Part 2: Sets, Induction, Counting

Contents [DOCUMENT FINALIZED]

Sets

Lecture 7 A central concept in mathematics are **sets**, which we understand to be specified collections of objects.

Objects in a given set are called **elements**.

For any object there must be a definite yes or no answer to the question whether the object is a member of the set.

If object x is an element of set A we write $x \in A$. If not, we write $x \notin A$.

Sets can be described with words, such as

"the set of odd integers between 1 and 12"

or the elements may be listed

$$\{1, 3, 5, 7, 9, 11\}$$

or partially listed if the pattern is obvious:

$$\{1, 3, 5, ..., 11\}$$

To define sets we will use the following set-builder no-

tation:

$$\{x \mid P(x)\}$$

where $P(x)$ is a one-variable predicate that characterizes the membership of x in the set.

Example: If $P(x)$ says

"x is an odd integer between 1 and 12",

then the set $\{x \mid P(x)\}$ is

$$\{1, 3, 5, 7, 9, 11\}$$

Caution: not all predicates lead to meaningful set definitions, as the following paradox shows that goes back to philosopher Bertrand Russell (1902):

$$M = \{x \mid x \text{ is a set that does not contain itself}\}$$

Is $M \in M$? Assume yes, then the set definition says $M \notin M$, a contradiction. On the other hand, if $M \notin M$ then $M \in M$!

These problems can be avoided by adhering to Zermelo's and Fraenkel's (ZF) axiomated set theory, which is beyond the scope of this course.

However, all our discussions of sets are consistent with this theory.

We will use the following notations for sets of numbers:

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ is the set of **natural numbers**.

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, ...\}$ is the set of **integers**.

$\mathbb{Q}$ is the set of **rational numbers**.

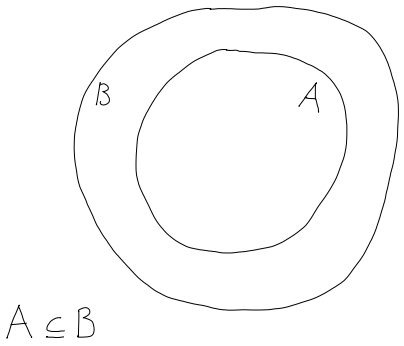
$\mathbb{R}$ is the set of **real numbers**.

Definition: Let $\emptyset = \{x \mid x \neq x\}$. Then $\emptyset$ contains no elements (because $x \neq x$ is false for every object x). $\emptyset$ is called **empty set**.

Definition: Let A and B be sets. We say A is a **subset** of B iff every element of A is also an element of B. In symbols:

$$A \subseteq B \;\Leftrightarrow\; \forall x\, (x \in A \Rightarrow x \in B)$$

Venn Diagram



Examples:

$$\{2, 3, 4\} \subseteq \{1, 2, 3, 4, 5\}$$
$$\{0\} \not\subseteq \{1, 2, 3, 4, 5\}$$

Note: Venn diagrams are useful tools for obtaining intuitions about set relationships. However, drawing Venn diagrams does not constitute a rigorous proof!

Theorem: For any set A,
1. $\emptyset \subseteq A$
2. $A \subseteq A$

Proof:

1. Let A be any set and x be any object. Then, because $x \in \emptyset$ is false, $x \in \emptyset \Rightarrow x \in A$ is true. Therefore $\emptyset \subseteq A$.
2. Let A be any set and x be any object. Then $x \in A \Rightarrow x \in A$ is true, because it is a tautology of the form $P \Rightarrow P$. Therefore, $A \subseteq A$. □

Theorem: Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$, i.e. $\subseteq$ is transitive.

Proof: exercise.

Often the question arises whether two descriptions of sets yield the same set. Intuitively, we call sets A and B equal if they contain exactly the same elements, i.e.

$$A = B \;\Leftrightarrow\; \forall x\, (x \in A \Leftrightarrow x \in B)$$

The latter condition is equivalent to

$$\forall x\, (x \in A \Rightarrow x \in B) \;\wedge\; \forall x\, (x \in B \Rightarrow x \in A)$$

which means

$$A \subseteq B \;\wedge\; B \subseteq A$$

Definition: Let A and B be sets. Then $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

If A is a subset of B, but $A \neq B$, then A is called a **proper subset** of B, denoted as $A \subset B$, or $A \subsetneq B$.

Example: $\{1\} \subsetneq \{1, 2, 3\}$

One of the axioms of set theory asserts that for every set A the collection of all subsets of A is also a set.

Definition: Let A be a set. The **power set** of A is the set whose elements are the subsets of A. It is denoted $\mathcal{P}(A)$. Thus

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Example: Let $A = \{1, 2, 3\}$. Then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$$

Note: elements of $\mathcal{P}(A)$ are themselves sets. When working with sets whose elements are sets, it is important to distinguish "is an element of" and "is a subset of". $A \in B$ reflects whether set A is an element of B, whereas $A \subseteq B$ requires each element of A also to be an element of B.

Example: Let $X = \{\emptyset, \{1, 2, 3\}, \{4, 5\}, 6\}$. All of the following statements are true:

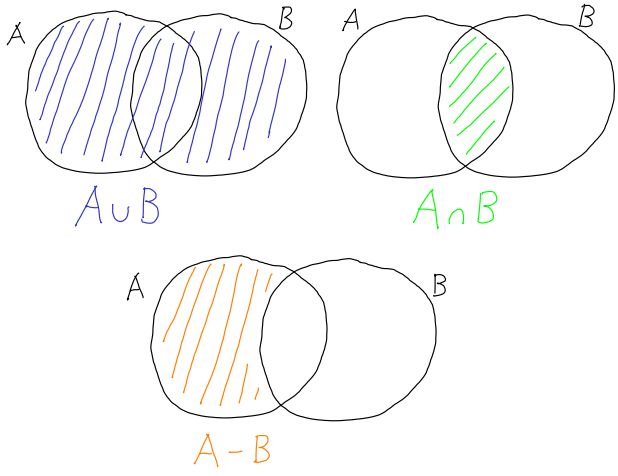
X has 4 elements
$6 \in X$
$\{6\} \notin X$
$\{6\} \subseteq X$
$\emptyset \in X$
$\emptyset \subseteq X$
$\{\{4, 5\}\} \subseteq X$
$\{4, 5\} \in X$
$\{4, 5\} \not\subseteq X$, because $5 \notin X$.

