CSE 20
DISCRETE MATH

SPRING 2016

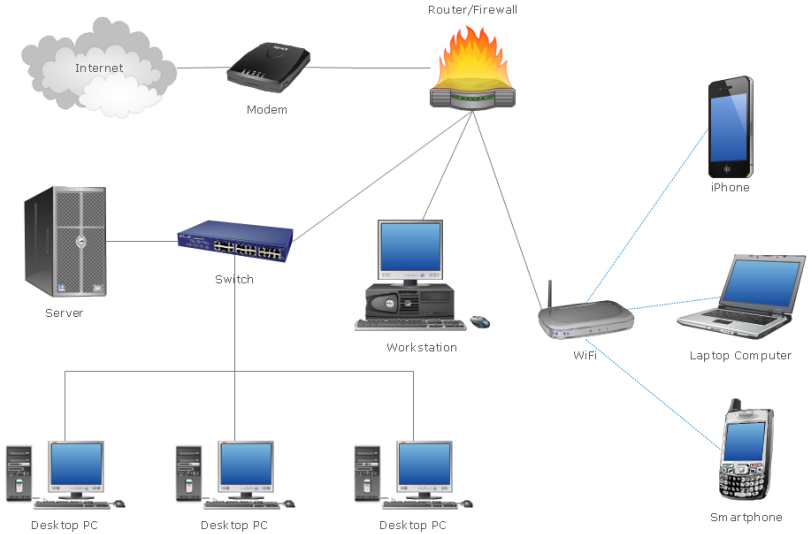
http://cseweb.ucsd.edu/classes/sp16/cse20-ac/

Today's learning goals

- Describe computer representation of sets with bitstrings
- Define and compute the cardinality of finite sets
- Explain the steps in a proof by mathematical induction
- Use mathematical induction to prove
  - correctness of identities and inequalities
  - properties of algorithms
  - properties of geometric constructions

Representing sets

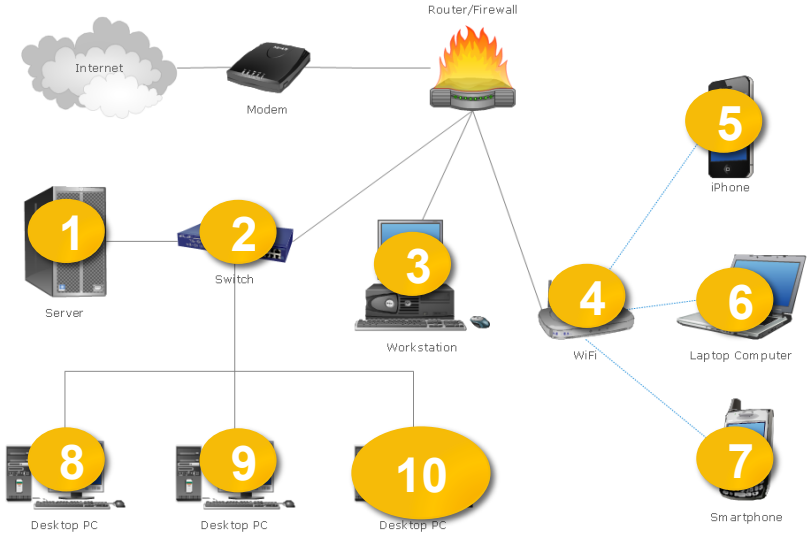
Rosen p. 134



Set of home network components:
{ server, switch, workstation, wifi, iPhone, laptop, Smartphone, Desktop Roommate1, Desktop Roommate2, Desktop Roommate3}

