Functions

CSE 215, Foundations of Computer Science
Stony Brook University
http://www.cs.stonybrook.edu/liu/~cse215
Functions defined on general sets

- A function \( f \) from a set \( X \) to a set \( Y \)
  \[
  f : X \rightarrow Y
  \]
  \( X \) is the domain, \( Y \) is the co-domain

  1. every element in \( X \) is related to some element in \( Y \)
  2. no element in \( X \) is related to more than one element in \( Y \)

- Thus, **for any** element \( x \in X \), there is a **unique** element \( y \in Y \) such that \( f(x) = y \)

- **range of** \( f = \text{image of } X \text{ under } f = \{y \in Y \mid y = f(x), x \in X\} \)
- **inverse image of** \( y = \{x \in X \mid f(x) = y\} \)
Arrow diagrams

- An arrow diagram, with elements in X and Y, and an arrow from each x in X to corresponding y in Y.

- It defines a function because:
  1. Every element of X has an arrow coming out of it
  2. No element of X has two arrows coming out of it that point to two different elements of Y
Arrow diagrams: example 1

- \( X = \{a, b, c\} \), \( Y = \{1, 2, 3, 4\} \)

Which one defines a function?

This one!
Arrow diagrams: example 2

- $X = \{a, b, c\}$, \hspace{1cm} $Y = \{1, 2, 3, 4\}$

- Domain of $f = \{a, b, c\}$, \hspace{1cm} Co-domain of $f = \{1, 2, 3, 4\}$

- Range of $f = \{2, 4\}$

- Inverse image of 2 = \{a, c\}

- Inverse image of 4 = \{b\}

- Inverse image of 1 = $\emptyset$

- Function representation as a set of pairs: $\{(a,2), (b,4), (c,2)\}$
Function equality

Note the set notation for a function: \( F(x) = y \iff (x, y) \in F \)

- If \( F: X \rightarrow Y \) and \( G: X \rightarrow Y \) are functions, then \( F = G \) if, and only if, \( F(x) = G(x) \) for all \( x \in X \).

**Proof:**

\[
F \subseteq X \times Y \quad \quad \quad \quad \quad \quad G \subseteq X \times Y
\]

\[
F(x) = y \iff (x, y) \in F \quad \quad \quad \quad \quad \quad G(x) = y \iff (x, y) \in G
\]

(\( \Rightarrow \)) Suppose \( F = G \). Then for all \( x \in X \),

\[
y = F(x) \iff (x, y) \in F \iff (x, y) \in G \iff y = G(x)
\]

\[
F(x) = y = G(x)
\]

(\( \Leftarrow \)) Suppose \( F(x) = G(x) \) for all \( x \in X \). Then for any \( x \in X \):

\[
(x, y) \in F \iff y = F(x) \iff y = G(x) \iff (x, y) \in G
\]

F and G consist of exactly the same elements, hence \( F = G \).
Function equality: example 1

- \( J_3 = \{0, 1, 2\} \)

\[
\begin{align*}
  f &: J_3 \to J_3 \\
  f(x) &= (x^2 + x + 1) \mod 3 \\
  g &: J_3 \to J_3 \\
  g(x) &= (x + 2)^2 \mod 3 \\
\end{align*}
\]

<table>
<thead>
<tr>
<th>( x )</th>
<th>( x^2 + x + 1 )</th>
<th>( f(x) = (x^2 + x + 1) \mod 3 )</th>
<th>( (x + 2)^2 )</th>
<th>( g(x) = (x + 2)^2 \mod 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>( 1 \mod 3 = 1 )</td>
<td>4</td>
<td>( 4 \mod 3 = 1 )</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>( 3 \mod 3 = 0 )</td>
<td>9</td>
<td>( 9 \mod 3 = 0 )</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>( 7 \mod 3 = 1 )</td>
<td>16</td>
<td>( 16 \mod 3 = 1 )</td>
</tr>
</tbody>
</table>

- \( f(0) = g(0) = 1 \)
- \( f(1) = g(1) = 0 \)
- \( f(2) = g(2) = 1 \)

Hence, \( f = g \)
Function equality: example 2

- \( F: \mathbb{R} \rightarrow \mathbb{R} \) and \( G: \mathbb{R} \rightarrow \mathbb{R} \)

  \( F + G: \mathbb{R} \rightarrow \mathbb{R} \) and \( G + F: \mathbb{R} \rightarrow \mathbb{R} \)

  \( (F + G)(x) = F(x) + G(x) \)

  \( (G + F)(x) = G(x) + F(x) \), for all \( x \in \mathbb{R} \)

For all real numbers \( x \):

\[
(F + G)(x) = F(x) + G(x) \\
= G(x) + F(x) \\
= (G + F)(x)
\]

by definition of \( F + G \)

by commutative law for addition of real numbers

by definition of \( G + F \)

Hence, \( F + G = G + F \)
Example functions (I)

• **Identity function on a set:**
  Given a set $X$, define identity function $I_X : X \to X$ by
  $$I_X(x) = x, \text{ for all } x \in X$$

• **Function for a sequence:**
  $1, -1/2, 1/3, -1/4, 1/5, \ldots, (-1)^n/(n + 1), \ldots$
  $0 \to 1, \ 1 \to -1/2, \ 2 \to 1/3, \ 3 \to -1/4, \ 4 \to 1/5$
  $$n \to (-1)^n/(n + 1)$$
  $f : \mathbb{N} \to \mathbb{R}, \text{ for each integer } n \geq 0, \ f(n) = (-1)^n/(n + 1)$
  where $(\mathbb{N} = \mathbb{Z}_{\text{nonneg}})$ OR
  $g : \mathbb{Z}^+ \to \mathbb{R}, \text{ for each integer } n \geq 1, \ g(n) = (-1)^{n+1}/n$
  where $(\mathbb{Z}^+ = \mathbb{Z}_{\text{nonneg}} - \{0\})$
Example functions (II)