Set Operations

Here we present the most common ways of combining two sets to produce a new set.

Definition: Let A and B be sets.

- The **union** of A and B is the set
$$A \cup B := \{x \mid x \in A \vee x \in B\}$$
- The **intersection** of A and B is the set
$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$
- The **difference** of A and B is the set
$$A - B := \{x \mid x \in A \wedge x \notin B\}$$



Examples: For $A = \{1, 2, 4, 5, 7\}$ and $B = \{1, 3, 5, 9\}$

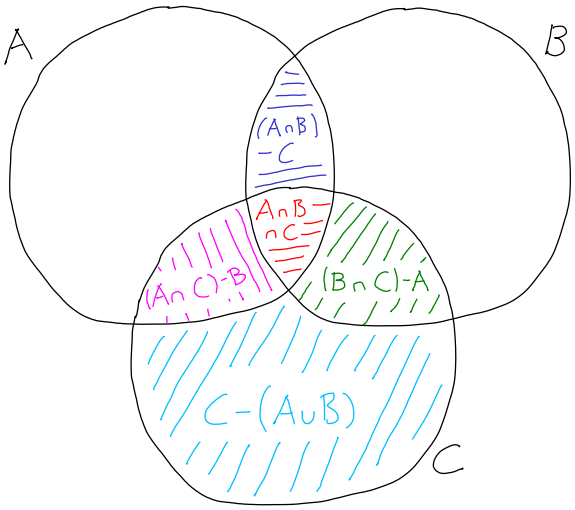
$A \cup B = \{1, 2, 3, 4, 5, 7, 9\}$

$A \cap B = \{1, 5\}$

$A - B = \{2, 4, 7\}$

$B - A = \{3, 9\}$

Another Venn Diagram



Definition
Two sets A and B are **disjoint** iff $A \cap B = \emptyset$.

Examples: The sets of even and odd integers are disjoint, but $\{1\}$ and $\{1, 2\}$ are not.

Like the logical connectives $\wedge, \vee, \neg$ we have seen earlier, the set operations $\cup, \cap, -$ obey certain rules that allow us to simplify set expressions and replace expressions with equivalent ones.

Here is a list of the basic rules:

Theorem: Let A, B, C be sets. Then

1. $A \subseteq A \cup B$
2. $A \cap B \subseteq A$
3. $A \cap \emptyset = \emptyset$
4. $A \cup \emptyset = A$
5. $A \cap A = A$
6. $A \cup A = A$
7. $A - \emptyset = A$
8. $\emptyset - A = \emptyset$
9. $A \cup B = B \cup A$ (commutative)
10. $A \cap B = B \cap A$
11. $(A \cup B) \cup C = A \cup (B \cup C)$ (associative)
12. $(A \cap B) \cap C = A \cap (B \cap C)$
13. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ (distributive)
14. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
15. $A \subseteq B \Leftrightarrow A \cup B = B$
16. $A \subseteq B \Leftrightarrow A \cap B = A$

Selected proofs (others exercise):

2. Prove $A \cap B \subseteq A$. We must show that, if $x \in A \cap B$ then $x \in A$. Suppose $x \in A \cap B$. Then, $x \in A$ and $x \in B$. Therefore, $x \in A$.

16. Prove $A \subseteq B \Leftrightarrow A \cap B = A$. This requires two steps, $\Rightarrow$ and $\Leftarrow$:

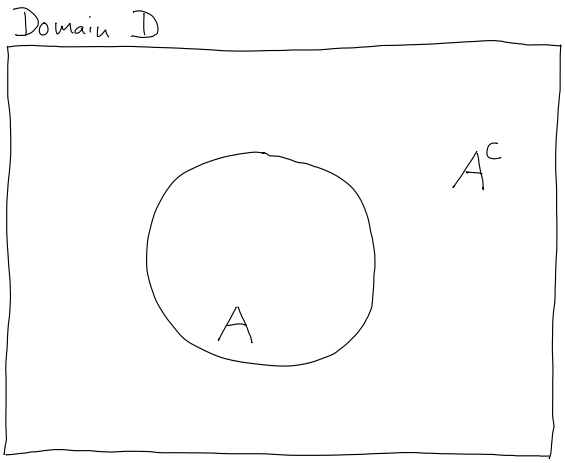
"$\Rightarrow$": Assume $A \subseteq B$. We have to show $A \cap B = A$. We start with $A \subseteq A \cap B$: If $x \in A$, then $x \in B$ according to the assumption, and thus $x \in A \cap B$. On the other hand, $A \cap B \subseteq A$ always holds (fact 2). Together, this shows $A \cap B = A$

"$\Leftarrow$": Assume $A \cap B = A$. We must prove $A \subseteq B$. So, if $x \in A$ then with the assumption we have $x \in A \cap B$, and therefore $x \in B$, which proves the claim. $\square$

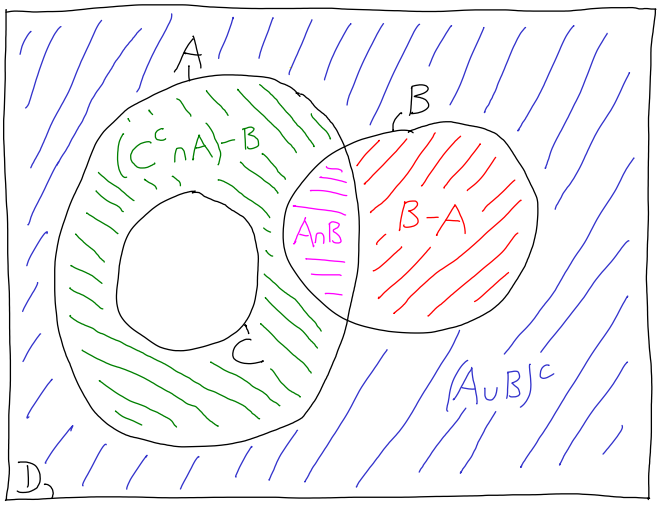
Lecture 8 When forming quantified expressions we introduced the notion of domains from which quantified variables would receive their values. A similar concept is useful in the context of sets.