Representing sets

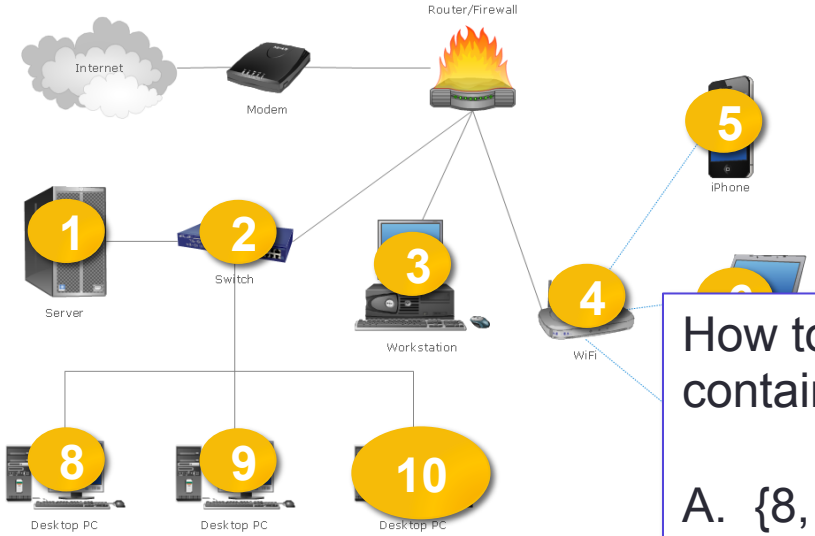
Rosen p. 134



Set of home network components:
{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

Representing sets

Rosen p. 134



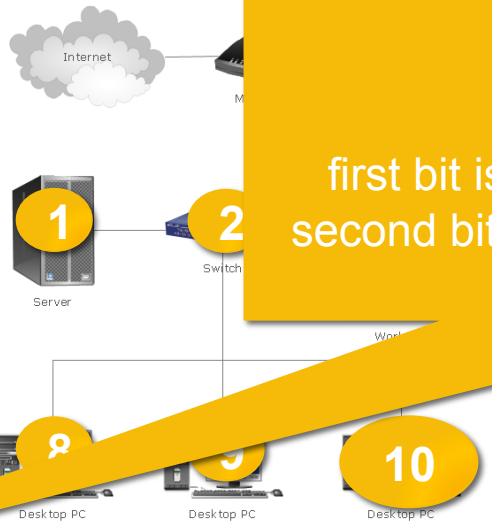
Set of home network components:
{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

How to represent the subset which contains all the desktop PCs?

A. {8, 9, 10}
B. {10, 8, 9}
C. {8, 8, 9, 10}
D. None of the above.
E. All of the above.

Representing sets

Rosen p. 134



Alternatively: using **bit strings**

– – – – – – – – – –

first bit is 0 if item 1 (server) is not in the set; 1 if it is
second bit is 0 if item 2 (switch) is not in the set; 1 if it is

Set of home network components:
{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

How to represent the subset which contains all the desktop PCs **using bit strings**?

A. 0000000000
B. 0000000111
C. 1110000000
D. None of the above.
E. All of the above.

Representing sets

Rosen p. 134

Assume that universal set U is finite of size *n* (and n is not too big).
Specify arbitrary ordering of elements of U: a_1, a_2, a_3, …, a_n .

Represent set X by the bit string where, for each i, the *i*th bit in the bit string is 1 if a_i is an element of X and it's 0 if a_i is not an element of X.

Describe, using set operations, the set described by the bit string which results from taking the bit string for A and flipping each bit 0 → 1, 1 → 0.

A. The power set of A, $\mathcal{P}(A)$
B. The union of A with itself, $A \cup A$
C. The difference U – A
D. The Cartesian product $A \times A$
E. None of the above.

Representing sets

Rosen p. 134

Assume that universal set U is finite of size *n* (and n is not too big).
Specify arbitrary ordering of elements of U: a_1, a_2, a_3, …, a_n .

Represent set X by the bit string where, for each i, the *i*th bit in the bit string is 1 if a_i is an element of X and it's 0 if a_i is not an element of X.

Describe, using set operations, the set described by the bit string which results from taking the bit string for A and flipping each bit 0 → 1, 1 → 0.

