Set Theory / Counting and Probability

Properties of Sets, Proofs & Disproofs / Introduction

Lecture Notes #10

Peter Blomgren
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
blomgren@terminus.SDSU.EDU
http://terminus.SDSU.EDU

$Id: lecture.tex,v 1.8 2006/11/02 19:59:22 blomgren Exp $

Properties of Sets

We continue our study of sets...

In particular we look at element based methods for proving relations between sets.

Also, we will see some examples of algebraic techniques (methods that use already known properties of sets to transform expressions) that involve set relations.

Our basic building blocks are the ***union***, ***intersection***, ***difference*** and ***complement*** of sets.

Note that these operations take precedence (are executed before) over set inclusion, *i.e.*

$$A \cap B \subseteq C \quad \Leftrightarrow \quad (A \cap B) \subseteq C$$

Some Subset Relations

Theorem: —

[1] **Inclusion of Intersection:** For all sets A and B,

$$(a)\ A \cap B \subseteq A, \quad \text{and} \quad (b)\ A \cap B \subseteq B$$

[2] **Inclusion in Union:** For all sets A and B,

$$(a)\ A \subseteq A \cup B, \quad \text{and} \quad (b)\ B \subseteq A \cup B$$

[3] **Transitive Property of Subsets:** For all sets A, B, and C,

$$\text{if } A \subseteq B \quad \text{and} \quad B \subseteq C, \quad \text{then} \quad A \subseteq C.$$

How Do We Prove Such Relations?

Element Argument: The basic method for proving that one set is a subset of another

To prove that a set (A) is a subset of another set (B):

(1) Let x be a particular, but arbitrarily chosen element of A.

(2) Show that x must necessarily be an element of B.

As always when we are trying to prove something, we state the assumptions, then use the definitions to express what the assumptions mean.

In particular, for set theoretical proofs, we use the ***procedural versions of the set definitions*** [next slide] to express the meaning of the assumptions.

Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose $x \in U$ and $y \in U$.

[1] $x \in X \cup Y \Leftrightarrow x \in X$ or $x \in Y$.

[2] $x \in X \cap Y \Leftrightarrow x \in X$ and $x \in Y$.

[3] $x \in X - Y \Leftrightarrow x \in X$ and $x \notin Y$.

[4] $x \in X^c \Leftrightarrow x \notin X$.

[5] $(x, y) \in X \times Y \Leftrightarrow x \in X$ and $y \in Y$.

With these tools handy, we can prove the statements on slide 3.

Proofs of $A \subseteq A \cup B$ and $A \cap B \subseteq A$

Statement: $A \subseteq A \cup B$.

Proof:

Statement: $A \cap B \subseteq A$.

Proof:

Here we have used

Generalization (Disjunctive Addition)
p
$\therefore \quad p \vee q$

Specialization (Conjunctive Simplification)
$p \wedge q$
$\therefore \quad p$

Proofs of $A \subseteq A \cup B$ and $A \cap B \subseteq A$

Statement: $A \subseteq A \cup B$.

Proof: Suppose A and B are sets. Let $x \in A$. Now the statement $(x \in A) \vee (x \in B)$ is certainly true, hence by the definition of the union $A \cup B$, we must have $x \in (A \cup B)$. $\square$

Statement: $A \cap B \subseteq A$.

Proof:

Here we have used

Generalization (Disjunctive Addition)
p
$\therefore \quad p \vee q$

Specialization (Conjunctive Simplification)
$p \wedge q$
$\therefore \quad p$

Proofs of $A \subseteq A \cup B$ and $A \cap B \subseteq A$

Statement: $A \subseteq A \cup B$.

Proof: Suppose A and B are sets. Let $x \in A$. Now the statement $(x \in A) \vee (x \in B)$ is certainly true, hence by the definition of the union $A \cup B$, we must have $x \in (A \cup B)$. $\square$

Statement: $A \cap B \subseteq A$.