Definition: If D is the domain and $A \subseteq D$, then we define the **complement** of A to be the set $A^c := D - A$.

Thus, A^c is the set of elements in the domain that are not in A.



Examples:



For $A = \{2, 4, 6, 8\}$, $A^c = \{0, 10, 12, 14, \ldots\}$ if the domain is the even natural numbers.

For domain $\mathbb{R}$, if $A = \{x \mid x \text{ is rational}\}$ then $A^c = \{x \mid x \text{ is irrational}\}$.

Theorem: Complement rules for A and B being subsets of domain D:

1. $(A^c)^c = A$
2. $A \cup A^c = D$
3. $A \cap A^c = \emptyset$
4. $A - B = A \cap B^c$
5. $A \subseteq B \Leftrightarrow B^c \subseteq A^c$
6. $(A \cup B)^c = A^c \cap B^c$ (De Morgan's Laws)
7. $(A \cap B)^c = A^c \cup B^c$
8. $A \cap B = \emptyset \Leftrightarrow A \subseteq B^c$

Note the similarities between $\wedge, \vee, \neg$ and $\cap, \cup$ and complement — they are not a coincidence.

Proof:

5.

$$\begin{aligned} A \subseteq B &\Leftrightarrow \forall x\ (x \in A \Rightarrow x \in B) \\ &\Leftrightarrow \forall x\ (x \notin B \Rightarrow x \notin A) \\ &\Leftrightarrow \forall x\ (x \in B^c \Rightarrow x \in A^c) \\ &\Leftrightarrow B^c \subseteq A^c \end{aligned}$$

Others: exercise.

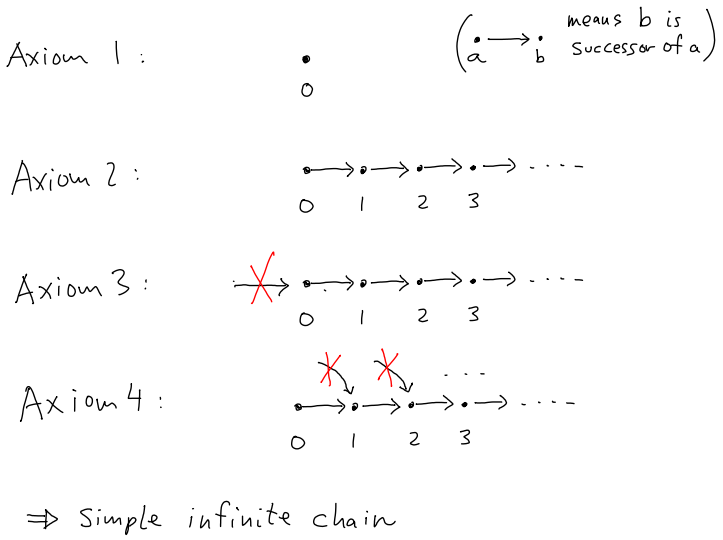
Mathematical Induction

The most familiar number system is the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Giuseppe Peano (1858-1932) devised five axioms, that based on the notion of successors, completely describe $\mathbb{N}$:

1. 0 is a natural number
2. Every natural number has a successor in the natural numbers
3. 0 is not the successor of any natural number
4. If the successor of two natural numbers is the same, then the two original numbers are the same
5. If a set contains 0 and the successor of every number in the set is in the set as well, then the set contains the natural numbers.

Illustration



Peano's fifth axiom leads to a characteristic property of $\mathbb{N}$, the **principle of mathematical induction (PMI)**:

If S is a subset of $\mathbb{N}$ with these properties:

- $0 \in S$
- For all $n \in \mathbb{N}$, if $n \in S$, then $n+1 \in S$,

then $S = \mathbb{N}$.

The PMI allows to do two imporant things: first to make inductive definitions, and second, to prove that some properties are shared by all natural numbers.

Inductive definitions define an infinite set of objects that can be indexed by the natural numbers. I.e., there is a first, second, third object and so on. Basic inductive definitions follow the form of the PMI. We define a first object, and the $(n+1)$-st object is defined in terms of the n-th object. The PMI ensures that the set of all n for which the corresponding object is defined is $\mathbb{N}$.

Example:

The **factorial** of a natural number n (written as $n!$) may be defined inductively:

1. $0! := 1$
2. For $n \in \mathbb{N}$, define $(n+1)! := n! \cdot (n+1)$.

Example:

$$4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2! = 4 \cdot 3 \cdot 2 \cdot 1! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 24$$

Let S be the set of n for which $n!$ is defined. According to 1. $0 \in S$. Condition 2. says how we define $(n+1)!$ in terms of $n!$. Thus, if $n \in S$ then $n+1 \in S$. By the PMI, $S = \mathbb{N}$.