A. The power set of A, $\mathcal{P}(A)$ **may not be subset of U**
B. The union of A with itself, $A \cup A$ **= A**
C. The difference U – A **Complement of A**
D. The Cartesian product $A \times A$ **may not be subset of U**
E. None of the a

Operations on sets

Rosen Sections 2.1, 2.2

- If the set A is finite then

$$|\mathcal{P}(A)| = ?$$

What are the possible subsets of A?

*Does the power set of A depend **just** on the size of A?*

*Does the **size** of the power set of A depend **just** on the size of A?*

Operations on sets

Rosen Sections 2.1, 2.2

- If the set A is finite then

Represent subset X of A by the bit string where, for each i, the *i*th bit in the bit string is 1 if a_i is an element of X and it's 0 if a_i is not an element of X.

What are the possible subsets of A?

*Does the power set of A depend **just** on the size of A?*

*Does the **size** of the power set of A depend **just** on the size of A?*

_ _ _ _ … _

a_1 a_2 a_3 a_4…$a_{|A|}$

Operations on sets

Rosen Sections 2.1, 2.2

- If the set A is finite then

$$|\mathcal{P}(A)| = 2^{|A|}$$

What are the possible subsets of A?
*Does the power set of A depend **just** on the size of A?*
*Does the **size** of the power set of A depend **just** on the size of A?*

(0/1) (0/1) (0/1) … (0/1)

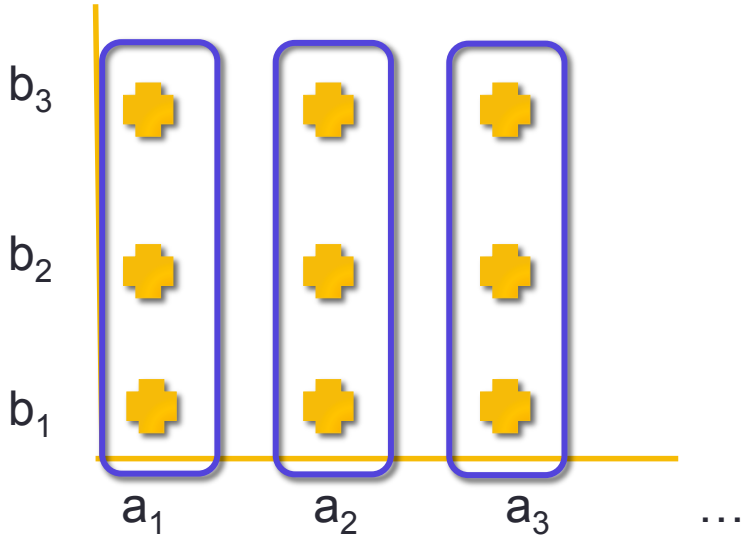
Operations on sets

Rosen Sections 2.1, 2.2

- If the sets A, B are finite **and disjoint** then

$$|A \times B| = |A| \cdot |B|$$

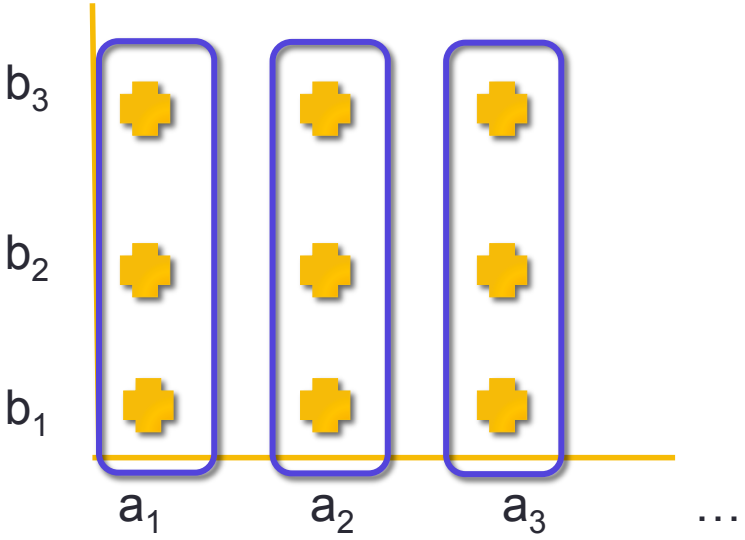
|B| many elements for each of the |A| many elements in A

