CS2209A 2017
Applied Logic for Computer Science

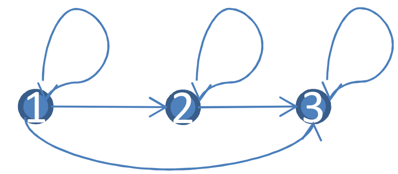
Lecture 18, 19

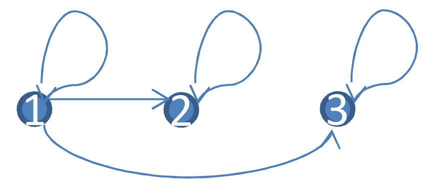
Well-ordering and induction

Instructor: Marc Moreno Maza

Partial and total orders

- A binary relation $R \subseteq A \times A$ is an **order** if R is **reflexive**, **anti-symmetric** and **transitive**.
  - R is a **total order** if $\forall x, y \in A \;\; R(x,y) \vee R(y,x)$
    - That is, every two elements of A are related.
    - E.g. $R_1 = \{(x,y) | x,y \in \mathbb{Z} \wedge x \leq y\}$ is a total order.
    - So is alphabetical order of English words.
    - But not $R_2 = \{(x,y) | x,y \in \mathbb{Z} \wedge x < y\}$
      - not reflexive, so not an order.





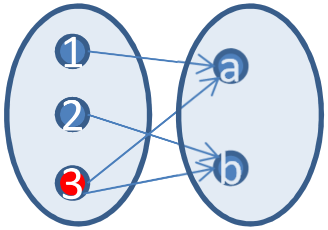
  - Otherwise, R is a **partial order**.
    - $SUBSETS = \{(A,B) \mid A, B \; are \; sets \wedge \; A \subseteq B\}$ is a partial order.
      - Reflexive: $\forall A, \;\; A \subseteq A$
      - Anti-symmetric: $\forall \, A, B \;\; A \subseteq B \wedge B \subseteq A \rightarrow A = B$
      - Transitive: $\forall A, B, C \;\; A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$
      - Not total: if A ={1,2} and B ={1,3}, then neither $A \subseteq B$ nor $B \subseteq A$
    - $DIVISORS = \{(\mathrm{x,y}) \mid x, y \in \mathbb{N} \wedge x, y \geq 2 \;\wedge \exists z \in \mathbb{N} \;\; y = z \cdot x\}$ is a partial order.
    - PARENT is not an order. But ANCESTOR would be, if defined so that each person is an ancestor of themselves. It is a partial order.

Partial and total orders

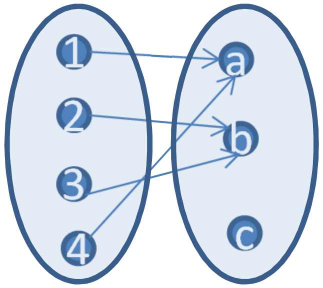
- An order may have **minimal** and **maximal** elements (maybe multiple)
  - $x \in A$ is minimal in R if $\forall y \in A \;\; y \neq x \rightarrow \;\neg R(y, x)$
    - and maximal if $\forall y \in A \; y \neq x \rightarrow \neg R(x, y)$
  - Ø is minimal in SUBSETS (its unique minimum); universe is maximal (its unique maximum).
  - All primes are minimal in DIVISORS, and there are no maximal elements.

Functions

- **A function** $f: X \to Y$ is a **relation** on $X \times Y$ such that for every $x \in X$ there is **at most one** $y \in Y$ for which (x, y) is in the relation.
  - Usual notation: $f(x) = y$
    - y is an **image** of x under f.
  - X is the **domain** of f
  - Y is the **codomain** of f
  - **Range** of f (**image** of X under f):
    - $\{y \in Y \mid \exists x \in X, f(x) = y\}$
  - **Preimage** of a given $y \in Y$:
    - $\{x \in X \mid f(x) = y\}$
      - Preimage of b is {2,3}.