Note: the idea of inductive definitions can be generalized to define complex objects in terms of less complex objects of similar form in a process called structural induction:

Example: Define well-formed propositional formulas

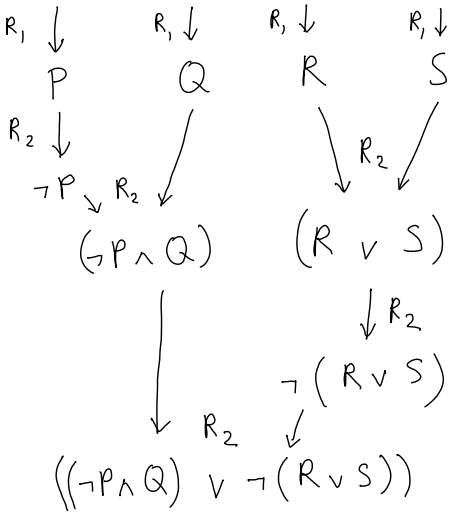
1. All proposition symbols $A, B, \ldots$ are well-formed formulas.
2. If φ and ψ are well-formed formulas, so are $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, and $\neg\varphi$.
3. No other formula is a well-formed formula.

Well formed formulas: Q, $(P \wedge \neg Q)$

To establish whether a formula is well-formed we need to be able to verify that each sub-formula is well-formed and that these sub-formulas have been combined correctly, according to 2. E.g.

$(P \wedge \neg Q) = (\varphi \wedge \psi)$ with $\varphi = P$ and $\psi = \neg Q$. φ is well-formed according to 1. and ψ is well-formed because it can be constructed by applying step 2. to Q.

Example



R_1: Rule 1

R_2: Rule 2

The other important application of PMI is to prove that certain statements hold for all natural numbers n.

Example: We want to prove that

$$\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots(2n-1) = n^2$$

holds for every natural number n.

[Here we are using the "sigma"-notation for sums, which reads: the sum for i equals 1 to n of $2i-1$. Summation terms are computed by setting i to values $1, 2, \ldots, n$ in turn: $(2{\cdot}1{-}1){+}(2{\cdot}2{-}1){+}\ldots{+}(2{\cdot}n{-}1)$. If the upper index is less than the lower index, the value of the sum is 0. Similarly, "pi"-notation is used for products: e.g. $\prod_{i=1}^{n} i \;=\; 1 \cdot 2 \cdots n$. The value of empty products is 1]

In our lifetime we can only check a finite number of cases manually by evaluating the sum and comparing the result with n^2.

So instead, we attempt a proof by using PMI.

Let $S = \{n \in \mathbb{N} \mid \sum_{i=1}^{n}(2i-1) = n^2\}$.

We want to show that $S = \mathbb{N}$, in which case above claim is true for all natural numbers n.

1. For $n = 0$ the sum is empty and $0 = 0^2$. Therefore, $0 \in S$.
2. Let $n \in S$. Then $\sum_{i=1}^{n}(2i-1) = n^2$ holds. We want to prove that $n+1 \in S$, which means
$$\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$$
We note that
$$\sum_{i=1}^{n+1}(2i-1) = [\sum_{i=1}^{n}(2i-1)] + 2(n+1) - 1$$
by splitting up the sum. Now we can use the fact that $n \in S$ and replace the sum that runs up to n by n^2. After simplifying the expression we get to:
$$\sum_{i=1}^{n+1}(2i-1) = [n^2] + 2(n+1) - 1 = (n+1)^2,$$
which means $n+1 \in S$. So, with PMI, $S = \mathbb{N}$. $\square$

To summarize, proofs using the PMI have the following form:

Let $S = \{n \in \mathbb{N} \mid$ statement that holds for $n\}$

1. Prove that $0 \in S$
2. Prove that S is inductive, i.e. $n \in S \Rightarrow (n+1) \in S$
3. By the PMI, $S = \mathbb{N}$

In practice, set S is not defined explicitely and the induction proof proceeds like follows:

Proof of $\forall n \in \mathbb{N}\ P(n)$ by induction: (*)

1. (Induction Base) Prove that $P(0)$ is true
2. (Induction Step) Show $P(n) \Rightarrow P(n+1)$, i.e. suppose that $P(n)$ is true — called the induction hypothesis — and show that $P(n+1)$ is true.
3. (Conclusion) By steps 1. and 2. and the PMI, $P(n)$ is true for all $n \in \mathbb{N}$.

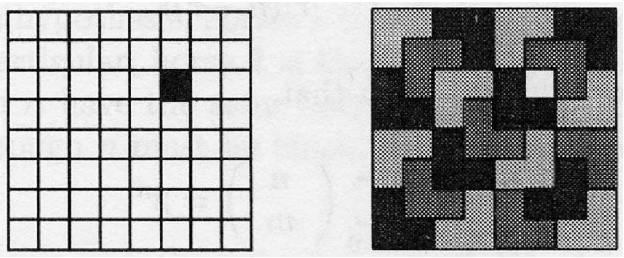
[(*) Note how we now make use of set notation to specify domains for quantified variables like so $\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}$...]

An Example from Geometry

This is an L-shaped tromino: 

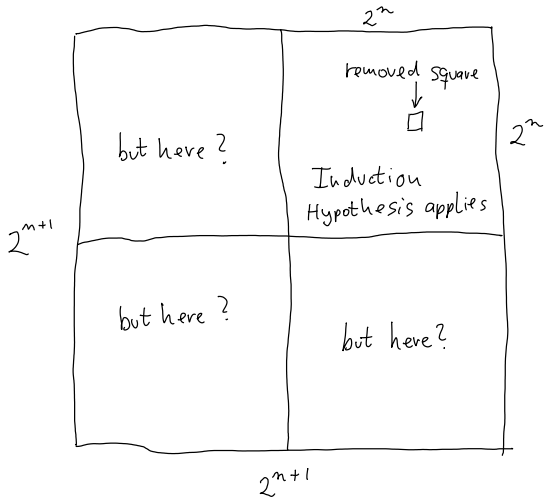
Question: Can chess boards of size 2^n by 2^n be tiled with L-shaped trominos for all $n \geq 1$, so that every square is covered by non-overlapping trominoes, except for one square that has been removed?