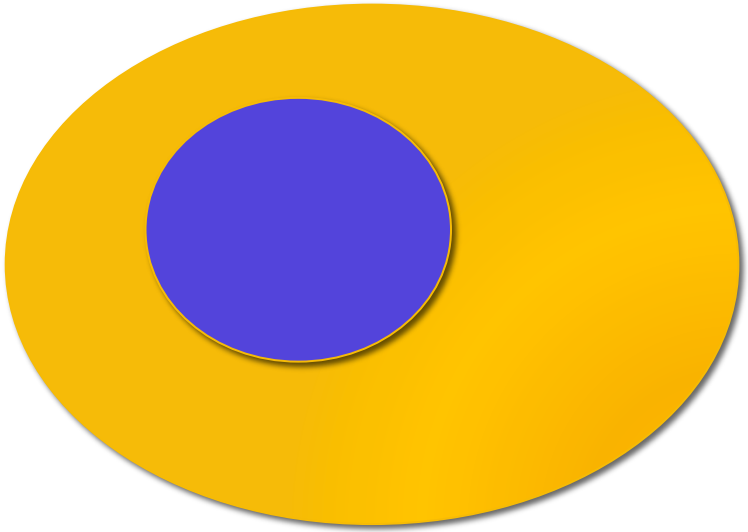


How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B|$$

$$|\mathcal{P}(A)| = 2^{|A|}$$



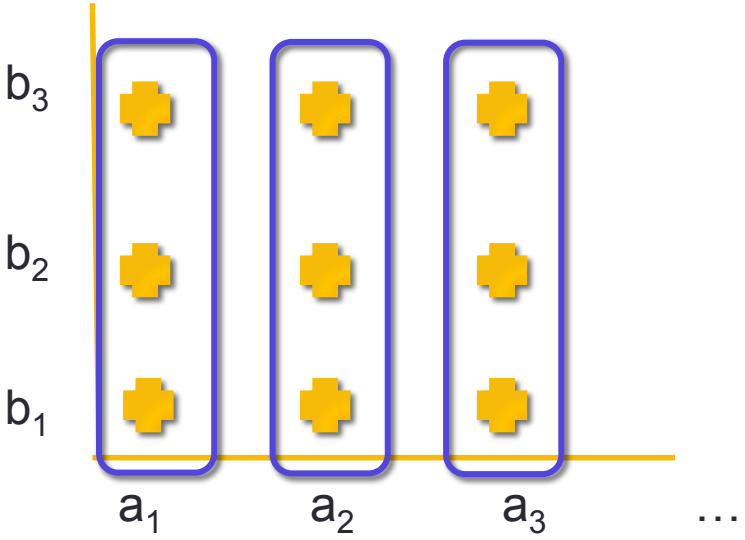


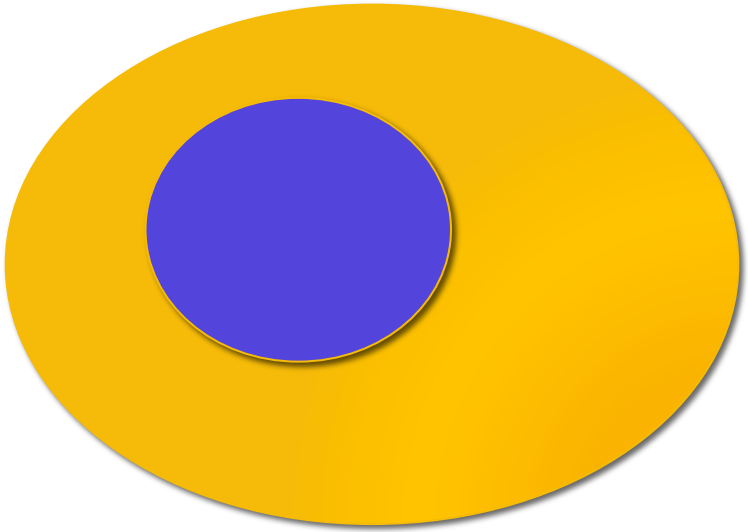
How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B|$$

