)

- The proof is the same as that for Eq. (42) on p. 297.
- Let \(|S| = n\) and fix an \(x \in S\).
- A group with \(k\) elements that contains \(x\) can be chosen in \(\binom{n-1}{k-1}\) ways.
- The remaining \(n - k\) elements can be partitioned in \(P_{n-k}\) ways.
The Proof (concluded)

- So the number of partitions in which the group containing \( x \) has \( k \) elements is \( \binom{n-1}{k-1} P_{n-k} \).

- Finally,

\[
P_n = \sum_{k=1}^{n} \binom{n-1}{k-1} P_{n-k} \\
= \sum_{k=1}^{n} \binom{n-1}{n-k} P_{n-k} \\
= \sum_{k=0}^{n-1} \binom{n-1}{k} P_{k}.
\]
Where five economists are gathered together there will be six conflicting opinions, and two of them will be held by Keynes.

— Thomas Jones (1954)
The Pigeonhole Principle$^a$

- If $m$ pigeons occupy $n$ pigeonholes and $m > n$, at least one pigeonhole has two or more pigeons roosting in it.

- With $m$ pigeons and $n$ single-occupancy pigeonholes with $m > n$, at least one pigeon is “homeless.”

$^a$Dirichlet (1834).
The Pigeonhole Principle (continued)

• If $m$ pigeons occupy $n$ pigeonholes and $m > n$, at least one pigeonhole has $\geq \left\lfloor (m - 1)/n \right\rfloor + 1$ pigeons.\(^a\)

  – Otherwise, every pigeonhole has $\leq \left\lfloor (m - 1)/n \right\rfloor$ pigeons.

  – So the number of pigeons is at most $n\left\lfloor (m - 1)/n \right\rfloor \leq m - 1 < m$, a contradiction.

• If $nk + 1$ pigeons occupy $n$ pigeonholes and $k \in \mathbb{Z}^+$, at least one pigeonhole has $\geq k + 1$ pigeons.

  – Otherwise, the number of pigeons is at most $nk$.

\(^a\)It may be called the averaging principle, similar to the mean-value theorem in calculus.
The Pigeonhole Principle (concluded)

**Theorem 42** If there are \( \geq p_1 + p_2 + \cdots + p_n - n + 1 \) pigeons occupying pigeonholes 1, 2, \ldots, n, then some pigeonhole \( j \) contains \( \geq p_j \) pigeons.

- Assume otherwise: Every pigeonhole \( j \) has at most \( p_j - 1 \) pigeons.

- The total number of pigeons is at most

\[
(p_1 - 1) + (p_2 - 1) + \cdots + (p_n - 1)
\]

\[
= p_1 + p_2 + \cdots + p_n - n,
\]

a contradiction.
Johann Peter Gustav Lejeune Dirichlet (1805–1859)
Application: Friendship

- Assumption 1: If A is a friend of B’s, then B is also a friend of A’s.

- Assumption 2: One cannot be a friend of oneself.\(^a\)

**Theorem 43** In any group of people, there exist 2 people who have the same number of friends in the group.

- Let \(x_i\) denote the number of friends of person \(i\), where \(0 \leq i \leq n - 1\).

- Note that \(0 \leq x_i \leq n - 1\).

- Suppose \(x_i\) are distinct.

\(^a\)“And so it was you that was your own friend, was it?” — Charles Dickens (1839), *Oliver Twist.*
The Proof (concluded)

- Relabel them so that $x_0 < x_1 < \cdots < x_{n-1}$.
- Then $x_i = i$ for all $i$ by the pigeonhole principle.
- Remove the friendless person 0 from the group.
- The remaining $n - 1$ persons’ friends will be unchanged.
- Hence person $n - 1$ is a friend of $n - 1$ other people.
- This is impossible because there are only $n - 1$ people.
Application: Dividends

Theorem 44 Let $n \in \mathbb{Z}^+$ be odd. Then there exists a positive integer $m \leq n$ such that $n \mid (2^m - 1)$.