This R is not a function

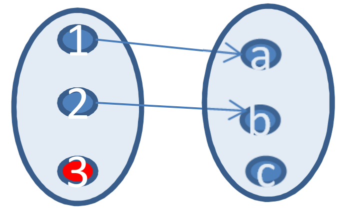


This R is a function with domain {1,2,3,4}, codomain {a,b,c} and range {a,b}

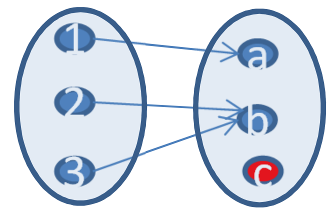
Functions

- **A function** $f: X \rightarrow Y$ **is**
  - **Total**: $\forall x \in X\ \exists y \in Y\ f(x) = y$
    - f: $\mathbb{Z} \rightarrow \mathbb{Z}$
    - $f(x) = x + 1$ is total.
    - $f(x) = \frac{100}{x}$ is not total. Why?
  - **Onto**: $\forall y \in Y\ \exists x \in X\ f(x) = y$
    - $f(x) = x + 1$ is onto over $\mathbb{Z}$, but not over $\mathbb{N}$
  - **One-to-one:** $\forall x_1, x_2 \in X\ (f(x_1) = \mathrm{f}(\mathrm{x}_1) \rightarrow x_1 = x_2)$
    - $f(x) = x + 1$ is one-to-one.
    - $f(x) = x^2$ is not one-to-one
  - **Bijection**: both one-to-one and onto.
    - $f(x) = x + 1$ is a bijection over $\mathbb{Z}$.

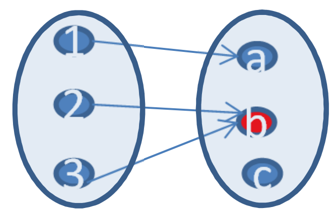
Not total



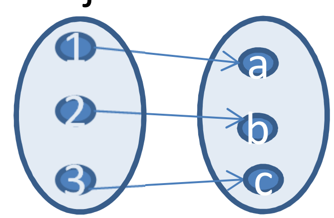
Not onto



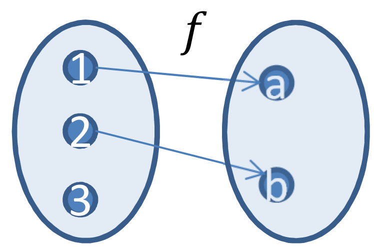
Not one-to-one



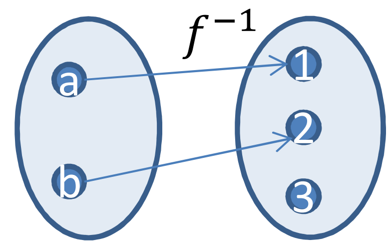
Bijection



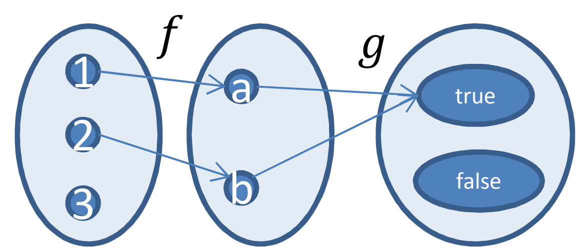
Functions



- An **inverse** of f is $f^{-1}: Y \rightarrow X$, such that $f^{-1}(y) = x$ iff $f(x) = y$
  - $f(x) = x + 1, f^{-1}(y) = y - 1$
  - *Only one-to-one functions have an inverse*



- **Composition** of $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ is $g \circ f: X \rightarrow Z$ such that $(g \circ f)(x) = g(f(x))$
  - $f(x) = \frac{x}{5}$, $g(x) = \lceil x \rceil$, over $\mathbb{R}$
    - $\lceil x \rceil$ is ceiling: x rounded up to nearest integer.
  - $(g \circ f)(x) = g(f(x)) = \left\lceil \frac{x}{5} \right\rceil$
  - $(f \circ g)(x) = f(g(x)) = \frac{\lceil x \rceil}{5}$
  - $(g \circ f)(12.5) = \lceil 2.5 \rceil = 3$
  - $(f \circ g)(12.5) = 13/5 = 2.6$
    - Order matters!



Puzzle: coins

- A not-too-far-away country recently got rid of a penny coin, and now everything needs to be rounded to the nearest multiple of 5 cents…
  - Suppose that instead of just dropping the penny, they would introduce a 3 cent coin.
    - Like British three pence.
  - What is the largest amount that cannot be paid by using only existing coins (5, 10, 25) and a 3c coin?

7c

Any number n >7 can be paid with 3,5,10,25 coins (even just 3 and 5).

Well-ordering principle

- **Any non-empty subset of natural numbers contains the least element**
  - With respect to the usual total order $x \leq y$
  - Very useful for proofs!