$$|\mathcal{P}(A)| = 2^{|A|}$$

Key: how do sizes change as increase |A| by 1?



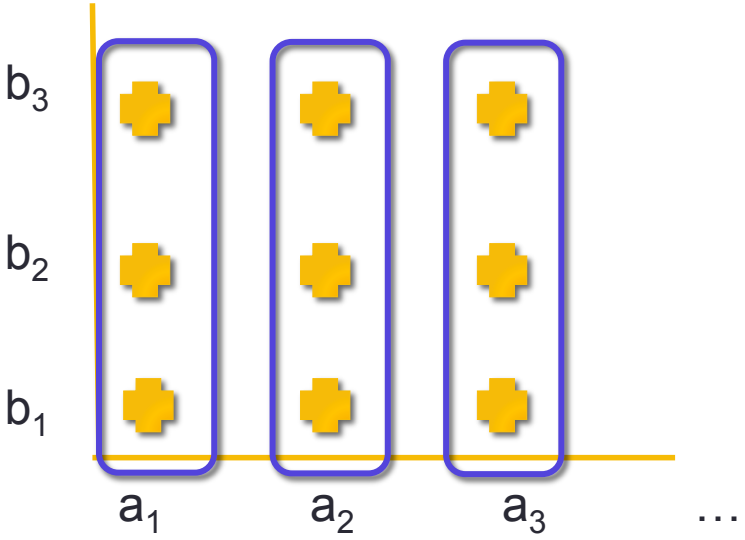


How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B|$$

$$|\mathcal{P}(A)| = 2^{|A|}$$

Key: how do sizes change as increase |A| by 1?



How much does |AxB| change when we add one new element to A?

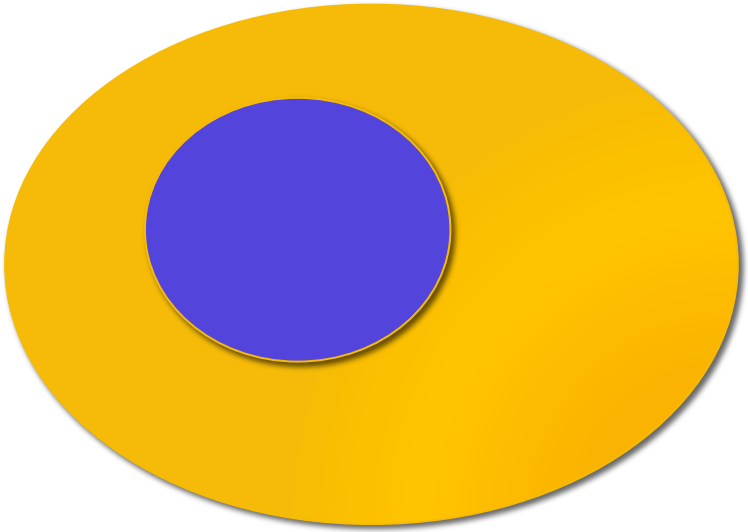
A. Add one element.
B. Add |B| many elements.
C. Multiply number of elements by |B|.
D. Raise number of elements to $|B|^{th}$ power.
E. None of the above.

How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B|$$

$$|\mathcal{P}(A)| = 2^{|A|}$$

Key: how do sizes change as increase |A| by 1?