- Consider $n+1$ integers: $2^1 - 1, 2^2 - 1, \ldots, 2^{n+1} - 1$.
- There exist $s < t$ such that $2^s - 1 \equiv 2^t - 1 \mod n$ by the pigeonhole principle.
  - Only $n$ remainders are possible.
- So $n \mid (2^t - 2^s)$, or equivalently $n \mid (2^{t-s} - 1) \cdot 2^s$.
- Because $n$ is odd, $n \mid (2^{t-s} - 1)$.
- Pick $m = t - s \leq n$ to finish the proof.
Application: Coding Theory

**Theorem 45** Let \( n \in \mathbb{Z}^+ \) and \( q \in \mathbb{Z}^+ \) such that \( \gcd(n, q) = 1 \). Then \( n \mid (q^m - 1) \) for some \( 1 \leq m \leq n \).

- Use the division algorithm to yield the following set of \( n + 1 \) equations:

\[
\begin{align*}
q &= Q_1n + r_1, \\
q^2 &= Q_2n + r_2, \\
&\vdots \\
q^{n+1} &= Q_{n+1}n + r_{n+1}.
\end{align*}
\]

- Above, \( 0 \leq r_i \leq n - 1 \) for all \( i \).
The Proof (concluded)

• Because there are $n + 1$ equations with $n$ possible remainders, two remainders must be identical, say

$$r_i = r_j, \quad i < j.$$  

• Hence

$$q^j - q^i = Q_j n + r_j - Q_i n - r_i.$$

• This implies that

$$q^i(q^{j-i} - 1) = (Q_j - Q_i)n.$$

• Because $\gcd(n, q) = 1$, $n$ divides $q^{j-i} - 1$.

• Finally, set $m = j - i \leq n$ to finish the proof.
Application: Mutual Divisibility

Theorem 46 (Putnam, 1958) Any subset of \( n + 1 \) numbers from \( \{1, 2, \ldots, 2n\} \) must contain \( x, y \) such that \( x \) divides \( y \) or \( y \) divides \( x \).

- Express every positive integer as \( 2^k m \), where \( m \) is odd.

- There are at most \( n \) possibilities for \( m \): 
  \[ 1, 3, 5, \ldots, 2n - 1. \]

- Hence any set of \( n + 1 \) integers must contain two \( x, y \) with the same \( m \): \( x = 2^{k_1} m \) and \( y = 2^{k_2} m \).

- Now, \( x \mid y \) if \( k_1 < k_2 \) and \( y \mid x \) otherwise.
Bijective Functions

- A function \( f : A \rightarrow B \) is **bijective** or a **one-to-one correspondence**\(^a\) if it is one-to-one and onto.
  - Necessarily, \( |A| = |B| \).

- For example, \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) is bijective for \( f(x) = x \).

- But \( f(x) = x \) is not bijective if \( f : \mathbb{Z} \rightarrow \mathbb{Q} \) (it is not onto).

- If \( |A| = |B| = m \), then there are \( m! \) bijective functions from \( A \) to \( B \).

---

\(^a\)Note the definitional difference between a one-to-one (injective) function (p. 260) and a one-to-one correspondence.
Function Composition

• Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$.

• The composite function $g \circ f : A \rightarrow C$ is defined as

\[(g \circ f)(a) = g(f(a))\]

for each $a \in A$.

• Note that $f$ is applied first.

• Also, $f$’s range must be a subset of $g$’s domain for $g \circ f$ to work.

---

Read as “$g$ circle $f$,” “$g$ composed with $f$,” “$g$ after $f$,” “$g$ following $f$,” or “$g$ of $f$.”

\[\text{a}\]
Properties of Composite Functions

**Theorem 47** Let \( f : A \rightarrow B \) and \( g : B \rightarrow C \). If \( f \) and \( g \) are one-to-one, then \( g \circ f \) is also one-to-one.