- Function defined on a power set:
  \[ F : P(\{a, b, c\}) \rightarrow \mathbb{Z}^{\text{nonneg}} \]

  For each \( X \in P(\{a, b, c\}) \),

  \[ F(X) = \text{the number of elements in } X \text{ (i.e., the cardinality of } X) \]
Example functions (III)

- Functions defined on a Cartesian product:
  \[ M : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \quad \text{and} \quad R : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R} \]

  **The multiplication function:** \( M(a, b) = a \times b \)
  We omit parenthesis for tuples: \( M((a, b)) = M(a, b) \)
  \[ M(1, 1) = 1, \quad M(2, 2) = 4 \]

  **The reflection function:** \( R(a, b) = (-a, b) \)
  \( R \) sends each point in the plane that corresponds to a pair of real numbers to the mirror image of the point across the vertical axis
  \[ R(1, 1) = (-1, 1), \quad R(2, 5) = (-2, 5), \quad R(-2, 5) = (2, 5) \]
Example functions (IV)

- **Logarithms and logarithmic functions:**
  - The base of a logarithm, $b$, is a positive real number with $b \neq 1$
  - The logarithm with base $b$ of $x$: $\log_b x = y \iff b^y = x$
  - The **logarithmic function with base $b$**:
    \[
    \log_b x : \mathbb{R}^+ \rightarrow \mathbb{R}
    \]

Examples:

- $\log_3 9 = 2$  
  because $3^2 = 9$
- $\log_{10}(1) = 0$  
  because $10^0 = 1$
- $\log_2 \frac{1}{2} = -1$  
  because $2^{-1} = \frac{1}{2}$
- $\log_2 (2^m) = m$
More example functions (I)

- **Encoding and decoding functions** on sequences of 0’s and 1’s also called bit strings

  Encoding function $E$: For each string $s$,
  \[
  E(s) = \text{the string obtained from } s \text{ by replacing each bit of } s \text{ by the same bit written 3 times}
  \]

  Decoding function $D$: For each string $t$ in the range of $E$,
  \[
  D(t) = \text{the string obtained from } t \text{ by replacing each consecutive 3 identical bits of } t \text{ by a single copy of that bit}
  \]

Redundancy helps with error detection and fix.
More example functions (II)

- **The Hamming distance function**

Let $S_n$ be the set of all strings of 0’s and 1’s of length $n$.

$H: S_n \times S_n \rightarrow \mathbb{Z}^{\text{nonneg}}$

For each pair of strings $(s, t) \in S_n \times S_n$

$H(s, t) =$ number of positions in which $s$ and $t$ differ

**Examples:** For $n = 5$, $H(11111, 00000) = 5$

$H(10101, 00000) = 3$

$H(01010, 00000) = 2$

It is important in coding theory: gives a measure of “difference”.
More example functions (III)

- **Boolean functions: (n-place) Boolean function**
  
  \[ f : \{0, 1\}^n \rightarrow \{0, 1\} \]

  
  Cartesian product

  domain = set of all ordered n-tuples of 0’s and 1’s

  co-domain = \{0, 1\}

  
  The input/output tables correspond to some circuits.
More example functions (IV)

- **Boolean functions example:**

  \[
  f : \{0, 1\}^3 \rightarrow \{0, 1\}
  \]

  \[
  f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \mod 2
  \]

  - \(f(0, 0, 0) = (0 + 0 + 0) \mod 2 = 0 \mod 2 = 0\)
  - \(f(0, 0, 1) = (0 + 0 + 1) \mod 2 = 1 \mod 2 = 1\)
  - \(f(0, 1, 0) = (0 + 1 + 0) \mod 2 = 1 \mod 2 = 1\)
  - \(f(0, 1, 1) = (0 + 1 + 1) \mod 2 = 2 \mod 2 = 0\)
  - \(f(1, 0, 0) = (1 + 0 + 0) \mod 2 = 1 \mod 2 = 1\)
  - \(f(1, 0, 1) = (1 + 0 + 1) \mod 2 = 2 \mod 2 = 0\)
  - \(f(1, 1, 0) = (1 + 1 + 0) \mod 2 = 2 \mod 2 = 0\)
  - \(f(1, 1, 1) = (1 + 1 + 1) \mod 2 = 3 \mod 2 = 1\)
Checking well-definedness

• A “function” \( f \) is not well defined if:

  (1) there is no element \( y \) in the co-domain that satisfies \( f(x) = y \) for some element \( x \) in the domain, or

  (2) there are two different values of \( y \) that satisfy \( f(x) = y \)

• Example:

  \( f : \mathbb{R} \rightarrow \mathbb{R} \), \( f(x) \) is the real number \( y \) such that \( x^2 + y^2 = 1 \)

  \( f \) is not well defined:

  (1) \( x = 2 \), there is no real number \( y \) such that \( 2^2 + y^2 = 1 \)

  (2) \( x = 0 \), there are 2 real numbers \( y=1 \) and \( y=-1 \) such that \( 0^2 + y^2 = 1 \)
Checking well-definedness: example 2

- \( f : \mathbb{Q} \to \mathbb{Z} \),

  \( f(m/n) = m \), for all integers \( m \) and \( n \) with \( n \neq 0 \)

\( f \) is not well defined:

\( 1/2 = 2/4 \ \Rightarrow \ f(1/2) = f(2/4) \)

but

\( f(1/2) = 1 \neq 2 = f(2/4) \)