Well-ordering principle

- Coins: $\forall x \in \mathbb{N}$, if x >7 then $\exists\ y, z \in \mathbb{N}$ such that x = 3y+5z. So any amount >7 can be paid with 3s and 5s.
  - Suppose, for the sake of **contradiction**, that there are amounts greater than 7 which cannot be paid with 3s and 5s.
  - *Take a set S of all such amounts. Since $S \subseteq \mathbb{N}$, and we assumed that $S \neq \emptyset$, by well-ordering principle S has the least element. Call it n.*
  - Now, look at n-3; it cannot be paid by 3s and 5s either.
  - Since n is the least element of S, $n - 3 \leq 7 < n$
  - 3 cases:
    - n-3 = 7. Then n=10=2*5.
    - n-3 = 6. Then n=9=3*3
    - n-3 = 5. Then n=8=3+5.
  - In all three cases, got a contradiction.
  - Therefore, for every $x \in \mathbb{N}$, if x >7 then x=3y+5z for some $y, z \in \mathbb{N}$.

Sums, products and sequences

- How to write long sums, e.g., 1+2+… (n-1)+n concisely?
  - Sum notation ("sum from 1 to n"): $\sum_{i=1}^{n} i = 1 + 2 + \ \ldots + n$
    - If n=3, $\sum_{i=1}^{3} i$ = 1+2+3=6.
    - The name "i" does not matter. Could use another letter not yet in use.
- In general, let $f: \mathbb{Z} \to \mathbb{R},\ m, n \in \mathbb{Z}, m \leq n$.
  - $\sum_{i=m}^{n} f(i) = \ f(m) + f(m+1) + \cdots + f(n)$
    - If m=n, $\sum_{i=m}^{n} f(i)$ =f(m)=f(n).
    - If n=m+1, $\sum_{i=m}^{n} f(i)$ = f(m)+f(m+1)
    - If n>m, $\sum_{i=m}^{n} f(i)$ = $(\sum_{i=m}^{n-1} f(i)) + f(n)$
    - Example: $f(x) = x^2$. $2^2 + 3^2 + 4^2 = \sum_{i=2}^{4} i^2 = 29$

Sums, products and sequences

- Similarly for product notation (product from m to n):
  - $\prod_{i=m}^{n} f(i) = f(m) \cdot f(m+1) \cdot \ldots \cdot f(n) = (\prod_{i=m}^{n-1} f(i)) \cdot f(n)$
  - For $f(x) = x,\ 2 \cdot 3 \cdot 4 \ = \prod_{i=2}^{4} i = 24$
  - $1 \cdot 2 \cdot \ldots \cdot n = \prod_{i=1}^{n} i = n!$ (n factorial)

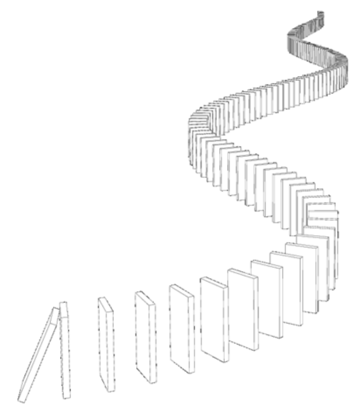
Sum of numbers formula

- Claim: for any n∈ ℕ, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- Proof.
  - Suppose not.
  - Let S be a set of all numbers n' such that $\sum_{i=0}^{n'} i \neq \frac{n'(n'+1)}{2}$. By well-ordering principle, if $S \neq \emptyset$, then there is the least number k in S.
  - Case 1: k=0. But $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$. So formula works for k=0.
  - Case 2: k>0. Then $k - 1 \geq 0$.
    - So $\sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i)$ +k.
    - As k is the smallest bad number, the formula works for k-1.
    - So $\sum_{i=0}^{k-1} i = \frac{(k-1)k}{2}$
    - Now, $\sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i)$ +k = $\frac{(k-1)k}{2} + k = \frac{k^2-k+2k}{2} = \frac{k^2+k}{2} = \frac{k(k+1)}{2}$
    - So the formula works for k>0, too.
  - Contradiction. So S is empty, thus the formula works for all $n \in \mathbb{N}$.