Proof: Suppose A and B are sets, and $x \in (A \cap B)$. By the definition of the intersection $(x \in A) \wedge (x \in B)$. In particular $x \in A$. $\square$

Here we have used

Generalization (Disjunctive Addition)
p
$\therefore \quad p \vee q$

Specialization (Conjunctive Simplification)
$p \wedge q$
$\therefore \quad p$

Let A, B, and C be subsets of a universal set U. The following twelve identities are true:

1. **Commutative laws:** For all sets A and B,

$$A \cap B = B \cap A, \text{ and } A \cup B = B \cup A.$$

2. **Associate laws:** For all sets A, B and C,

$$(A \cap B) \cap C = A \cap (B \cap C), \text{ and } (A \cup B) \cup C = A \cup (B \cup C).$$

3. **Distributive laws:** For all sets A, B and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \text{ and } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

4. **Identity laws:** (U acts as an identity for $\cap$, and $\emptyset$ acts as a "zero" for $\cup$): For all sets A,

$$A \cup \emptyset = A, \quad \text{and} \quad A \cap U = A.$$

5. **Complement laws:** For all sets A,

$$A \cup A^c = U, \quad \text{and} \quad A \cap A^c = \emptyset$$

6. **Double complement law:** For all sets A,

$$(A^c)^c = A.$$

7. **Idempotent laws:** For all sets A,

$$A \cap A = A, \quad \text{and} \quad A \cup A = A.$$

8. **Universal bounds laws:** For all sets A,

$$A \cup U = U, \quad \text{and} \quad A \cap \emptyset = \emptyset$$

9. **De Morgan's laws:** For all sets A and B,

$$(A \cup B)^c = A^c \cap B^c, \quad \text{and} \quad (A \cap B)^c = A^c \cup B^c.$$

10. **Absorption laws:** For all sets A and B

$$A \cup (A \cap B) = A, \quad \text{and} \quad A \cap (A \cup B) = A.$$

11. **Complements of U and $\emptyset$:**

$$U^c = \emptyset, \quad \text{and} \quad \emptyset^c = U$$

12. **Set difference law:** For all sets A and B,

$$A - B = A \cap B^c.$$

Proving the Set Identities

The proofs of the set identities are quite straight-forward. Use the procedural definitions (slide 5) and the following rule:

Basic Method for Proving that Sets are Equal

Let X and Y be subsets of a universal set U. To prove that $X = Y$:

[1] Prove that $X \subseteq Y$.

[2] Prove that $Y \subseteq X$.

Note: After using the definitions, and introduction of predicates such as $P(x) = (x \in A)$, and noting that $(x \in A \cup B) \equiv ((x \in A) \vee (x \in B))$ all the proofs follow directly from the laws of logic.

Proof: Suppose A and B are sets.

[$\mathbf{A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)}$] — Suppose $x \in A \cup (B \cap C)$.

By definition of union $x \in A$ or $x \in (B \cap C)$.

Proof: Suppose A and B are sets.

[$\mathbf{A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)}$] — Suppose $x \in A \cup (B \cap C)$.

By definition of union $x \in A$ or $x \in (B \cap C)$.

Case $x \in A$: Since $x \in A$, $x \in A \cup B$ by definition of union and also $x \in A \cup C$ by definition of union. Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

Proof: Suppose A and B are sets.

[$\mathbf{A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)}$] — Suppose $x \in A \cup (B \cap C)$.

By definition of union $x \in A$ or $x \in (B \cap C)$.

Case $x \in A$: Since $x \in A$, $x \in A \cup B$ by definition of union and also $x \in A \cup C$ by definition of union. Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

Case $x \in (B \cap C)$: Since $x \in (B \cap C)$, $x \in B$ and $x \in C$ by definition of intersection. Since $x \in B$, $x \in A \cup B$ by definition of union; also since $x \in C$, $x \in A \cup C$ by definition of union Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

In both cases the containment $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ is true.

[continued]

Proof: Suppose A and B are sets.

[$(\mathbf{A} \cup \mathbf{B}) \cap (\mathbf{A} \cup \mathbf{C}) \subseteq \mathbf{A} \cup (\mathbf{B} \cap \mathbf{C})$] — Suppose $x \in (A \cup B) \cap (A \cup C)$. By definition of intersection $x \in (A \cup B)$ and $x \in (A \cup C)$.

Proof: Suppose A and B are sets.

[$(\mathbf{A} \cup \mathbf{B}) \cap (\mathbf{A} \cup \mathbf{C}) \subseteq \mathbf{A} \cup (\mathbf{B} \cap \mathbf{C})$] — Suppose $x \in (A \cup B) \cap (A \cup C)$. By definition of intersection $x \in (A \cup B)$ and $x \in (A \cup C)$.

Case $x \in A$: We can immediately conclude that $x \in A \cup (B \cap C)$ by definition of union.