8 by 8 case and tiling:



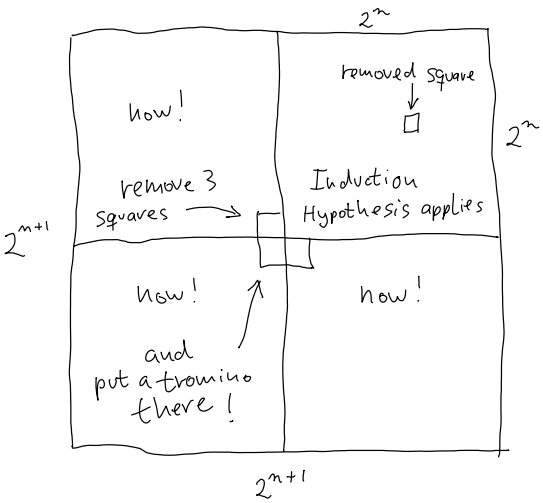
We think the answer is yes and try to prove this claim by induction. The induction base $n = 0$ (1 by 1 board with one removed square) is easy: the tiling consists of 0 trominoes.

Induction step: suppose all 2^n by 2^n boards with one removed square can be tiled. Show, that then also all 2^{n+1} by 2^{n+1} boards with one removed square can be tiled. We try to tile quadrants separately.



This doesn't seem to work because only one of the four quadrants has one square removed, and so the induction hypothesis does not apply to the other three ... but

we could remove the squares in the other three quadrants that are closest to the center. Then the induction hypothesis applies to these quadrants as well, i.e. we can tile them. What's left is to tile the 3 squares in the middle — by putting one tromino down — to complete the tiling of the 2^{n+1} by 2^{n+1} chess board.



So the induction step works, and therefore, by applying the PMI, the claim is true for all n.

Lecture 9 Other Forms of Mathematical Induction

Some statements are not true for all natural numbers, but they are true for all $n \geq k$ where k is a fixed natural number. It is not hard to prove that the following variation of the PMI holds:

Generalized Principle of Mathematical Induction

Let $k \in \mathbb{N}$. If $S \subseteq \mathbb{N}$ with the following two properties:

1. $k \in S$
2. for all $n \in \mathbb{N}$ with $n \geq k$, if $n \in S$, then $n+1 \in S$,

then S contains all natural numbers greater or equal to k.

Moreover, showing $P(n) \Rightarrow P(n+1)$ in the induction step may be a difficult task, when there is no apparent connection between the statements for n and $n+1$. However, the statement for $n+1$ may be related to statements for $k < n$. A generalization of the PMI suitable for such cases is called **complete** or **strong** induction.

The Principle of Complete Induction (PCI)

Suppose $S \subseteq \mathbb{N}$ has these properties:
1. $0 \in S$
2. $\{0, 1, \ldots, n\} \subseteq S \Rightarrow n+1 \in S$,

then $S = \mathbb{N}$.

It can be proved that PCI is equivalent to PMI, and as such is a valid tool to prove $S = \mathbb{N}$.

Example:

Theorem: Every natural number > 1 is a prime or a product of primes. E.g.: $4 = 2{\cdot}2,\ 6 = 2{\cdot}3,\ 30 = 2{\cdot}3{\cdot}5$

Recall: $n \in \mathbb{N}$ is a prime iff $n > 1$ and n is only divisible by 1 and n.

Proof by using the PCI.

We have to show $\forall n \in \mathbb{N}\ P(n)$, where $P(n)$ says

$(n \leq 1) \vee (n \text{ is prime}) \vee (n \text{ can be factored into primes})$

Induction Base: $n = 0$ and $n = 1$

Both $P(0)$ and $P(1)$ are true, because $n \leq 1$ in these cases.

Induction Step:

Suppose $n \geq 1$ and $P(k)$ holds for all $k \leq n$. We want to show that $P(n+1)$ then also holds.

Case 1: If $n+1$ is prime, then $P(n+1)$ holds trivially.

Case 2: If $n+1$ is not prime, then we can write it as product

$$n + 1 = a \cdot b$$

with $2 \leq a \leq n$ and $2 \leq b \leq n$, because $n+1$ is divisible by a number between 2 and n, inclusive. Therefore, we can apply the induction hypothesis to a and b because they are $\leq n$:

a is a prime, or can be factored into primes, and

b is a prime, or can be factored into primes.

Thus, $n + 1 = a \cdot b$ can be factored into primes.

So, $P(n+1)$ is true in both cases. □

More Induction Examples

Claim: $\forall n \in \mathbb{N}: \ \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Examples $1 = 2^1 - 1$ $\quad 1 + 2 = 3 = 2^2 - 1$

$$1 + 2 + 4 = 7 = 2^3 - 1$$

Proof: By induction on n

Induction Base $n = 0$

We check $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^1 - 1$. OK

Induction Step $n \rightsquigarrow n+1$

Assume claim holds for n, i.e. $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

This is called the induction hypothesis

Using this, we want to show that the claim also holds for $n+1$, i.e. $\sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1$

(replaced all occurrences of n by $n+1$)

Split up the new sum (sum up to n + last element):

$$\sum_{i=0}^{n+1} 2^i = [\sum_{i=0}^{n} 2^i] + 2^{n+1}$$

By the induction hypothesis we know the value of the sum and we can replace it by that value:

$$= [2^{n+1} - 1] + 2^{n+1}$$
$$= 2^{n+2} - 1$$

which is the result we wanted to prove. So, by the PMI the claim is true. □

Claim: $\sqrt{2}$ is irrational, i.e. it cannot be represented by $\frac{p}{q}$, where p, q are natural numbers > 0 (denoted $\mathbb{N}_+$).

Proof: We rephrase the claim and prove the following statement by induction on n:

$$\forall n \in \mathbb{N}_+ \; \forall b \in \mathbb{N}_+ : \; \sqrt{2} \neq \frac{n}{b}$$

Induction Base $n = 1$

$\frac{1}{b} \leq 1 < \sqrt{2}$ for all $b \in \mathbb{N}_+$. So, the claim holds for $n = 1$.