- Let \( a_1, a_2 \in A \) with
  \[
  (g \circ f)(a_1) = (g \circ f)(a_2).
  \]
- Then
  \[
  g(f(a_1)) = g(f(a_2)).
  \]
- As \( g \) is one-to-one, this implies
  \[
  f(a_1) = f(a_2).
  \]
- As \( f \) is one-to-one, this implies \( a_1 = a_2 \), as desired.
Function Composition Is Associative

**Theorem 48** Let $f : A \rightarrow B$, $g : B \rightarrow C$, and $h : C \rightarrow D$

Then $(h \circ g) \circ f = h \circ (g \circ f)$.

For every $a \in A$,

\[
((h \circ g) \circ f)(a) \\
= (h \circ g)(f(a)) \\
= h(g(f(a))) \\
= h((g \circ f)(a)) \\
= (h \circ (g \circ f))(a).
\]
Powers of Functions

- As function composition is associative (p. 321), we write
  \[ h \circ g \circ f \]
  in place of \((h \circ g) \circ f\) or \(h \circ (g \circ f)\).
- Let \(f : A \to A\).
- Define \(f^1 = f\).
- In general,
  \[ f^{n+1} = f \circ (f^n) = \cdots = f\left(\underbrace{f(f(\cdots f)}_{n}\right) \]
  for \(n \in \mathbb{Z}^+\).
The Identity Function

• Function $1_A : A \rightarrow A$ is defined by

$$1_A(a) = a$$

for all $a \in A$.

• This function is called the **identity function** for $A$. 
Invertibility of Functions

• Suppose \( f : A \to B \).

• \( f \) is said to be invertible if there is a function \( g : B \to A \) such that
  \[
  g \circ f = 1_A \quad \text{and} \quad f \circ g = 1_B.
  \]

• So
  - \( g(f(a)) = a \) for all \( a \in A \).
  - \( f(g(b)) = b \) for all \( b \in B \).

• Is \( g \) unique?
Uniqueness of the Inverse Function

**Theorem 49** Suppose $f : A \to B$ is invertible. Then a function $g : B \to A$ such that

\[
g \circ f = 1_A, \\
f \circ g = 1_B,
\]

must be unique.

- Suppose there is another function $h : B \to A$ with

\[
h \circ f = 1_A, \\
f \circ h = 1_B.
\]
The Proof (concluded)

• Now,

\[
\begin{align*}
    h &= h \circ 1_B \\
    &= h \circ (f \circ g) \\
    &= (h \circ f) \circ g \\
    &= 1_A \circ g \\
    &= g.
\end{align*}
\]
The Inverse Function

• We call the function $g$ in Theorem 49 (p. 325), the **inverse** of $f$, written as
  $$f^{-1}.$$  

• Again by Theorem 49 (p. 325), if $f$ is invertible, so is $f^{-1}$, whose inverse is $(f^{-1})^{-1}$ by definition.

• In fact, if $f$ is invertible, then
  $$ (f^{-1})^{-1} = f. $$

  – Note that
  $$ (f^{-1})^{-1} \neq f^{-2}. $$
Conditions for Invertibility

**Theorem 50** \( f \) is invertible if and only if it is bijective.

- Assume that \( f : A \to B \) is invertible first.
- Then by Theorem 49 (p. 325) there is a unique function \( g : B \to A \) such that \( g \circ f = 1_A \) and \( f \circ g = 1_B \).
- Suppose \( a_1, a_2 \in A \) such that \( f(a_1) = f(a_2) \).
- Then \( g(f(a_1)) = g(f(a_2)) \); i.e.,
  \[
  (g \circ f)(a_1) = (g \circ f)(a_2).
  \]
- This implies \( (1_A)(a_1) = (1_A)(a_2) \); i.e., \( a_1 = a_2 \).
- Hence \( f \) is one-to-one.
The Proof (continued)

- Let $b \in B$.
- Then
  \[ b = (1_B)(b) = (f \circ g)(b) = f(g(b)). \]
- So $f$ is onto.
- Conversely, suppose $f$ is bijective.
- Define $g : B \to A$ by
  \[ g(b) = a \]
  whenever $f(a) = b$. 