Proof: Suppose A and B are sets.

[$(\mathbf{A \cup B}) \cap (\mathbf{A \cup C}) \subseteq \mathbf{A \cup (B \cap C)}$] — Suppose $x \in (A \cup B) \cap (A \cup C)$. By definition of intersection $x \in (A \cup B)$ and $x \in (A \cup C)$.

Case $x \in A$: We can immediately conclude that $x \in A \cup (B \cap C)$ by definition of union.

Case $x \notin A$: Since $x \notin A$, we must have $x \in B$ and $x \in C$ by definition of union. By the definition of intersection $x \in (B \cap C)$, and by the definition of union $x \in A \cup (B \cap C)$.

In both cases the containment $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ is true.

Since both subset relations have been proved, it follows by definition of set equality that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\square$

Proof: $(A \cup B)^c = A^c \cap B^c$ Alternative Approach

If we feel more comfortable arguing a proof from the laws of logic, be can convert to an equivalent problem...

Proof: Suppose A and B are subsets of a universal set U. Define the predicates $P(x)$ and $Q(x)$:

$$P(x) = \text{“}x \in A\text{”}, \quad Q(x) = \text{“}x \in B\text{”}.$$

Our two sets are

$$\begin{aligned} (A \cup B)^c &= \{x \in U \mid \sim (P(x) \vee Q(x))\} \\ (A^c \cap B^c) &= \{x \in U \mid (\sim P(x)) \wedge (\sim Q(x))\} \end{aligned}$$

Since

$$\sim (P(x) \vee Q(x)) \equiv (\sim P(x)) \wedge (\sim Q(x)) \quad \text{[De Morgan's laws of logic]}$$

the sets must be equal. □

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

Proof: [by contradiction]

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

Proof: [by contradiction] Suppose the proposition is false.

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

Proof: [by contradiction] Suppose the proposition is false. Then there exists two sets A and B such that $(A - B) \cap B \neq \emptyset$ [$(A - B)$ and B not disjoint]

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

Proof: [by contradiction] Suppose the proposition is false. Then there exists two sets A and B such that $(A - B) \cap B \neq \emptyset$ [$(A - B)$ and B not disjoint] By the definition of intersection there is an element $x \in (A - B)$ and $x \in B$.

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

Proof: [by contradiction] Suppose the proposition is false. Then there exists two sets A and B such that $(A - B) \cap B \neq \emptyset$ [$(A - B)$ and B not disjoint] By the definition of intersection there is an element $x \in (A - B)$ and $x \in B$. By the definition of set difference $x \in A$ and $x \notin B$.

The Empty Set — Proof Technique

Element Method for Proving a Set Equals the Empty Set

To prove that a set S equals to the empty set $\emptyset$, prove that S has no elements. — To achieve this, suppose S has an element and derive a contradiction.

Proposition: Given any two sets A and B, $(A-B)$ and B are disjoint.

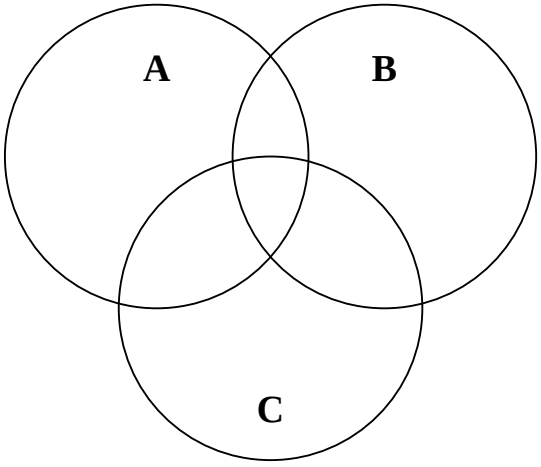
Proof: [by contradiction] Suppose the proposition is false. Then there exists two sets A and B such that $(A - B) \cap B \neq \emptyset$ [$(A - B)$ and B not disjoint] By the definition of intersection there is an element $x \in (A - B)$ and $x \in B$. By the definition of set difference $x \in A$ and $x \notin B$. Hence we have shown that $x \in B$ and $x \notin B$, which is a contradiction. □

[The supposition that there exists sets A and B such that $(A - B)$ and B are not disjoint is false, and hence the proposition is true.]