That is, there are two different values of \( y \) that satisfy \( f(x) = y \)
Functions acting on sets

- If \( f : X \rightarrow Y \) is a function and \( A \subseteq X \) and \( C \subseteq Y \), then
  \[
  f(A) = \{ y \in Y \mid y = f(x) \text{ for some } x \in A \}
  \]
  is the **image** of \( A \)
  \[
  f^{-1}(C) = \{ x \in X \mid f(x) \in C \}
  \]
  is the **inverse image** of \( C \)

**Example:** \( X = \{1, 2, 3, 4\} \), \( Y = \{a, b, c, d, e\} \), \( f : X \rightarrow Y \)

\[
\begin{align*}
  f(\{1,4\}) &= \{b\} & f^{-1}(\{a,b\}) &= \{1, 2, 4\} \\
  f(X) &= \{a, b, d\} & f^{-1}(\{c,e\}) &= \emptyset
\end{align*}
\]
Functions acting on sets: an example proof

- Let $X$ and $Y$ be sets, let $F : X \rightarrow Y$ be a function, $A \subseteq X$, and $B \subseteq X$, then $F(A \cup B) \subseteq F(A) \cup F(B)$

**Proof:**

Suppose $y \in F(A \cup B)$.

By definition of function, $y = F(x)$ for some $x \in A \cup B$.

By definition of union, $x \in A$ or $x \in B$.

**Case 1, $x \in A$:** $F(x) = y$, so $y \in F(A)$.

By definition of union: $y \in F(A) \cup F(B)$

**Case 2, $x \in B$:** $F(x) = y$, so $y \in F(B)$.

By definition of union: $y \in F(A) \cup F(B)$
**One-to-one, onto, inverse functions**

- $F : X \rightarrow Y$ is **one-to-one** (or **injective**) (often written 1-1) $\iff$
  
  For all $x_1 \in X$ and $x_2 \in X$, $F(x_1) = F(x_2) \implies x_1 = x_2$
  
  Or, equivalently (by contraposition), $x_1 \neq x_2 \implies F(x_1) \neq F(x_2)$

- $F : X \rightarrow Y$ is **not one-to-one** $\iff$
  
  $\exists x_1 \in X$ and $x_2 \in X$, such that $x_1 \neq x_2$ and $F(x_1) = F(x_2)$. 

---

**Notes on one-to-one functions:**

- **One-to-one** functions map each element of the domain to a unique element of the codomain.
- **Injective** functions are a specific type of one-to-one function.

---

**Notes on not one-to-one functions:**

- **Not one-to-one** functions map at least one pair of domain elements to the same codomain element. This violates the uniqueness property of one-to-one functions.
- Examples of not one-to-one functions can be visualized where two or more elements in the domain map to the same element in the codomain.
One-to-one functions on finite sets

- **Example 1:**

  $F: \{a, b, c, d\} \rightarrow \{u, v, w, x, y\}$ defined by the following arrow diagram is one-to-one:

\[
\forall x_1 \in X \text{ and } x_2 \in X, \quad x_1 \neq x_2 \implies F(x_1) \neq F(x_2)
\]
One-to-one functions on finite sets

- **Example 2:**
  
  \( G: \{a, b, c, d\} \rightarrow \{u, v, w, x, y\} \) defined by the following arrow diagram is not one-to-one:

  \[ G(a) = G(c) = w \]

  \( \exists \) elements \( x_1 \in X \) and \( x_2 \in X \), such that \( x_1 \neq x_2 \) and \( G(x_1) = G(x_2) \)

  that is, \( a \in X \) and \( c \in X \), such that \( a \neq c \) and \( G(a) = G(c) \)
One-to-one functions on finite sets

• **Example 3:**
  
  \[ H: \{1, 2, 3\} \to \{a, b, c, d\}, \ H(1) = c, \ H(2) = a, \ H(3) = d \]

  \[ H \text{ is one-to-one:} \]

  \[ \forall x_1 \in X \text{ and } x_2 \in X, \ x_1 \neq x_2 \implies H(x_1) \neq H(x_2) \]

• **Example 4:**

  \[ K: \{1, 2, 3\} \to \{a, b, c, d\}, \ K(1) = d, \ K(2) = b, \ K(3) = d \]

  \[ K \text{ is not one-to-one:} \]

  \[ K(1) = K(3) = d \]

  That is, \( \exists \ x_1 \in X \text{ and } x_2 \in X, \text{ such that } x_1 \neq x_2 \text{ and } K(x_1) = K(x_2) \)
One-to-one functions on infinite sets

- Copied definition:
  \[ f \text{ is one-to-one} \iff \forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2 \]

- To show f is one-to-one, generally use direct proof:
  - suppose \( x_1 \) and \( x_2 \) are elements of \( X \) such that \( f(x_1) = f(x_2) \)
  - show that \( x_1 = x_2 \).

- To show f is not one-to-one, generally use counterexample:
  - find elements \( x_1 \) and \( x_2 \) in \( X \) so that \( f(x_1) = f(x_2) \) but \( x_1 \neq x_2 \).
One-to-one functions on infinite sets

copied: \( f \text{ is one-to-one } \iff \forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2 \)

- **Example 1:** \( f : \mathbb{R} \rightarrow \mathbb{R} \), \[ f(x) = 4x - 1 \text{ for all } x \in \mathbb{R} \]
  is \( f \) one-to-one?
  Suppose \( x_1 \) and \( x_2 \) are any real numbers such that \( 4x_1 - 1 = 4x_2 - 1 \).
  Adding 1 to both sides and dividing by 4 both sides gives \( x_1 = x_2 \).
  Yes, \( f \) is one-to-one

- **Example 2:** \( g : \mathbb{Z} \rightarrow \mathbb{Z} \), \[ g(n) = n^2 \text{ for all } n \in \mathbb{Z} \]
  is \( g \) one-to-one?
  Start by trying to show that \( g \) is one-to-one
  Suppose \( n_1 \) and \( n_2 \) are integers such that \( n_1^2 = n_2^2 \) and try to show \( n_1 = n_2 \).
  But \( 1^2 = (-1)^2 = 1 \).
  No, \( g \) is not one-to-one
Application: hash functions

- **Hash functions** are functions defined from larger to smaller sets of integers used in identifying documents.