Induction Step $\leq n \rightsquigarrow n + 1$

Assume the claim holds for all $k \leq n$, i.e.

$$\forall k \leq n \; \forall b \in \mathbb{N}_+ : \; \sqrt{2} \neq \frac{k}{b}$$

We want to show:

$$\forall b \in \mathbb{N}_+ : \; \sqrt{2} \neq \frac{n+1}{b}$$

The proof is by contradiction:

Assume the opposite, i.e. $\exists b \in \mathbb{N}_+ : \; \sqrt{2} = \frac{n+1}{b}$

Take such a b and square the equality:

$$2 = \frac{(n+1)^2}{b^2}$$
$$\Rightarrow \quad 2b^2 = (n+1)^2$$

This means $(n+1)^2$ is even, and therefore $n+1$, say $n + 1 = 2t$:

$$\Rightarrow \quad 2b^2 = (2t)^2 = 4t^2$$
$$\Rightarrow \quad b^2 = 2t^2$$

This means b^2 is even, and therefore b, say $b = 2s$.

Coming back to the original assumption:

$$\sqrt{2} = \frac{n+1}{b} = \frac{2t}{2s} = \frac{t}{s}$$

But $t = \frac{n+1}{2} \leq n$ for $n \geq 1$ and therefore, the statement in the previous line contradicts the induction hypothesis which stated:

$$\forall k \leq n \; \forall b \in \mathbb{N}_+ : \; \sqrt{2} \neq \frac{k}{b}$$

Thus, our assumption was wrong, proving $\forall b \in \mathbb{N}_+ : \; \sqrt{2} \neq \frac{n+1}{b}$ and — with the PCI — the claim. □

Claim: $\forall n \in \mathbb{N} : \; n < 2^n$

Check small cases:

$$0 < 1, \quad 1 < 2, \quad 2 < 4, \quad 3 < 8, \quad 4 < 16$$

Proof: By induction on n

Induction Base $n = 0$

$0 < 2^0 = 1$. OK.

Induction Step $n \rightsquigarrow n + 1$

Suppose the induction hypothesis $n < 2^n$ holds for an $n \geq 0$. Using this, we want to show

$$n + 1 < 2^{n+1}$$

By the induction hypothesis and adding 1 on both sides which maintains the $<$ relation:

$$n + 1 < 2^n + 1$$

Because $n \geq 0$ we know $1 \leq 2^n$. Therefore

$$n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$$

which is what we wanted to show. With the PMI, the claim is therefore true for all n. □

Lecture 10

Preview: Proving Loop Correctness

Principles of Counting

Lecture 11 This section introduces some of the basic techniques for counting the number of elements in finite sets.

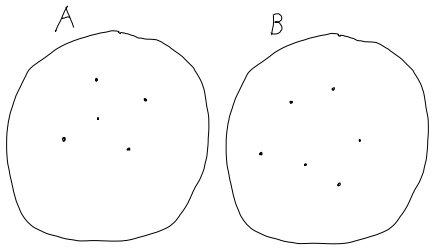
Definition: We call a set A **finite** iff A has n elements for some $n \in \mathbb{N}$. The **size** or **cardinality** of a finite set A is the number of elements it contains. This number is denoted by $|A|$.

Examples: $|\emptyset| = 0,\ |\{2,3,4\}| = 3$

Theorem (Sum Rule): If A and B are disjoint finite sets then

$$|A \cup B| = |A| + |B|$$

($\cup$ requires the sets to be unified to be disjoint)



Example: For $A = \{1,2\}$ and $B = \{3,4,5\}$, $|A \cup B| = |\{1,2,3,4,5\}| = |A| + |B| = 2 + 3 = 5$

Proof: We prove: for all finite sets A, B $|A \cup B| = |A| + |B|$ by induction on $n = |B|$, i.e. predicate $P(n)$ for which we want to prove $\forall n \in \mathbb{N}\ P(n)$ states

"forall finite disjoint sets A, B with $|B| = n$, $|A \cup B| = |A| + |B|$"

Induction Base: $n = 0, 1$

If B is empty, $A \cup B = A$ and therefore $|A \cup B| = |A| = |A| + 0 = |A| + |B|$

If B contains one element that is not element of A then $A \cup B$ contains one element more than A, i.e. $|A \cup B| = |A| + |B|$.

Induction Step: $n \rightsquigarrow n+1$

Assume that $|A \cup C| = |A| + |C|$ holds for all finite sets A and C with $|C| = n \geq 1$.

Consider set B with $n+1$ elements and $A \cap B = \emptyset$. Pick an element x of B and set $C := B - \{x\}$. Because C has n elements, by the induction hypothesis we know

$$|A \cup C| = |A| + |C|$$

x is neither an element of A nor C and $B = C \cup \{x\}$. Therefore, by the base case ($n = 1$) and the induction hypothesis:

$|A \cup B| = |(A \cup C) \cup \{x\}| = |A| + |C| + 1 = |A| + |B|$

Thus, the claim holds for all n. □

The Sum Rule can be extended to any finite number of pairwise disjoint sets:

Theorem (Generalized Sum Rule): For pairwise disjoint sets $A_1, \ldots, A_n$, the following holds:

$$|\dot{\bigcup_{i=1}^{n}} A_i| = \sum_{i=1}^{n} |A_i|$$

[The $\dot{\bigcup}$ operator unifies all sets for $i = 1 \ldots n$ and the dot indicates that disjoint sets are being unified]

Proof: By induction on n — the number of sets.