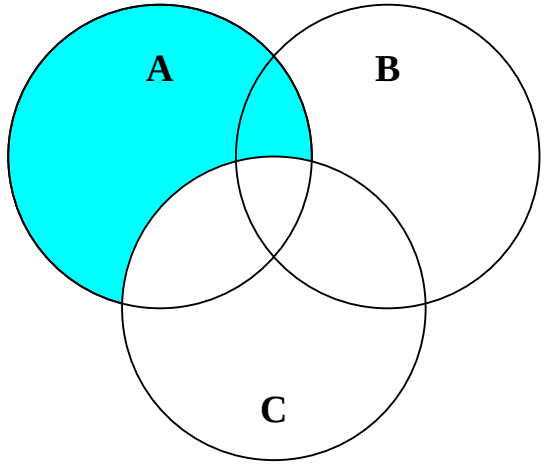
Showing the Falsity of an Alleged Set Property

False statement: For all sets A, B and C

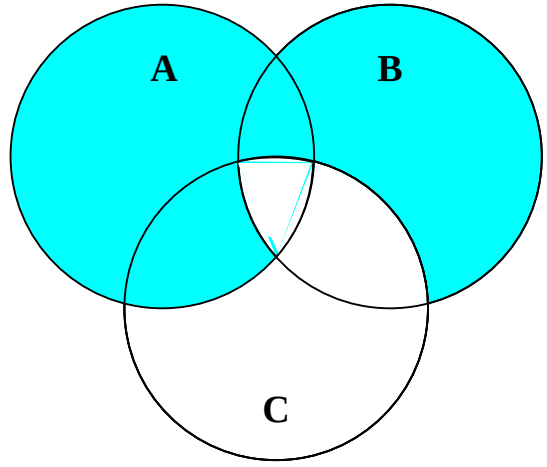
$$(A - B) \cup (B - C) = A - C$$



The sets A, B, and C.



$A - C$



$(A - B) \cup (B - C)$

Counterexample:

$$A = \{a, b\}, \quad B = \{b, c\}, \quad C = \{a, d\}$$

$$A - C = \{b\}, \quad (A - B) \cup (B - C) = \{a\} \cup \{b, c\} = \{a, b, c\}$$

How to Approach Set-Theory Problems

The Problem: "Prove or disprove some statement about sets!"

The Optimist: Start trying to prove the statement! Think about *what you need to show* and, of course, *how to show it*.

The Pessimist: Think about conditions that must be fulfilled to construct a counterexample.

If the statement is ***true***, the optimist succeeds, and the pessimist ends up with incompatible conditions (possibly a form of contradiction, or no elements satisfying the conditions)... The pessimist must switch gears.

If the statement is ***false***, the pessimist succeeds in finding a counterexample, and the optimist ends up with a step in the proof which is clearly not true... and s/he must switch gears.

Theorem: $\forall n \in \mathbb{Z}$, $n \geq 0$, if a set S has n elements, then $\mathcal{P}(S)$ has 2^n elements.

The proof is based on mathematical induction [back to haunt us again!] and uses the following observations... Suppose S is a set and $z \in S$.

1. The subsets of S can be split into two categories: those that contain z, and those who do not contain z.

2. The subsets of S that do not contain z are the same as the subsets of $S - \{z\}$.

3. The subsets of S that do not contain z can be matched up one-to-one with the subsets that contain z by matching each subset $S_i \subseteq S$ which does not contain z with the subset $S_i \cup \{z\}$ that contains z. Thus ***there are as many subsets of*** S ***that contain*** z ***as there are subsets that do not contain*** z***.*** .

Consider the example $S = \{1, 2, 3\}$, $z = 3$

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

Subsets of S that do not contain 3		Subsets of S that contain 3
$\emptyset$	$\leftrightarrow$	$\{3\}$
$\{1\}$	$\leftrightarrow$	$\{1, 3\}$
$\{2\}$	$\leftrightarrow$	$\{2, 3\}$
$\{1, 2\}$	$\leftrightarrow$	$\{1, 2, 3\}$

Proof: Let $P(x)$ be the property "Any set S with n elements has 2^n subsets." (The power set $\mathcal{P}(S)$ has 2^n elements.)

True for $n = 0$:

Proof: Let $P(x)$ be the property "Any set S with n elements has 2^n subsets." (The power set $\mathcal{P}(S)$ has 2^n elements.)

True for $n = 0$: The only set with 0 elements is the empty set. The only subset of the empty set is itself. Thus a set with 0 elements has 1 subset. The property $\mathbf{P(0)}$ is true.