- **Example**: Hash: \( \text{SSN} \rightarrow \{0, 1, 2, 3, 4, 5, 6\} \)
  
  \[ \text{SSN} = \text{set of all social security numbers (ignoring hyphens)} \]
  
  \[ \text{Hash}(n) = n \mod 7 \quad \text{for all social security numbers } n \]
  
  e.g., \( \text{Hash}(328343419) = 328343419 - (7 \cdot 46906202) = 5 \)

- Hash is not one-to one: called a **collision** for hash functions.
  
  e.g., \( \text{Hash}(328343412) = 328343412 - (7 \cdot 46906201) = 5 \)

  Collision resolution:

  if position \( \text{Hash}(n) \) is already occupied, then start from that position and search downward to place the record in the first empty position.
Onto functions

- **F: X → Y is onto (surjective) ⇔**
  \[ \forall y \in Y, \; \exists x \in X \text{ such that } F(x) = y. \]
  For arrow diagrams, a function is onto if each element in the co-domain has an arrow to it from some element in the domain.

- **F: X → Y is not onto (surjective) ⇔**
  \[ \exists y \in Y \text{ such that } \forall x \in X, \; F(x) \neq y. \]
  There is some element in Y that is not the image of any element in X.
  For arrow diagrams, a function is not onto if at least one element in its co-domain does not have an arrow pointing to it.
Onto functions with arrow diagrams

- $F$ is onto:

Given the diagram:

- $X =$ domain of $F$
- $Y =$ co-domain of $F$

Each element $y$ in $Y$ equals $F(x)$ for at least one $x$ in $X$. 
Onto functions: example 1

- $G: \{1,2,3,4,5\} \rightarrow \{a,b,c,d\}$

$G$ is onto because $\forall y \in Y, \exists x \in X$, such that $G(x) = y$
Not onto functions

- \( F \) is not onto

At least one element in \( Y \) does not equal \( F(x) \) for any \( x \) in \( X \).
Onto functions: example 2

- $F: \{1,2,3,4,5\} \rightarrow \{a,b,c,d\}$

$F$ is not onto

because $b \neq F(x)$ for any $x$ in $X$

that is, $\exists y \in Y$ such that $\forall x \in X$, $F(x) \neq y$
Onto functions: more examples

- **H**: \(\{1,2,3,4\} \rightarrow \{a,b,c\}\)
  
  \[
  H(1) = c, \quad H(2) = a, \quad H(3) = c, \quad \text{and} \quad H(4) = b
  \]

  *H is onto* because \(\forall y \in Y, \exists x \in X\) such that \(H(x) = y:\)
  
  \[
  a = H(2) \\
  b = H(4) \\
  c = H(1) = H(3)
  \]

- **K**: \(\{1,2,3,4\} \rightarrow \{a,b,c\}\)
  
  \[
  K(1) = c, \quad K(2) = b, \quad K(3) = b, \quad \text{and} \quad K(4) = c
  \]

  *H is not onto* because \(a \neq K(x)\) for any \(x \in \{1, 2, 3, 4\}\).
Onto functions on infinite sets

-Copied definition:
  \( F \text{ is onto } \iff \forall y \in Y, \exists x \in X \text{ such that } F(x) = y \).

- To prove \( F \) is onto, generally use direct proof:
  - suppose \( y \) is any element of \( Y \),
  - show there is an element \( x \) of \( X \) with \( F(x) = y \).

- To prove \( F \) is \textbf{not} onto, use counterexample:
  - find an element \( y \) of \( Y \) such that \( y \neq F(x) \) for any \( x \) in \( X \).
Onto functions on infinite sets: examples

• Prove that a function is onto or give counterexample

• \( f : \mathbb{R} \to \mathbb{R} \)

\[
f(x) = 4x - 1 \text{ for all } x \in \mathbb{R}
\]

Suppose \( y \in \mathbb{R} \). Show there is a real number \( x \) such that \( y = 4x - 1 \).

\[
4x - 1 = y \iff x = (y + 1)/4 \in \mathbb{R}
\]

So, \( f \) is onto \( \blacksquare \)

• \( h : \mathbb{Z} \to \mathbb{Z} \)

\[
h(n) = 4n - 1 \text{ for all } n \in \mathbb{Z}
\]

\( 0 \in \mathbb{Z} \), \( h(n) = 0 \iff 4n - 1 = 0 \iff n = 1/4 \notin \mathbb{Z} \)

\( h(n) \neq 0 \) for any integer \( n \). So \( h \) is not onto \( \blacksquare \)
Exponential functions

- The exponential function with base $b$: $\exp_b : \mathbb{R} \rightarrow \mathbb{R}^+$
  $$\exp_b(x) = b^x$$
  $$\exp_b(0) = b^0 = 1$$
  $$\exp_b(-x) = b^{-x} = 1/b^x$$

- The exponential function is one-to-one and onto:
  for any positive real number $b \neq 1$, $b^v = b^u \Rightarrow u = v$, $\forall \, u, v \in \mathbb{R}$