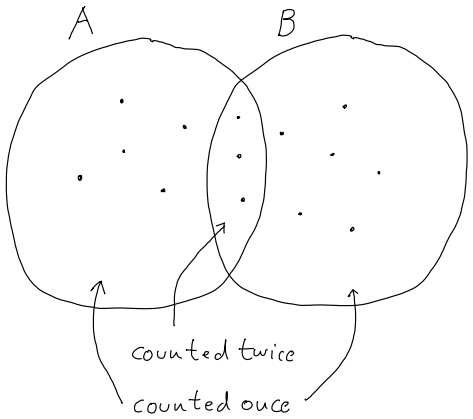
1. If $n = 1$, then $|\dot{\bigcup}_{i=1}^{1} A_i| = |A_1| = \sum_{i=1}^{1} |A_i|$
2. Suppose that $|\dot{\bigcup}_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$ holds. Because $\dot{\bigcup}_{i=1}^{n} A_i$ and A_{n+1} are disjoint, we can apply the Sum Rule and the induction hypothesis:

$$|\dot{\bigcup_{i=1}^{n+1}} A_i| = |(\dot{\bigcup_{i=1}^{n}} A_i) \cup A_{n+1}| = |\dot{\bigcup_{i=1}^{n}} A_i| + |A_{n+1}|$$

$$= (\sum_{i=1}^{n} |A_i|) + |A_{n+1}|. \quad \text{Thus, } |\dot{\bigcup_{i=1}^{n+1}} A_i| = \sum_{i=1}^{n+1} |A_i|$$

□

How to compute $|A \cup B|$ in case A and B are not disjoint?



By simply adding $|A|$ and $|B|$ we overcount $|A \cup B|$ because elements in $A \cap B$ are counted twice. The following theorem corrects this error:

Theorem: For finite sets A and B

1. $|A \cup B| = |A| + |B| - |A \cap B|$
2. $|A \cap B| = |A| + |B| - |A \cup B|$ (follows from 1.)

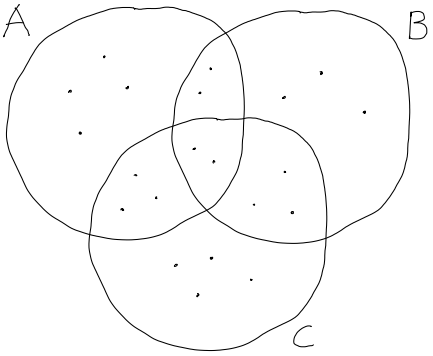
Example: $A = \{1, 2, 3\},\ B = \{3, 4, 5, 6\}$

$|A \cup B| = |A| + |B| - |A \cap B| = 3 + 4 - |\{3\}| = 6$

This theorem can be generalized to more than two sets by the **Principle of Inclusion and Exclusion**.

Example for 3 sets:

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & -|A \cap B| - |A \cap C| - |B \cap C| \\ & +|A \cap B \cap C| \end{aligned}$$

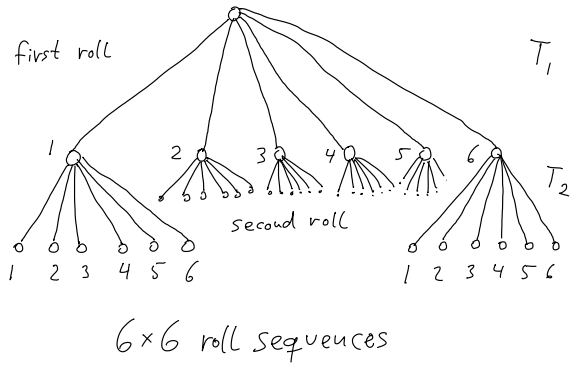


Elements in double intersections are counted twice

Elements in the triple intersection are counted thrice

Theorem (Product Rule): If two independent tasks T_1 and T_2 are to be performed, and T_1 can be executed in c_1 ways, and T_2 can be performed in c_2 ways, then the two tasks can be executed in sequence in $c_1 \cdot c_2$ ways.

Example: Consider rolling two regular dice in turn. How many outcomes are there? $6 \cdot 6 = 36$ — 6 for the first die, and for the outcomes 6 for the second die. Note, roll $1\ 3$ is different from roll $3\ 1$.



6×6 roll sequences

Like the Sum Rule, the Product Rule can be extended to n tasks by induction:

Theorem (Generalized Product Rule): If n independent tasks T_i are to be performed and the number of ways T_i can be performed is c_i, then the number of ways to perform all tasks in sequence is $c_1 \cdot c_2 \cdots c_n$

One of the many applications of this rule is to compute the cardinality of power sets.

Theorem: For finite sets A with n elements, $|\mathcal{P}(A)| = 2^n$.

Proof: We need to count the subsets of A, which has n elements. Each subset is characterized by the elements we select from A. For each of the n elements we define task T_i to be either selecting element i or not, i.e. $c_i = 2$. The tasks are independent of each other. So, according to the generalized product rule, the total number of choice sequences is $\prod_{i=1}^{n} c_i = \prod_{i=1}^{n} 2 = 2^n$. □

Definition: A **permutation** of a set is an arrangement of the elements of the set in a specific order.

How many permutations exist for sets with n elements?

Let's count permutations for small n:

$n = 1 : \{1\} : (1)$ **1**

$n = 2 : \{1, 2\} : (12 \;\; 21)$ **2**

$n = 3 : \{1, 2, 3\} : (123 \;\; 132 \;\; 213 \;\; 231 \;\; 312 \;\; 321)$ **6**

$n = 4 : \{1, 2, 3, 4\} : (1234\; 1243 \;\ldots\; 4312 \;\; 4321)$ **24**

What is the pattern? $2/1 = 2 \;\; 6/2 = 3 \;\; 24/6 = 4$

$$1 = 1! \quad 2 = 2! \quad 6 = 3! \quad 24 = 4!$$

Recall: $n! = n(n-1)(n-2)\cdots 2 \cdot 1$

Why would there be $n!$ different permutations for sets with n elements?

The intuition is this: for the first element in the sequence we have n choices. Then there are $n-1$ elements left to choose from, so we have $n-1$ choices for the second element, and so on. All choices are independent of each other. So, by the generalized product rule the total number of possibilities is

$$n(n-1)(n-2)\cdots 2 \cdot 1 = n!$$

Lecture 12 This proves the following

Theorem: The number of permutations of n objects is $n!$

A central question in many counting problems is how many subsets of a certain size exist.