Proof: Let $P(x)$ be the property "Any set S with n elements has 2^n subsets." (The power set $\mathcal{P}(S)$ has 2^n elements.)

True for $n = 0$: The only set with 0 elements is the empty set. The only subset of the empty set is itself. Thus a set with 0 elements has 1 subset. The property $\mathbf{P(0)}$ is true.

$\mathbf{P(k) \Rightarrow P(k+1)}$: Let $k \geq 0$ and suppose that any set with k elements has 2^k subsets. [The Inductive Hypothesis] [We must show that any set with $k+1$ elements has 2^{k+1} subsets.]

Proof: Let $P(x)$ be the property "Any set S with n elements has 2^n subsets." (The power set $\mathcal{P}(S)$ has 2^n elements.)

True for $n = 0$: The only set with 0 elements is the empty set. The only subset of the empty set is itself. Thus a set with 0 elements has 1 subset. The property $\mathbf{P(0)}$ is true.

$\mathbf{P(k) \Rightarrow P(k+1)}$: Let $k \geq 0$ and suppose that any set with k elements has 2^k subsets. [The Inductive Hypothesis] [We must show that any set with $k+1$ elements has 2^{k+1} subsets.] Let S be a set with $k+1$ elements, and $z \in S$. Any subset of S either contains z or it does not.

Proof: Let $P(x)$ be the property "Any set S with n elements has 2^n subsets." (The power set $\mathcal{P}(S)$ has 2^n elements.)

True for $n = 0$: The only set with 0 elements is the empty set. The only subset of the empty set is itself. Thus a set with 0 elements has 1 subset. The property $\mathbf{P(0)}$ is true.

$\mathbf{P(k) \Rightarrow P(k+1)}$: Let $k \geq 0$ and suppose that any set with k elements has 2^k subsets. [The Inductive Hypothesis] [We must show that any set with $k+1$ elements has 2^{k+1} subsets.] Let S be a set with $k+1$ elements, and $z \in S$. Any subset of S either contains z or it does not. Any subset A of S which does not contain z is a subset of $S - \{z\}$, further such a set can be matched up with $A \cup \{z\}$ that contains z. Consequently there are as many subsets of S than contain z as do not, and thus twice as many subsets of S as there are subsets of $S - \{z\}$. [continued...]

The set $S - \{z\}$ has k elements, thus by the inductive hypothesis ***the number of subsets of*** $S - \{z\}$ ***is*** 2^k.

Now it follows that

$$\#\text{subsets}(S) = 2 \cdot \#\text{subsets}(S - \{z\}) = 2 \cdot 2^k = 2^{k+1}. \square$$

[Since we have proved both the basis step $P(0)$ and the inductive step $P(k) \Rightarrow P(k+1)$, we conclude that the theorem is true.]

Theorem: ***Number of Elements of the Power Set*** —
$\forall n \in \mathbb{Z}$, $n \geq 0$, if a set S has n elements, then $\mathcal{P}(S)$ has 2^n elements.

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof:

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof: Suppose A and B are sets such that $A \subseteq B$. [**We must show** $\mathcal{P}(A) \subseteq \mathcal{P}(B)$]

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof: Suppose A and B are sets such that $A \subseteq B$. [**We must show** $\mathcal{P}(A) \subseteq \mathcal{P}(B)$]

Let $X \in \mathcal{P}(A)$.

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof: Suppose A and B are sets such that $A \subseteq B$. [**We must show** $\mathcal{P}(A) \subseteq \mathcal{P}(B)$]

Let $X \in \mathcal{P}(A)$. Since $X \in \mathcal{P}(A)$, $X \subseteq A$ by the definition of the power set.

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof: Suppose A and B are sets such that $A \subseteq B$. [**We must show** $\mathcal{P}(A) \subseteq \mathcal{P}(B)$]

Let $X \in \mathcal{P}(A)$. Since $X \in \mathcal{P}(A)$, $X \subseteq A$ by the definition of the power set. Further we know that $A \subseteq B$, hence

$$X \subseteq A \subseteq B$$

and $X \subseteq B$ by the transitive property for subset inclusion.