©2024 Prof. Yuh-Dauh Lyuu, National Taiwan University
The Proof (concluded)

• As $f$ is onto, for each $b \in B$ there is an $a \in A$ such that $f(a) = b$.

• This $a$ is also unique.
  - If $f(a_1) = f(a_2) = b$, then $a_1 = a_2$ because $f$ is one-to-one.

• Hence $g$ is a function.

• By $g$’s definition, $g \circ f = 1_A$ and $f \circ g = 1_B$.

• Hence $g = f^{-1}$ by Theorem 49 (p. 325).
Inverse of the Composite Function

Theorem 51  If $f : A \to B$ and $g : B \to C$ are invertible, then $g \circ f$ is also invertible and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$
Preimage of a Function

- Consider $f : A \to B$, an arbitrary function.
- Let $B' \subseteq B$.
- Define
  $$f^{-1}(B') = \{ a \in A : f(a) \in B' \}.$$
- The set $f^{-1}(B')$ is called the **preimage** or **inverse image** of $B'$ under $f$.
  - Above, $f^{-1}$ is **not** meant to denote the inverse function of $f$.
  - In fact, $f$ is not required to be invertible.
Relations: The Second Time Around
Whatsoever we imagine is \textit{finite}. Therefore there is no idea, or conception of any thing we call \textit{infinite}.

— Thomas Hobbes (1588–1679), \textit{Leviathan} (1651)
Reflexive Relations

- $R \subseteq A \times A$ is a relation on $A$.
- $R$ is \textbf{reflexive} if $(x, x) \in R$ (or $xRx$) for all $x \in A$.
  - “$\leq$” is reflexive because $x \leq x$.
  - “$=$” is reflexive because $x = x$.
- If $|A| = m$, then there are $2^{m^2} - m$ reflexive relations on $A$.
  - Except the $m$ required $(x, x) \in R$, membership in $R$ for the other $m^2 - m$ pairs of $A \times A$ is arbitrary.
Irreflexive Relations

- Relation \( R \) on \( A \) is **irreflexive** if \((x, x) \notin R\) for all \( x \in A \).
  - “\(<\)” is irreflexive because \( x \not< x \).

- For \(|A| = m\), there are again
  \[ 2^{m^2 - m} \]

irreflexive relations on \( A \) (see next page).

- “Being irreflexive” (exact opposite) is not the same thing as “not being reflexive” \(^a\) (complement).

\(^a\)Which means there is an \( x \) such that \((x, x) \notin R\). By Eq. (27) on p. 240, there are \( 2^{m^2} - 2^{m^2 - m} \) relations that are *not* reflexive.
Symmetric Relations

- \( R \) is **symmetric** if \((x, y) \in R \Rightarrow (y, x) \in R\) for all \( x, y \in A \).

- For example, “=” and “\( \neq \)” are symmetric.
  - If \( x = y \), then \( y = x \).
  - If \( x \neq y \), then \( y \neq x \).
Number of Symmetric Relations

**Lemma 52** If $|A| = m$, then there are

$$2^{(m^2+m)/2}$$

symmetric relations on $A$.

- There are $m \ (x, x)$s and $\binom{m}{2} = (m^2 - m)/2 \ \{x, y\}$s with $x \neq y$.

- Number of decisions to make for membership in $\mathcal{R}$:

$$m + (m^2 - m)/2 = (m^2 + m)/2.$$  

\[^{a}\text{Or the upper triangular elements on the next page.}\]
Transitive Relations

- \( R \) is \textbf{transitive} if \( (x, y) \in R \land (y, z) \in R \Rightarrow (x, z) \in R \)
  for all \( x, y, z \in A \).
  
  - “\( \leq \)” is transitive.
  
  - “\( < \)” is transitive.
  
  - “\( \subseteq \)” is transitive.