Definition: The number of k-element subsets of sets with n elements is denoted $\binom{n}{k}$ and read "n choose k". The number $\binom{n}{k}$ is called a **binomial coefficient**.

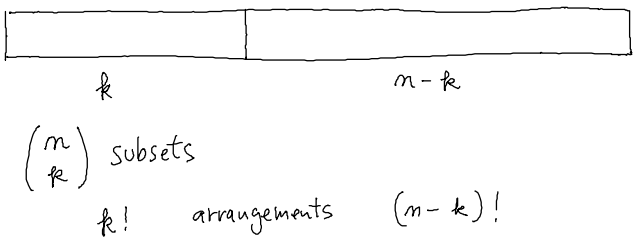
Example: What are the 2-element subsets of $\{1, 2, 3\}$?

$$\{1,2\} \;\; \{1,3\} \;\; \{2,3\}, \text{ thus } \binom{3}{2} = 3$$

For any n-element set there is only one subset of size n. Thus, $\binom{n}{n} = 1$ for every $n \in \mathbb{N}$. Likewise, there is only one subset of size 0, so $\binom{n}{0} = 1$ for all $n \in \mathbb{N}$.

Theorem: Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ such that $0 \le k \le n$. Then

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$



Proof: We count the number of ways to arrange n objects in two different ways. By an earlier theorem we know that this number is $n!$. The n objects may also be arranged by first selecting k objects ($\binom{n}{k}$ possibilities), arranging them ($k!$ choices), and then arranging the remaining $n-k$ objects ($(n-k)!$ choices). Thus, by the generalized product rule, the number of choices is

$$\binom{n}{k} k!(n-k)! = n!$$

Therefore, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ □

Examples

Using the formula we verify:

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$

$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n(n-1)!}{1 \cdot (n-1)!} = n$$

Number of 2-element subsets of n elements:

$$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n!}{2 \cdot (n-2)!} = \frac{n(n-1)}{2}$$

Number of 3-element subsets of n elements:

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6}$$

...

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n! \cdot 0!} = 1$$

Theorem: Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ with $0 \le k \le n$.

(a) $\binom{n}{k} = \binom{n}{n-k}$

(b) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for $n, k \ge 1$

(c) (Binomial Theorem)

For $a, b \in \mathbb{R}$, $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$

(d) $\sum_{i=0}^{n} \binom{n}{i} = 2^n$

Proof:

(a): Using the formula we just derived we note:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!}$$
$$= \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}$$

This means, the number of ways we can select k objects out of n is the same as the number of ways selecting $n-k$ elements. In hindsight this seems obvious, be-

cause choosing k objects corresponds to choosing $n-k$ objects to exclude.

(b): How can we split up the number of ways to select k items out of n?

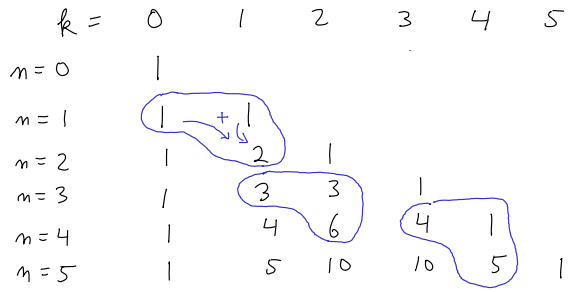
One option is to distinguish the case in which the first item is among the k selected items from the case where it isn't. Both cases are clearly disjoint, and together form all the choices we have.

Thus,

$$\binom{n}{k} = \underbrace{\binom{n-1}{k-1}}_{\text{first element selected}} + \underbrace{\binom{n-1}{k}}_{\text{not selected}}$$

In the first case, there are $k-1$ items yet to be selected out of $n-1$ items, and in the second case we need to select k out of $n-1$.

Application: Part (b) can be used to construct Pascal's triangle, which contains the binomial coefficients $\binom{n}{k}$, by just using additions:



$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad k, n \ge 1$$

To compute a new row we start with $1 = \binom{n}{0}$ and then add the numbers located on top and to the left in the previous row. Rows are finished by $1 = \binom{n}{n}$.

Lecture 13

(c): Prove: For $a, b \in \mathbb{R}$, $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$

Examples

$(a+b)^1 = \boxed{1}a^1b^0 + \boxed{1}a^0b^1 = \boxed{1}a + \boxed{1}b$

$(a+b)^2 = \boxed{1}a^2 + \boxed{2}ab + \boxed{1}b^2$

$(a+b)^3 = \boxed{1}a^3 + \boxed{3}a^2b + \boxed{3}ab^2 + \boxed{1}b^3$

$(a+b)^4 = \boxed{1}a^4 + \boxed{4}a^3b + \boxed{6}a^2b^2 + \boxed{4}ab^3 + \boxed{1}b^4$

Observation: the coefficients are $\binom{n}{k}$ and the powers of a and b always add up to n.

Example: $(a+b)(a+b) = aa + ab + ba + bb$

In general

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ times}},$$

each term of the expansion of $(a+b)^n$ — in which we multiply out all factors — contains one term from each of the n factors $(a+b)$.

Thus, each term of $(a+b)^n$ contains a total of n a's and b's, i.e. for some i it contains

$$a^{n-i}b^i$$

For a given i, the term $a^{n-i}b^i$ arises exactly $\binom{n}{i}$ times, because this is the number of ways to choose i b's out of the n $(a+b)$ terms. Therefore, each $a^{n-i}b^i$ appears $\binom{n}{i}$ times.

(d): We use part (c). Choose $a = b = 1$, then:

$$(1+1)^n = 2^n = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^i = \sum_{i=0}^{n} \binom{n}{i}$$

This is an alternate proof of $|\mathcal{P}(A)| = 2^{|A|}$, because the sum counts all subsets arranged by increasing size.

□