Power Sets — A Theorem

Theorem: $\forall$ sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof: Suppose A and B are sets such that $A \subseteq B$. [**We must show** $\mathcal{P}(A) \subseteq \mathcal{P}(B)$]

Let $X \in \mathcal{P}(A)$. Since $X \in \mathcal{P}(A)$, $X \subseteq A$ by the definition of the power set. Further we know that $A \subseteq B$, hence

$$X \subseteq A \subseteq B$$

and $X \subseteq B$ by the transitive property for subset inclusion. By the definition of the power set $X \in \mathcal{P}(B)$.

Thus $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. $\square$

Deriving New Set Properties — Algebraic Method

It is possible to derive new set properties from the ones we have established. The set identities we derived apply to all sets (they are universal statements), so we have plenty of room to play...

Example #1 — Relabeling We know that for all sets A, B, and C the distributive laws state

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

If we rename $A \to A_1$, $B \to A_2$, and $C \to A_3$, we get the relation

$$A_1 \cap (A_2 \cup A_3) = (A_1 \cap A_2) \cup (A_1 \cap A_3)$$

Which shows that the rule holds for any collection 3 three sets.

For any sets V, W, X, Y, and Z, can let $A_1 = (V \cap W)$, $A_2 = (X - Y)$, and $A_3 = (Z \cap W^c)$. We now get

$$(V \cap W) \cap ((X - Y) \cup (Z \cap W^c)) = ((V \cap W) \cap (X - Y)) \cup ((V \cap W) \cap (Z \cap W^c))$$

Algebraic Derivations of Set Properties

Example #2 Let A, B, and C be given. Then

$$\begin{aligned}
(A \cup B) - C &= (A \cup B) \cap C^c && \text{alternate representation} \\
&= C^c \cap (A \cup B) && \text{commutative law} \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{distributive law} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{commutative law} \\
&= (A - C) \cup (B - C) && \text{alternate representation}
\end{aligned}$$

This shows that for all sets A, B and C

$$\mathbf{(A \cup B) - C = (A - C) \cup (B - C)}$$

Algebraic Derivations of Set Properties

Example #3 Let A_1, A_2, A_3 and A_4 be given. Then

$$\begin{aligned}((A_1 \cup A_2) \cup A_3) \cup A_4 &= (A_1 \cup (A_2 \cup A_3)) \cup A_4 && \text{associative law} \\ &= A_1 \cup ((A_2 \cup A_3) \cup A_4) && \text{associative law} \\ &= A_1 \cup (A_2 \cup (A_3 \cup A_4)) && \text{associative law}\end{aligned}$$

This shows that for all sets A, B and C

$$((\mathbf{A_1} \cup \mathbf{A_2}) \cup \mathbf{A_3}) \cup \mathbf{A_4} = \mathbf{A_1} \cup (\mathbf{A_2} \cup (\mathbf{A_3} \cup \mathbf{A_4}))$$

The Empty Set — In an Algebraic Proof

Suppose A and B are sets, then $A - (A \cap B) = A - B$.

Proof:

$$
\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{Alternate representation} \\
&= A \cap (A^c \cup B^c) && \text{De Morgan's laws} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{Distributive law} \\
&= \emptyset \cup (A \cap B^c) && \text{Intersection with complement} \\
&= (A \cap B^c) \cup \emptyset && \text{Commutative law} \\
&= A \cap B^c && \text{Union with empty set} \\
&= A - B && \text{Alternate representation}
\end{aligned}
$$

Earlier we indicated the strong connection between set theory and logic — the concept of a **Boolean Algebra** formalizes this connection.

A **Boolean Algebra** is a set S together with two operations, usually denoted by $+$ and $\cdot$ such that $\forall a, b \in S$ both $(a + b) \in S$ and $(a \cdot b) \in S$ and the following axioms hold:

[Commutative Laws] $\forall a, b \in S$: $a + b = b + a$, $a \cdot b = b \cdot a$.

[Associative Laws] $\forall a, b, c \in S$: $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

[Distributive Laws] $\forall a, b, c \in S$: $a + (b \cdot c) = (a + b) \cdot (a + c)$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

[Identities] $\exists 0 \in S,\ 1 \in S$: $\forall a \in S$: $a + 0 = a$, $a \cdot 1 = a$.

[Complement / Negation] $\forall a \in S$, $\exists \overline{a} \in S$: $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$

So far, we have seen two Boolean algebras: statement forms in a finite number of variables (Logic), and Set Theory:

Boolean Algebra	$+$	$\cdot$	1	0	$\overline{}$
Statement forms / Logic	$\vee$	$\wedge$	t	c	$\sim$
Set Theory	$\cup$	$\cap$	U	$\emptyset$	^{c}

Notes:

For Logic, t is the tautology, c the contradiction.