- Laws of exponents: $\forall \, b, c \in \mathbb{R}^+$ and $u, v \in \mathbb{R}$
  $$b^u b^v = b^{u+v}$$
  $$b^u / b^v = b^{u-v}$$
  $$(b^u)^v = b^{uv}$$
  $$(bc)^u = b^u c^u$$
Logarithmic functions

- The logarithmic function with base b: \( \log_b : \mathbb{R^+} \rightarrow \mathbb{R} \)
  \[ \log_b(x) = y \iff b^y = x \]
- The logarithmic function is one-to-one and onto:
  for any positive real number \( b \neq 1 \),
  \[ \log_b u = \log_b v \implies u = v, \quad \forall u, v \in \mathbb{R^+} \]
- Properties of logarithms: \( \forall \ b, c, x \in \mathbb{R^+} \), with \( b \neq 1 \) and \( c \neq 1 \)
  \[ \log_b(xy) = \log_b x + \log_b y \]
  \[ \log_b(x/y) = \log_b x - \log_b y \]
  \[ \log_b(x^a) = a \log_b x \]
  \[ \log_c x = \log_b x / \log_b c \]
Logarithmic functions: example proofs

\[ \forall b, c, x \in \mathbb{R}^+, \text{ with } b \neq 1 \text{ and } c \neq 1: \log_c x = \log_b x / \log_b c \]

Proof:

Suppose positive real numbers b, c, and x are given, s.t.

(1) \( u = \log_b c \)  
(2) \( v = \log_c x \)  
(3) \( w = \log_b x \)

By definition of logarithm: \( c = b^u, x = c^v \) and \( x = b^w \)

\( x = c^v = (b^u)^v = b^{uv} \), \ by laws of exponents

So \( x = b^w = b^{uv} \), so \( uv = w \)

That is, \( (\log_b c)(\log_c x) = \log_b x \), \ by (1), (2), and (3)

By dividing both sides by \( \log_b c \): \( \log_c x = \log_b x / \log_b c \quad \blacksquare \)
Logarithmic functions: notations

- Logarithms with base 10 are called **common logarithms** and are denoted by simply log.

- Logarithms with base $e$ are called **natural logarithms** and are denoted by ln.

**Example:**

$$\log_2 5 = \log 5 / \log 2 = \ln 5 / \ln 2$$
One-to-one correspondences

• A one-to-one correspondence (or bijection) from a set $X$ to a set $Y$ is a function $F: X \rightarrow Y$ that is both one-to-one and onto.

• Example:
One-to-one correspondences: example 2

- A function from a power set to a set of strings
  \[ h : P(\{a, b\}) \rightarrow \{00, 01, 10, 11\} \]

If \( a \) is in \( A \), write a 1 in the 1\(^{st}\) position of the string \( h(A) \).
If \( a \) is not in \( A \), write a 0 in the 1\(^{st}\) position of the string \( h(A) \).
If \( b \) is in \( A \), write a 1 in the 2\(^{nd}\) position of the string \( h(A) \).
If \( b \) is not in \( A \), write a 0 in the 2\(^{nd}\) position of the string \( h(A) \).

<table>
<thead>
<tr>
<th>Subset of ( {a, b} )</th>
<th>Status of ( a )</th>
<th>Status of ( b )</th>
<th>String in ( S )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \emptyset )</td>
<td>not in</td>
<td>not in</td>
<td>00</td>
</tr>
<tr>
<td>( {a} )</td>
<td>in</td>
<td>not in</td>
<td>10</td>
</tr>
<tr>
<td>( {b} )</td>
<td>not in</td>
<td>in</td>
<td>01</td>
</tr>
<tr>
<td>( {a, b} )</td>
<td>in</td>
<td>in</td>
<td>11</td>
</tr>
</tbody>
</table>
One-to-one correspondences: example 3

- **Example:** $F: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$

  \[ F(x, y) = (x + y, x - y), \text{ for all } (x, y) \in \mathbb{R} \times \mathbb{R} \]

**Proof that $F$ is one-to-one:**

Suppose that $(x_1, y_1)$ and $(x_2, y_2)$ are any ordered pairs in $\mathbb{R} \times \mathbb{R}$ such that $F(x_1, y_1) = F(x_2, y_2)$.

\[ (x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2), \text{ by definition of } F \]

\[ (1) \ x_1 + y_1 = x_2 + y_2 \quad \text{and} \quad (2) \ x_1 - y_1 = x_2 - y_2, \text{ by pair equalty} \]

\[ (1) + (2) \Rightarrow 2x_1 = 2x_2 \Rightarrow (3) \ x_1 = x_2 \]

Substituting (3) in (2) \[ x_1 + y_1 = x_1 + y_2 \Rightarrow y_1 = y_2 \]

So, $(x_1, y_1) = (x_2, y_2)$

So, $F$ is one-to-one.
Example: \( F: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R} \)

\[ F(x, y) = (x + y, x - y), \text{ for all } (x, y) \in \mathbb{R} \times \mathbb{R} \]

Proof that \( F \) is onto:

Let \((u,v)\) be any ordered pair in \(\mathbb{R} \times \mathbb{R}\)

Suppose that we found \((r, s) \in \mathbb{R} \times \mathbb{R}\) such that \(F(r, s) = (u, v)\).

\[ (r + s, r - s) = (u, v) \iff r + s = u \quad \text{and} \quad r - s = v \]

\[ 2r = u + v \quad \text{and} \quad 2s = u - v \]

\[ r = \frac{u + v}{2} \quad \text{and} \quad s = \frac{u - v}{2} \]

We found \((r, s) \in \mathbb{R} \times \mathbb{R}\) such that \(F(r, s) = (u, v)\)

So, \( F \) is onto.