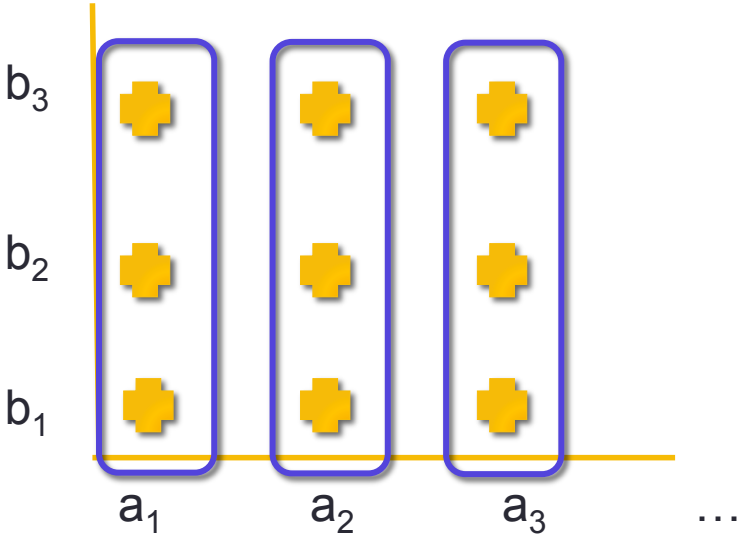
How much does |P(A)| change when we add one new element to A?

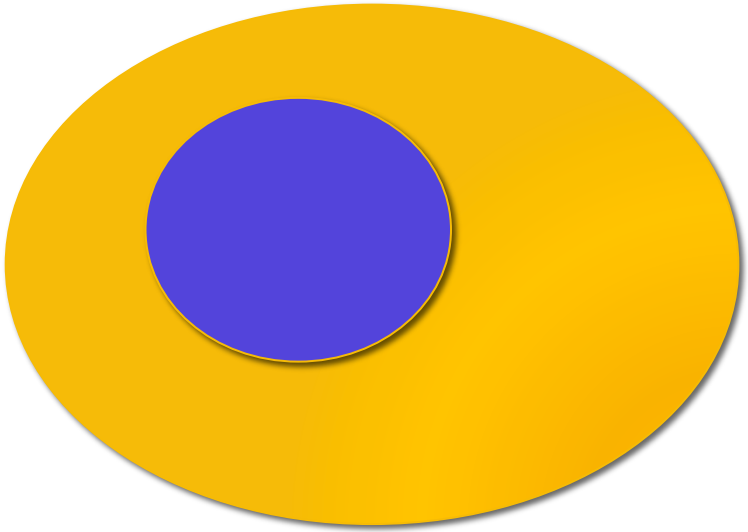
A. Add one element.
B. Add |B| many elements.
C. Multiply number of elements by |B|.
D. Raise number of elements to $|B|^{th}$ power.
E. None of the above.

How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B| \qquad f(n+1) = f(n) + |B|$$