- The number of transitive relations on a finite set seems hard to derive.\(^a\)

\(^a\)It will make a nice research project.
Tournaments

• \( \mathcal{R} \) is a tournament if
  
  - \( \mathcal{R} \) is irreflexive: \((x, x) \notin \mathcal{R}\).
  
  - For all \( x \neq y \), either \((x, y) \in \mathcal{R}\) (\(x\) beats \(y\)) or \((y, x) \in \mathcal{R}\) (\(y\) beats \(x\)), but not both.
Number of Tournaments

Lemma 53  There are $2^\binom{m}{2}$ possible tournaments on $m$ players.

• There are $\binom{m}{2}$ games for a tournament on $m$ players.

• Each tournament has 2 outcomes.
Transitive Tournaments Can Be Ranked

- Suppose every player is beaten at least once.
- Start with any node $a$ and follow the “is beaten by” edges, we will eventually obtain a cycle.
- Suppose node $a'$ is on the cycle.
- This implies $(a', a') \in \mathcal{R}$ by transitivity, a contradiction because $\mathcal{R}$ is irreflexive.
- Hence some player $x$ is unbeaten and $x$ is a “champion.”

\[ \text{a} \]

\[ \text{a} \text{Could there be multiple such } x \text{’s?} \]
Transitive Tournaments Can Be Ranked (concluded)

- Remove $x$ and repeat the above argument.
- Player $x$ must beat the next “champion” because $x$ was unbeaten.
- Continue this process until there are no players left.
- The result is a sequence of players where earlier ones beat the later ones by transitivity.
Antisymmetric Relations

- \( \mathcal{R} \) is antisymmetric if
  \[
  (x, y) \in \mathcal{R} \land (y, x) \in \mathcal{R} \Rightarrow x = y
  \]
  for all \( x, y \in A \).
  
  - “\( \subseteq \)” is antisymmetric.
  
  - “\( \leq \)” is antisymmetric.

- Alternatively, \( \mathcal{R} \) is antisymmetric if
  \[
  x \neq y \Rightarrow (x, y) \notin \mathcal{R} \lor (y, x) \notin \mathcal{R} \quad (44)
  \]
  for all \( x, y \in A \).
Antisymmetric Relations (continued)

- With DeMorgan’s law, Eq. (44) can be rewritten as
  \[ x \neq y \Rightarrow \neg[(x, y) \in \mathcal{R} \land (y, x) \in \mathcal{R}]. \]

- “<” is antisymmetric because
  \[ x \neq y \Rightarrow \neg[(x < y) \land (y < x)]. \]
  - The original version would have asked us to prove
    \[ (x < y) \land (x > y) \Rightarrow x = y, \]
    which is perhaps less intuitive.
Antisymmetric Relations (concluded)

- Antisymmetry is clearly different from symmetry.
  - “⊆” is antisymmetric (p. 347) but not symmetric.

- Antisymmetry is not the same as “not being symmetric” either.
  - Take $\mathcal{R}$ as the relation that is the empty set.
  - So $(x, y) \not\in \mathcal{R}$ for any $x, y$.
  - Then $\mathcal{R}$ is antisymmetric.
  - $\mathcal{R}$ is also symmetric.
Number of Antisymmetric Relations

Lemma 54  If $|A| = m$, then there are

$$2m \cdot 3(m^2 - m)/2$$

antisymmetric relations on $A$.

• The $m$ decisions on $(x, x) \in \mathcal{R}$ are arbitrary.

• For each of the other $\binom{m}{2} = (m^2 - m)/2$ unordered pairs

{ $x, y$ } ($x \neq y$), there are 3 choices by Eq. (44) on p. 347:

1. $(x, y) \in \mathcal{R}$ but $(y, x) \notin \mathcal{R}$.

2. $(x, y) \notin \mathcal{R}$ but $(y, x) \in \mathcal{R}$.

3. $(x, y) \notin \mathcal{R}$ and $(y, x) \notin \mathcal{R}$. 