Thus, \( F \) is a One-to-One correspondence.
Inverse functions

- If $F: X \rightarrow Y$ is a one-to-one correspondence, then there is an inverse function for $F$, $F^{-1}: Y \rightarrow X$, such that for any element $y \in Y$,

  $$F^{-1}(y) = \text{that unique element } x \in X \text{ such that } F(x) = y$$

  $$F^{-1}(y) = x \iff y = F(x)$$

$X = \text{domain of } F$  $Y = \text{co-domain of } F$
Inverse functions: example 1

- Function $h$:  

\[ P(\{a, b\}) \xrightarrow{h} S \]

\[
\begin{align*}
\emptyset & \rightarrow 00 \\
\{a\} & \rightarrow 10 \\
\{b\} & \rightarrow 01 \\
\{a, b\} & \rightarrow 11
\end{align*}
\]

The inverse function for $h$ is $h^{-1}$:

\[ P(\{a, b\}) \xleftarrow{h^{-1}} S \]

\[
\begin{align*}
\emptyset & \leftarrow 00 & h^{-1}(00) = \emptyset \\
\{a\} & \leftarrow 10 & h^{-1}(10) = \{a\} \\
\{b\} & \leftarrow 01 & h^{-1}(01) = \{b\} \\
\{a, b\} & \leftarrow 11 & h^{-1}(11) = \{a, b\}
\end{align*}
\]
Inverse functions: example 2

- Function \( f : \mathbb{R} \rightarrow \mathbb{R} \)
  \[
  f(x) = 4x - 1 \text{ for all real numbers } x.
  \]

The inverse function for \( f \) is \( f^{-1} : \mathbb{R} \rightarrow \mathbb{R} \),
for any \( y \) in \( \mathbb{R} \),
\( f^{-1}(y) \) is that unique real number \( x \) such that \( f(x) = y \).
\[
4x - 1 = y \iff x = (y + 1)/4
\]
Hence, \( f^{-1}(y) = (y + 1)/4 \).
Inverse functions: one-to-one, onto

If $X$ and $Y$ are sets and $F : X \rightarrow Y$ is one-to-one and onto, then $F^{-1} : Y \rightarrow X$ is also one-to-one and onto.

Proof:

$F^{-1}$ is one-to-one:

Suppose $y_1$ and $y_2$ are elements of $Y$, such that $F^{-1}(y_1) = F^{-1}(y_2)$.

Let $x = F^{-1}(y_1) = F^{-1}(y_2)$. Then $x \in X$.

By definition of $F^{-1}$, $F(x) = y_1$ and $F(x) = y_2$, so $y_1 = y_2$.

$F^{-1}$ is onto:

Suppose $x \in X$. Need to find $y$ in $Y$, such that $F^{-1}(y) = x$.

Let $y = F(x)$. Then $y \in Y$.

By definition of $F^{-1}$, $F^{-1}(y) = x$. 

The Pigeonhole principle (sec 9.4)

- A function from a finite set to a smaller set cannot be 1-1: at least 2 elements in the domain have the same image in co-domain.

If $n$ pigeons fly into $m$ pigeonholes with $n > m$, then at least one hole contains two or more pigeons.
The Pigeonhole principle: example 1

- In a group of 6 people, must there be at least two who were born in the same month?
- In a group of 13 people, must there be at least two who were born in the same month.
The Pigeonhole principle: example 2

• Finding the number to pick to ensure a result:
  at least the cardinality of the co-domain + 1

• A drawer contains black and white socks.
  What is the least number of socks you must pull out to be sure to get a matched pair?

  2 socks are not enough: one white and one black

  3 socks are enough by the pigeonhole principle
The Pigeonhole principle: example 3

- **Reach a certain sum:** Let \( A = \{1, 2, 3, 4, 5, 6, 7, 8\} \)
- If we select 4 integers from \( A \), must at least one pair of the integers have a sum of 9? 
  No. Let \( B = \{1, 2, 3, 4\} \)
  \[ 1+2 = 3 ; 1+3 = 4 ; 1+4 = 5 ; 2+3 = 5 ; 2+4 = 6 ; 3+4 = 7 \]
- If we select 5 integers from \( A \), must at least one pair of the integers have a sum of 9? 
  Yes.
Generalized Pigeonhole principle

- For any function $f$ from a finite set $X$ with $n$ elements to a finite set $Y$ with $m$ elements and for any positive integer $k$, if $k < n/m$ (i.e., $km < n$), then there is some $y \in Y$ such that $y$ is the image of at least $k + 1$ distinct elements of $X$.

- **Example:**
  
  $n = 9$ pigeons  
  $m = 4$ holes

  a least one pigeonhole contains 3 or more pigeons.

  $k = 2 < 9/4$, $k+1 = 3$
One-to-one and onto for finite sets

- Let $X$ and $Y$ be finite sets with the **same number of elements** and $f$ is a function from $X$ to $Y$. Then **$f$ is 1-1 $\iff$ $f$ is onto**

**Proof:** Let $X = \{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_m\}$

($\Rightarrow$) If $f$ is 1-1, then $f(x_i)$ for $i = 1, \ldots, m$ are all distinct.
Let $S = \{y \in Y \mid \forall x \in X, f(x) \neq y\}$; all $\{f(x_i)\}$ and $S$ are mutually disjoint.

$m = |Y| = |\{f(x_1)\}| + |\{f(x_2)\}| + \ldots + |\{f(x_m)\}| + |S| = m + |S|$

$\iff |S| = 0$, no element of $Y$ is not the image of some element of $X$.