For Set theory, ^{c} is the complement.

***Theorem:* Properties of Boolean Algebras — (Part 1/2)**

Let $\mathcal{B}$ be any Boolean Algebra.

1. ***Uniqueness of the Complement:*** $\forall a$ and $\forall x$ in $\mathcal{B}$, if $a + x = 1$, and $a \cdot x = 0$, then $x = \overline{a}$.
2. ***Uniqueness of*** 0 ***and*** 1***:*** If $\exists x \in \mathcal{B}$ such that $a + x = a$ $\forall a \in \mathcal{B}$, then $x = 0$, and if $\exists y \in \mathcal{B}$ such that $a \cdot y = a$ $\forall a \in \mathcal{B}$, then $y = 1$.
3. ***Double Complement:*** $\forall a \in \mathcal{B}$, $\overline{(\overline{a})} = a$.
4. ***Idempotent law:*** $\forall a \in \mathcal{B}$,

(a) $a + a = a$, and **(b)** $a \cdot a = a$.

***Theorem:* Properties of Boolean Algebras — (Part 2/2)**

Let $\mathcal{B}$ be any Boolean Algebra.

5. Universal Bound: $\forall a \in \mathcal{B}$,

(a) $a + 1 = 1$, and **(b)** $a \cdot 0 = 0$.

6. De Morgan's Laws: $\forall a, b \in \mathcal{B}$,

(a) $\overline{a + b} = \overline{a} \cdot \overline{b}$, and **(b)** $\overline{a \cdot b} = \overline{a} + \overline{b}$.

7. Absorption laws: $\forall a, b \in \mathcal{B}$,

(a) $(a + b) \cdot a = a$, and **(b)** $(a \cdot b) + a = a$.

8. Complements of 0 ***and*** 1***:***

(a) $\overline{0} = 1$, and **(b)** $\overline{1} = 0$.

Epp v3.0

Epp-5.2.1, Epp-5.2.5, Epp-5.2.17, Epp-5.2.37

Epp-5.3.20, Epp-5.3.39

Epp v2.0

Epp-5.2.1, Epp-5.2.5, Epp-5.2.24, Epp-5.2.26

Epp-5.3.45, —

A Quick Recap...

So far (in the realm of set theory) we have discussed the properties of the union, intersection, difference, and complements of sets.

We have combined these operations and discussed how to show that a set is a subset of some other set — by

(1) using element based methods,
(2) defining predicates and applying our knowledge from logic,
(3) algebraic manipulation of known set identities.

We will talk more about set theory later on in the class — when we talk about ***relations on sets.***

Counting and Probability

Counting is the key to many probabilistic problems, and to quite a few games... We start our discussion by tossing coins:

Assume we have two balanced (no cheating) coins, we repeatedly toss them and take note of how many heads we obtain:

The Book's Experiment			**Peter's Experiment**		
Event	Frequency	Relative Frequency	Event	Frequency	Relative Frequency
2 heads	11	22%	2 heads	24,953	25.0%
1 head	27	54%	1 head	50,301	50.3%
0 heads	12	24%	0 heads	24,746	24.7%

Note: No, Peter did not sit in his office tossing coins for two days — he let the computer do it for him (in less than a second)...

Tossing Coins, continued

It seems like the probability of getting 1 head is twice that of getting 2 heads (or 0 heads)...

If we have two coins and mark them "A" and "B", we have the following four possible outcomes:

Each time we perform the experiment (toss the coins), we get one of these outcomes (with equal probability). We should expect to get twice as many "1 head" outcomes as "2 heads" (and "0 heads") outcomes...

In order to be able to discuss more complicated scenarios, we introduce the concepts ***random process***, ***sample space***, ***event***, and ***probability***.

To say that a process is **random** means that when it takes place, one outcome from some set of outcomes is sure to occur, but it is impossible to *a priori* predict with certainty what the outcome will be.

In our coin-tossing example, each coin has an outcome in the set $\{\textbf{heads}, \textbf{tails}\}$, and the pair of coins has an outcome in the set (formed by a Cartesian product)

$$\{\textbf{heads}, \textbf{tails}\} \times \{\textbf{heads}, \textbf{tails}\} =$$
$$\{\ \textbf{(heads,heads), (heads,tails), (tails,heads), (tails,tails)}\ \}$$

Definition: ***Sample Space*** **—**

A **sample space** is the set of all possible outcomes of a random process or experiment.