Gauss' proof:
1 + 2 + … + 99 + 100 +
100 + 99 + … + 2 + 1 =
101 + 101+ … +101 + 101 =100*101
So 1+2+ … + 99 + 100 =$\frac{100*101}{2}$
Works for any n, not just n=100

Mathematical induction

- Want to prove a statement $\forall x \in \mathbb{N}\ \ P(x)$.
  - Check that $P(0)$ holds
  - And whenever $P(k)$ does not hold for some k, $P(k-1)$ does not hold either
    - Contradicting well-ordering principle.
    - Contrapositive:
      - if P(k-1) holds for arbitrary k,
      - then P(k) also must be true.
  - Conclude that $\forall x \in \mathbb{N}\ \ P(x)$



Mathematical induction

- Want to prove a statement $\forall x \in \mathbb{N}\ P(x)$.
  - Check that $P(0)$ holds
    Proving that P(0) holds is called the **base case**.
  - And whenever $P(k)$ does not hold for some k, $P(k-1)$ does not hold either
    - Contradicting well-ordering principle.
    - Contrapositive:
      That P(k-1) holds is an **induction hypothesis**
      - if P(k-1) holds for arbitrary k,
      - then P(k) also must be true.
      Proving that P(k-1) → P(k) Is the **induction step**
  - Conclude that $\forall x \in \mathbb{N}\ P(x)$

Mathematical Induction principle:
If $P(0) \land \forall\, k \in \mathbb{N}$ P(k) → P(k+1) then $\forall x \in \mathbb{N}\, P(x)$

Sum of numbers formula

- Claim: for any n$\in \mathbb{N}$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- Proof (by **induction**).
  - P(n) is $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ (*statement* we are proving by induction on n)
  - ***Base case****:* k=0. Then $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$.
  - ***Induction hypothesis****:* Assume that $\sum_{i=0}^{k-1} i = \frac{(k-1)k}{2}$ for an arbitrary k >0
    - That is, for an arbitrary number k-1 $\in \mathbb{N}$
    - Can take k instead of k-1, but k-1 makes calculations simpler.
  - ***Induction step****:* show that P(k-1) implies P(k).
    - $\sum_{i=0}^{k} i = (\sum_{i=1}^{k-1} i)$ +k.
    - By induction hypothesis, $\sum_{i=1}^{k-1} i = \frac{(k-1)k}{2}$
    - Now, $\sum_{i=1}^{k} i = (\sum_{i=1}^{k-1} i)$ +k = $\frac{(k-1)k}{2} + k = \frac{k^2-k+2k}{2} = \frac{k^2+k}{2} = \frac{k(k+1)}{2}$
  - ***By induction***, therefore, P(n) holds for all $n \in \mathbb{N}$.

Changing the base case

- Mathematical Induction principle:
  - $(\mathrm{P}(0) \wedge \forall\, k \in \mathbb{N}$ P(k) → P(k+1)) → $\forall x \in \mathbb{N}\ P(x)$
- What if want to prove it only for $x \geq a$?
  - Make a the base case (when $a \geq 0$). For the rest, assume $k \geq a$.
  - $(\mathrm{P}(\mathrm{a}) \wedge \forall\, k \geq a$ P(k) → P(k+1)) → $\forall x \geq a\ \ P(x)$
    - Here, $\forall x \geq a\ \ P(x)$ is a shorthand for $$\forall x \in \mathbb{N}\ \ \big(x \geq a \rightarrow P(x)\big)$$
  - To prove it works, prove P(n’) where n’ = n-a.

Changing the base case

- Example: show that for all $n \geq 4,\ 2^n \geq n^2$
  - $P(n)$: $2^n \geq n^2$
  - **Base case**: n=4. $2^4 = 16 = 4^2$
  - **Induction hypothesis**: assume that for an arbitrary $k \geq a$, $2^k \geq k^2$
  - **Induction step**: show that $2^k \geq k^2$ implies $2^{k+1} \geq (k+1)^2$
    - $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2$
    - $(k+1)^2 = k^2 + 2k + 1.$
    - Want: $k^2 + k^2 \geq k^2 + 2k + 1$, so $k^2 \geq 2k + 1$
      - Dividing both sides of the inequality by k: $k \geq 2 + \frac{1}{k}$
      - Since k ≥ 4, and $2 + \frac{1}{k} \leq 3$, $2 + \frac{1}{k} \leq 3 < 4 \leq k$. So $k \geq 2 + \frac{1}{k}$ and thus $k^2 \geq 2k + 1$
    - So $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2 \geq k^2 + 2k + 1 = (k+1)^2$
  - **By induction**, for all $n \geq 4,\ 2^n \geq n^2$