That is, $f$ is onto.

($\Leftarrow$) If $f$ is onto, then $|f^{-1}(y_i)| \geq 1$ for all $i = 1, \ldots, m$.

All $\{f^{-1}(y_i)\}$ are mutually disjoint by $f$.

$m = |X| = |f^{-1}(y_1)| + \ldots + |f^{-1}(y_m)|$. $m$ terms, so $|f^{-1}(y_i)| = 1$.

That is, $f$ is 1-1.
Composition of functions

- Let \( f : X \rightarrow Y' \) and \( g : Y \rightarrow Z \) be functions with the property that the range of \( f \) is a subset of the domain of \( g \): \( Y' \subseteq Y \)

The composition of \( f \) and \( g \) is a function \( g \circ f : X \rightarrow Z \):

\[
(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X
\]
Composition of functions: example 1

- $f : \mathbb{Z} \to \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{Z}$
  - $f(n) = n + 1$, for all $n \in \mathbb{Z}$
  - $g(n) = n^2$, for all $n \in \mathbb{Z}$

$(g \circ f)(n) = g(f(n)) = g(n+1) = (n + 1)^2$, for all $n \in \mathbb{Z}$

$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1$, for all $n \in \mathbb{Z}$

$(g \circ f)(1) = (1 + 1)^2 = 4$
$(f \circ g)(1) = 1^2 + 1 = 2$

So, $f \circ g \neq g \circ f$
Composition of functions: example 2

- \( f : \{1,2,3\} \rightarrow \{a,b,c,d\} \) and \( g : \{a,b,c,d,e\} \rightarrow \{x,y,z\} \)

\[ X \xrightarrow{f} Y \xrightarrow{g} Z \]

\[ X \xrightarrow{g \circ f} Z \]
X = \{a, b, c, d\} and Y = \{u, v, w\}, f : X \rightarrow Y

I_X : X \rightarrow X is an identity function
I_X(x) = x, for all x \in X

(f \circ I_X )(x) = f(I_X(x)) = f(x), for all x \in X

I_Y : Y \rightarrow Y is an identity function
I_Y(y) = y, for all y \in Y

(I_Y \circ f)(x) = I_Y(f(x)) = f(x), for all x \in X
Composition of functions: example 4

- Composing a function with its inverse:

Let $f : \{a, b, c\} \rightarrow \{x, y, z\}$ be a one-to-one and onto function.

$f$ is one-to-one correspondence $\Rightarrow f^{-1} : \{x, y, z\} \rightarrow \{a, b, c\}$

$\begin{align*}
(f^{-1} \circ f)(a) &= f^{-1}(f(a)) = f^{-1}(z) = a \\
(f^{-1} \circ f)(b) &= f^{-1}(f(b)) = f^{-1}(x) = b \\
(f^{-1} \circ f)(c) &= f^{-1}(f(c)) = f^{-1}(y) = c
\end{align*}$

$\Rightarrow f^{-1} \circ f = I_X$

also $f \circ f^{-1} = I_Y$
Composition of functions: example 4

- Composing a function with its inverse:

If \( f : X \rightarrow Y \) is a one-to-one and onto function with inverse function \( f^{-1} : Y \rightarrow X \), then (1) \( f^{-1} \circ f = I_X \) and (2) \( f \circ f^{-1} = I_Y \)

**Proof of (1):**

Let \( x \) be any element in \( X \): \( (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x' \in X \) (*)

Definition of inverse function:

\( f^{-1}(b) = a \iff f(a) = b \) for all \( a \in X \) and \( b \in Y \)

\( \Rightarrow f^{-1}(f(x)) = x' \iff f(x') = f(x) \)

Since \( f \) is one-to-one, this implies that \( x' = x \).

(*) \( \Rightarrow (f^{-1} \circ f)(x) = x \)
Composition of one-to-one functions

- If \( f : X \to Y \) and \( g : Y \to Z \) are both one-to-one functions, then \( g \circ f \) is also one-to-one.

**Proof** (by direct proof):
Suppose \( f : X \to Y \) and \( g : Y \to Z \) are both one-to-one functions.

Suppose \( x_1, x_2 \in X \) such that: \((g \circ f)(x_1) = (g \circ f)(x_2)\)

By definition of composition of functions, \( g(f(x_1)) = g(f(x_2)) \).

Since \( g \) is one-to-one, \( f(x_1) = f(x_2) \).

Since \( f \) is one-to-one, \( x_1 = x_2 \).
Composition of one-to-one functions

Example:

\[ f \circ g \]
Composition of onto functions

- If \( f: X \to Y \) and \( g: Y \to Z \) are both onto functions, then \( g \circ f \) is onto.

**Proof:**

Suppose \( f: X \to Y \) and \( g: Y \to Z \) are both onto functions.

Let \( z \) be an element of \( Z \).

Since \( g \) is onto, there is an element \( y \) in \( Y \) such that \( g(y) = z \).

Since \( f \) is onto, there is an element \( x \) in \( X \) such that \( f(x) = y \).

\[ z = g(y) = g(f(x)) = (g \circ f)(x) \implies g \circ f \text{ is onto} \]
Composition of onto functions

- Example:
Cardinality and sizes of infinity

- **cardinal number** (cardinal): describe number of elements in a set.
- **ordinal number** (ordinal): describe order of elements in an ordered set.

- **finite set**: the empty set or a set that can be put into 1-1 correspondence with \{1,2,…,n\} for some positive integer n.

- **infinite set**: a nonempty set that cannot be put into 1-1 correspondence with \{1,2,…,n\} for any positive integer n.