$$|\mathcal{P}(A)| = 2^{|A|} \qquad g(n+1) = 2g(n)$$

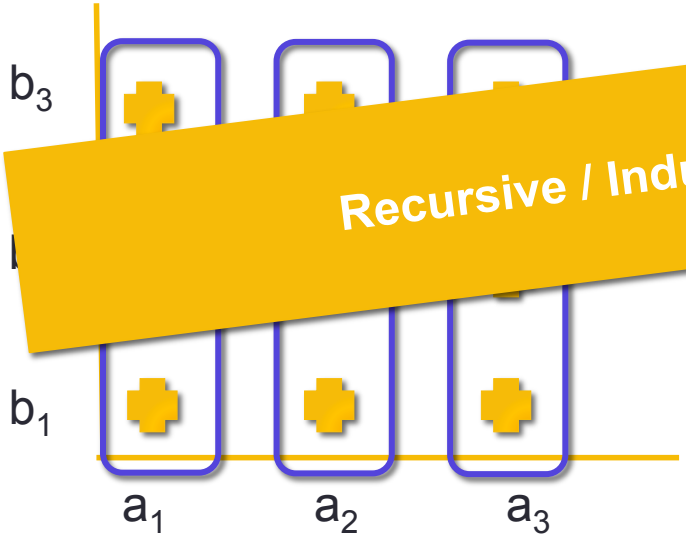




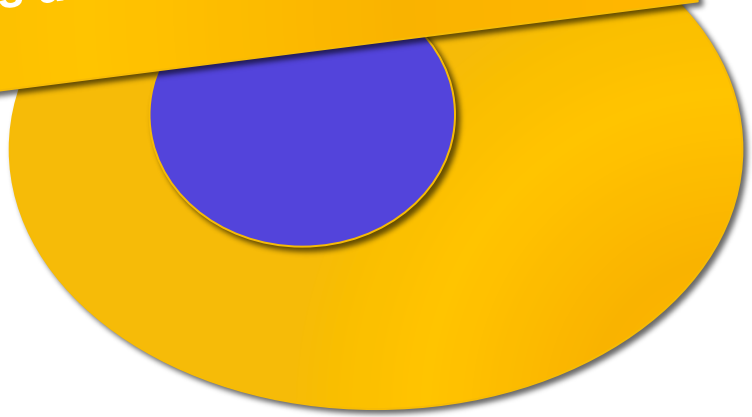
How do we prove these general formulas?

$$|A \times B| = |A| \cdot |B| \qquad f(n+1) = f(n) + |B|$$

$$|\mathcal{P}(A)| = 2^{|A|} \qquad g(n+1) = 2g(n)$$



Recursive / Inductive definitions and induction!



Induction: a road map

- Today
  - What is a proof by induction?
  - Examples: inequalities, algorithms, constructions
- Tuesday
  - Strong induction
  - Recursive definitions: functions, sets, sigma notation
  - More examples / proofs: identities, constructions

Proof strategies so far

Theorem: $\forall x P(x)$ over a given domain.

Strategy (1): Let x be arbitrary element of the domain. WTS P(x) is true.

Strategy (2) if domain finite: Enumerate all x in domain. WTS P(x) is true.

Strategy (3) Proof by contradiction: Assume there is an x with P(x) false. WTS badness!

Theorem: $\exists x P(x)$ over a given domain.

Strategy (1): Define x = …. (some specific element in domain) WTS P(x) is true.

Strategy (2) Proof by contradiction: Assume that for all x, P(x) is false. WTS badness!

Theorem: $P \rightarrow Q$ over a given domain.

Strategy (1): Toward direct proof, assume P and WTS Q.

Strategy (2): Toward proof by contrapositive, assume Q is false and WTS P is also false.

Strategy (3) Proof by contradiction: Assume both P is true and Q is false. WTS badness!

A new proof strategy

Rosen p. 311

To show that some statement P(k) is true about all nonnegative integers k,

1. Show that it's true about 0 — i.e. P(0)
2. Show P(0) → P(1) — Hence conclude P(1)
3. Show P(1) → P(2) — Hence conclude P(2)
4. Show P(2) → P(3) — Hence conclude P(3)
5. …..

A new proof strategy

Rosen p. 311

To ~~show that some~~ statement P(k) is true about all nonnegative integers k,

Need both for induction to be applicable

1. Show that it's true about 0 — i.e. P(
2. Show P(0) → P(1) — Hence conclude P(1)
3. Show P(1) → P(2) — Hence conclude P(2)
4. Show P(2) → P(3) — Hence conclude P(3)
5. …..

Mathematical induction

Rosen p. 311

To show that some statement P(k) is true about all nonnegative integers k,

1. Show that it's true about 0 i.e. P(0)
2. Show $\forall k \; P(k) \rightarrow P(k+1)$ Hence conclude P(1),…

An inequality $\left(1+\frac{1}{2}\right)^n \geq 1+\frac{n}{2}$

Theorem: This inequality is true for all nonnegative integers

Proof: by Mathematical Induction.