- **Corollary**: as n grows, an algorithm running in time n^2 will quickly outperform an algorithm running in time 2^n

Strong induction

- For our coins problem, needed not just P(k-1), but P(k-3), and to look at three cases.
- **Mathematical Induction** principle:
  - $(P(0) \land \forall k \in \mathbb{N}\ \ P(k) \rightarrow P(k+1)) \ \ \rightarrow \forall x \in \mathbb{N}\ P(x)$
- **Strong Induction** principle:
  - $\left(\exists b \in \mathbb{N}\ \ \forall c \in \mathbb{N}\left(0 \leq c \land c \leq b \rightarrow \ P(c)\right)\right)$

    $\land \forall k > b\ \ (\forall\, i\ \ \in \{0, \dots, k-1\}\ \ P(i))\ \ \rightarrow\ \ P(k))$

    $\rightarrow \forall x \in \mathbb{N}\ P(x)$

Strong induction

- Strong induction seems stronger…
  - But in fact, **mathematical induction**, **strong induction** and **well-order principles** are equivalent to each other.
  - So choose the most convenient one.

Puzzle: coins

- A not-too-far-away country recently got rid of a penny coin, and now everything needs to be rounded to the nearest multiple of 5 cents…
  - Suppose that instead of just dropping the penny, they would introduce a 3 cent coin.
    - Like British three pence.
  - What is the largest amount that cannot be paid by using only existing coins (5, 10, 25) and a 3c coin?

7c

Any number n >7 can be paid with 3,5,10,25 coins (even just 3 and 5).

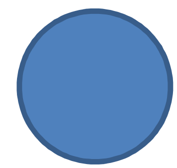
Strong induction

- **Strong Induction** principle (general form):
  - $(\exists b \in \mathbb{N}\ \ \forall c \in \mathbb{N}\left(a \leq c \wedge c \leq b \rightarrow \ \mathrm{P(c)}\right)$
    $\wedge \forall\, k > b\ \ (\forall\, i\ \in \{a, \dots, k-1\}\ \ \mathrm{P(i)}) \rightarrow \mathrm{P(k)})$
    $\rightarrow \forall x \in \mathbb{N}\left(x \geq a \rightarrow\ P(x)\right)$

- **Coins**: $\forall x \in \mathbb{N}$, if x >7 then $\exists\ y, z \in \mathbb{N}$ such that x = 3y+5z.
  - P(n): $\exists\ y, z \in \mathbb{N}\ \ n = 3y + 5z$. Also, a=8.
  - **Base cases**: b = 10, so $c \in \{8,9,10\}$
    - n=8. $8 = 3 \cdot 1 + 5 \cdot 1$, so y=1, z=1.
    - n=9. 9=3· 3, y=3, z=0
    - n=10. 10=5 · 5. y=0, z=2.
  - **Induction hypothesis**: Let k be an arbitrary integer such that $k > 10$. Assume that for all $i \in \mathbb{N}$ such that $8 \leq i\ <$ $k \,\exists\, y_i, z_i \in \mathbb{N}\ \ \ i = 3y_i + 5z_i$
  - **Induction step**. Show that induction hypothesis implies that $\exists\ y, z \in \mathbb{N}\ \ k = 3y + 5z$
    - Since $k \geq b$, $k - 3 \geq a$. So by induction hypothesis $\exists\ y_{k-3}, z_{k-3} \in \mathbb{N}\ \ \ k - 3 = 3y_{k-3} + 5z_{k-3}$. Now take z=$z_{k-3}$ and y = y_{k-3} +1. Then k = 3y+5z.
  - **By strong induction**, get that for all x > 7, $\exists\ y, z \in \mathbb{N}$ such that x = 3y+5z.

Puzzle: all horses are white

- Claim: all horses are white.
- Proof (by induction):
  - P(n): any n horses are white.
  - Base case: P(0) holds vacuously
  - Induction hypothesis: any k horses are white.
  - Induction step: if any k horses are white, then any k+1 horses are white.
    - Take an arbitrary set of k+1 horses. Take a horse out.
      - The remaining k horses are white by induction hypothesis.
    - Now put that horse back in, and take out another horse.
      - Remaining k horses are again white by induction hypothesis.
    - Therefore, all the k+1 horses in that set are white.
  - By induction, all horses are white.



What's wrong here?