- A set A has the same cardinality a set B if, and only if, there is a 1-1 correspondence from A to B.
  - reflexivity: A has same cardinality as A
  - symmetry: if A has same cardinality as B, then B has same cardinality as A
  - transitivity: if A has same cardinality as B, and B has same cardinality as C, then A has same cardinality as C.
Cardinality: surprising example

- An infinite set and a proper subset can have the same cardinality

- Example:
  \( \mathbb{Z} \), the set of integers, and \( 2\mathbb{Z} \), the set of even numbers have the same cardinality.

**Proof:** define function \( H: \mathbb{Z} \rightarrow 2\mathbb{Z} \) as \( H(n) = 2n \) for all \( n \in \mathbb{Z} \).

- \( H \) is 1-1: if \( H(n_1) = H(n_2) \) then \( n_1 = n_2 \), by def of \( H \) and div by 2.
- \( H \) is onto: any \( m \in 2\mathbb{Z} \), \( m \) is even, so \( m = 2k \) for some \( k \in \mathbb{Z} \)

Thus \( H \) is a 1-1 correspondence.
Countable sets

- Counting

A set is countably infinite if, and only if, it has the same cardinality as $\mathbb{Z}^+$, the set of positive integers.

- A set is countable if, and only if, it is finite or countably infinite.
- A set is uncountable if and only if it is not countable.
Countable sets: easy example

- The set \( Z \) of all integers is countable (and so \( 2Z \) is too)

Proof:
No \( n \) in \( Z \) is counted twice:

1-1: \( n \) in \( Z \) -- at most 1 \( m \) in \( Z^+ \)

All \( n \) in \( Z \) is counted:
onto: each \( n \) in \( Z \) -- some \( m \) in \( Z^+ \)

Formally, define function \( F: Z^+ \rightarrow Z \) as

\[
F(n) = \begin{cases} 
  n/2 & \text{if } n \text{ is an even positive integer} \\
  -(n-1)/2 & \text{if } n \text{ is an odd positive integer}
\end{cases}
\]
Countable sets of same cardinality

- For function $f: A \rightarrow B$, where $A$ and $B$ have the same cardinality,
  if $A$ and $B$ are finite, then $f$ is 1-1 $\iff$ $f$ is onto (slide 53)

- If $A$ and $B$ are infinite, then there exist
  functions that are both 1-1 and onto,
  functions that are 1-1 but not onto,
  functions that are onto but not 1-1.

**Examples:** $\mathbb{Z}^+$ and $\mathbb{Z}$ have the same cardinality (previous slide)

- $i: \mathbb{Z}^+ \rightarrow \mathbb{Z}$ with $i(n)=n$ is 1-1 but not onto
- $j: \mathbb{Z} \rightarrow \mathbb{Z}^+$ with $j(n)=|n|+1$ is onto but not 1-1
Larger infinities? surprising example

- The set $Q^+$ of all positive rational numbers is countable

Rational number are dense:
between any two, there is another!

Proof:

Count following arrows, skipping duplicates

$F(1)=1/1$, $F(2)=1/2$, $F(3)=2/1$, $F(4)=3/1$,
skip $2/2=1/1$, $F(t)=1/3$, …

$F$ is onto: all $q$ in $Q^+$ will be counted

$F$ is 1-1: no $q$ in $Q^+$ is counted twice
Larger infinities: famous example

- The set of **all real numbers** between 0 and 1 is **uncountable**

**Proof** (by contradiction): Suppose the set [0,1] is countable.

Then **decimal representations of all these numbers can be written in a list**, on right:

The i-th number’s j-th decimal digit is \( a_{ij} \):

\[
\begin{align*}
0. \ &a_{11}a_{12}a_{13} \ldots a_{1n} \ldots \\
0. \ &a_{21}a_{22}a_{23} \ldots a_{2n} \ldots \\
0. \ &a_{31}a_{32}a_{33} \ldots a_{3n} \ldots \\
\vdots
\end{align*}
\]

Construct a decimal number \( d = 0.d_1d_2d_3 \ldots d_n \ldots \)

\[
d_n = \begin{cases} 
1 & \text{if } a_{nn} \neq 1 \\
2 & \text{if } a_{nn} = 1
\end{cases}
\]

\( e.g., \ d_1 = 1, \ d_2 = 2, \ d_3 = 1, \ldots \) so \( d = 0.12112\ldots \)

Each n, \( d \) differs from the n-th number on list in n-th decimal digit.

\( d \) is not in the list, contradiction! **Cantor diagonalization process**
Larger infinities: famous example 2

- The set of all real numbers and the set of real numbers between 0 and 1 have the same cardinality

Proof:

Let $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Make a circle:

- no 0 or 1, so top-most point of circle is omitted

Define function $F: S \rightarrow \mathbb{R}$ where $F(x)$ is projection of $x$ on number line.

F is 1-1: different points on circle go to distinct points on number line.

F is onto: for any point on number line, a line can be drawn to top of circle and intersect circle at some point.

Thus, $F$ is a 1-1 correspondence from $S$ to $\mathbb{R}$. 

More countable sets and infinities

- The set of all bit strings (strings of 0’s and 1’s) is countable (think of mapping each positive integer to its binary representation)
- The set of all computer programs in a language is countable (finite alphabet, each symbol translated to bit string)
- The set of all functions from integers to \( \{0,1\} \) is uncountable

- Any subset of any countable set is countable
- Any set with an uncountable subset is uncountable

- There is an infinite sequence of larger infinities.
  Example: \( \mathbb{Z}, \mathcal{P}(\mathbb{Z}), \mathcal{P}(\mathcal{P}(\mathbb{Z})), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{Z}))), \ldots \)