What's P(n)?

A. $\left(1+\frac{1}{2}\right)^n \geq 1+\frac{n}{2}$

B. $\left(1+\frac{1}{2}\right) \geq 1+\frac{n}{2}$

C. $\left(1+\frac{1}{2}\right)^k$

D. $\left(1+\frac{n}{2}\right)^k$

E. None of the above.

An inequality $\left(1+\frac{1}{2}\right)^n \geq 1+\frac{n}{2}$

Theorem: This inequality is true for all nonnegative integers

Proof: by Mathematical Induction.

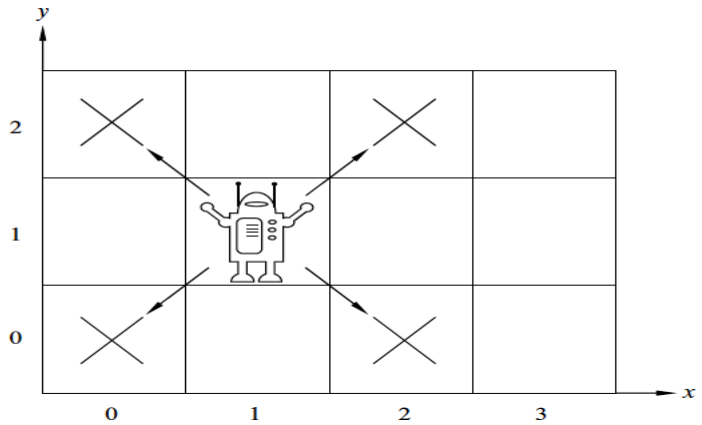
1. Basis step WTS $\left(1+\frac{1}{2}\right)^0 \geq 1+\frac{0}{2}$

2. Inductive hypothesis Let k be a nonnegative integer. Assume
$\left(1+\frac{1}{2}\right)^k \geq 1+\frac{k}{2}$

3. Induction step WTS
$\left(1+\frac{1}{2}\right)^{k+1} \geq 1+\frac{k+1}{2}$

Robot

Start at origin, moves on infinite 2-dimensional integer grid.
At each step, move to diagonally adjacent grid point.



Can it ever reach (1,0)?

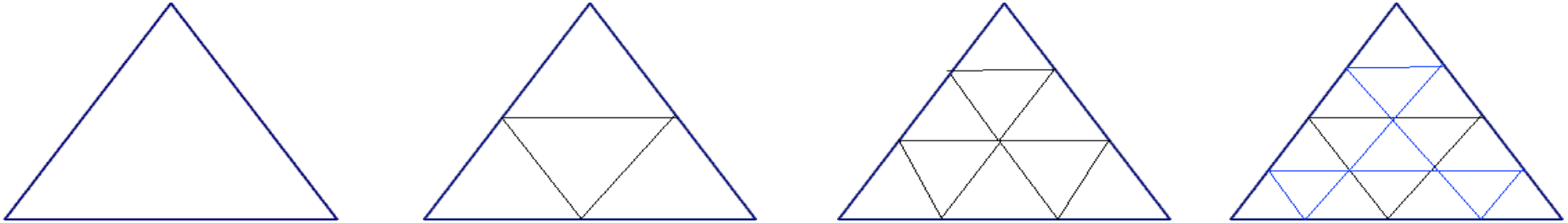
Robot

Lemma (Invariant): The sum of the coordinates of any state reachable by the robot is even.

Proof of Lemma: by mathematical induction on the number of steps.

Using proof: Sum of coordinates of (1,0) is 1 so not even!

Triangles



Theorem: If start with an equilateral triangle and divide each side into n equal segments, then connect the division points with all possible line segments parallel to sides of original triangle, then _____ many small triangles will be contained in the larger one.