Definition: ***Event*** **—**

An **event** is a subset of a sample space.

In the case an experiment has finitely many outcomes and all outcomes are equally likely to occur, the ***probability*** of an event (set of outcomes) is just the ratio if the number of outcomes in the event to the total number of outcomes.

Equally Likely Probability Formula

If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability of E**, denoted $\mathbf{P(E)}$ is

$$P(E) = \frac{\text{the number of outcomes in } E}{\text{the total number of outcomes in } S}$$

Notation: For any finite set S, $\mathbf{n(S)}$ denotes the number of elements in S.

With this notation, the equally likely probability formula becomes

$$P(E) = \frac{n(E)}{n(S)}$$

A deck of cards contains 52 cards divided into 4 suits:

Red suits		Black suits	
Diamonds	**Hearts**	**Clubs**	**Spades**
$\diamondsuit$	$\heartsuit$	$\clubsuit$	$\spadesuit$
$2\diamondsuit$, $3\diamondsuit$	$2\heartsuit$, $3\heartsuit$	$2\clubsuit$, $3\clubsuit$	$2\spadesuit$, $3\spadesuit$
$4\diamondsuit$, $5\diamondsuit$	$4\heartsuit$, $5\heartsuit$	$4\clubsuit$, $5\clubsuit$	$4\spadesuit$, $5\spadesuit$
$6\diamondsuit$, $7\diamondsuit$	$6\heartsuit$, $7\heartsuit$	$6\clubsuit$, $7\clubsuit$	$6\spadesuit$, $7\spadesuit$
$8\diamondsuit$, $9\diamondsuit$	$8\heartsuit$, $9\heartsuit$	$8\clubsuit$, $9\clubsuit$	$8\spadesuit$, $9\spadesuit$
$10\diamondsuit$	$10\heartsuit$	$10\clubsuit$	$10\spadesuit$
$J\diamondsuit$, $Q\diamondsuit$	$J\heartsuit$, $Q\heartsuit$	$J\clubsuit$, $Q\clubsuit$	$J\spadesuit$, $Q\spadesuit$
$K\diamondsuit$, $A\diamondsuit$	$K\heartsuit$, $A\heartsuit$	$K\clubsuit$, $A\clubsuit$	$K\spadesuit$, $A\spadesuit$

Figure: A deck of cards, J — Jack, Q — Queen, K — King, these are known as *"face cards;" and A — Ace.*

Imagine a shuffled deck of cards (the cards are in random order), with the cards turned over so that their values are hidden. Suppose you pick one card at random.

Questions:

[a] What is the sample space of outcomes?

[b] What is the event that the chosen card is a black face card?

[c] What is the probability that the chosen card is a black face card?

[a] The sample space is

$$S = \left\{ \begin{array}{l} 2\diamondsuit, 3\diamondsuit, 4\diamondsuit, 5\diamondsuit, 6\diamondsuit, 7\diamondsuit, 8\diamondsuit, 9\diamondsuit, 10\diamondsuit, J\diamondsuit, Q\diamondsuit, K\diamondsuit, A\diamondsuit, \\ 2\heartsuit, 3\heartsuit, 4\heartsuit, 5\heartsuit, 6\heartsuit, 7\heartsuit, 8\heartsuit, 9\heartsuit, 10\heartsuit, J\heartsuit, Q\heartsuit, K\heartsuit, A\heartsuit, \\ 2\clubsuit, 3\clubsuit, 4\clubsuit, 5\clubsuit, 6\clubsuit, 7\clubsuit, 8\clubsuit, 9\clubsuit, 10\clubsuit, J\clubsuit, Q\clubsuit, K\clubsuit, A\clubsuit, \\ 2\spadesuit, 3\spadesuit, 4\spadesuit, 5\spadesuit, 6\spadesuit, 7\spadesuit, 8\spadesuit, 9\spadesuit, 10\spadesuit, J\spadesuit, Q\spadesuit, K\spadesuit, A\spadesuit \end{array} \right\}$$

[b] The event "black face-card" is

$$E = \{J\clubsuit, Q\clubsuit, K\clubsuit, J\spadesuit, Q\spadesuit, K\spadesuit\}$$

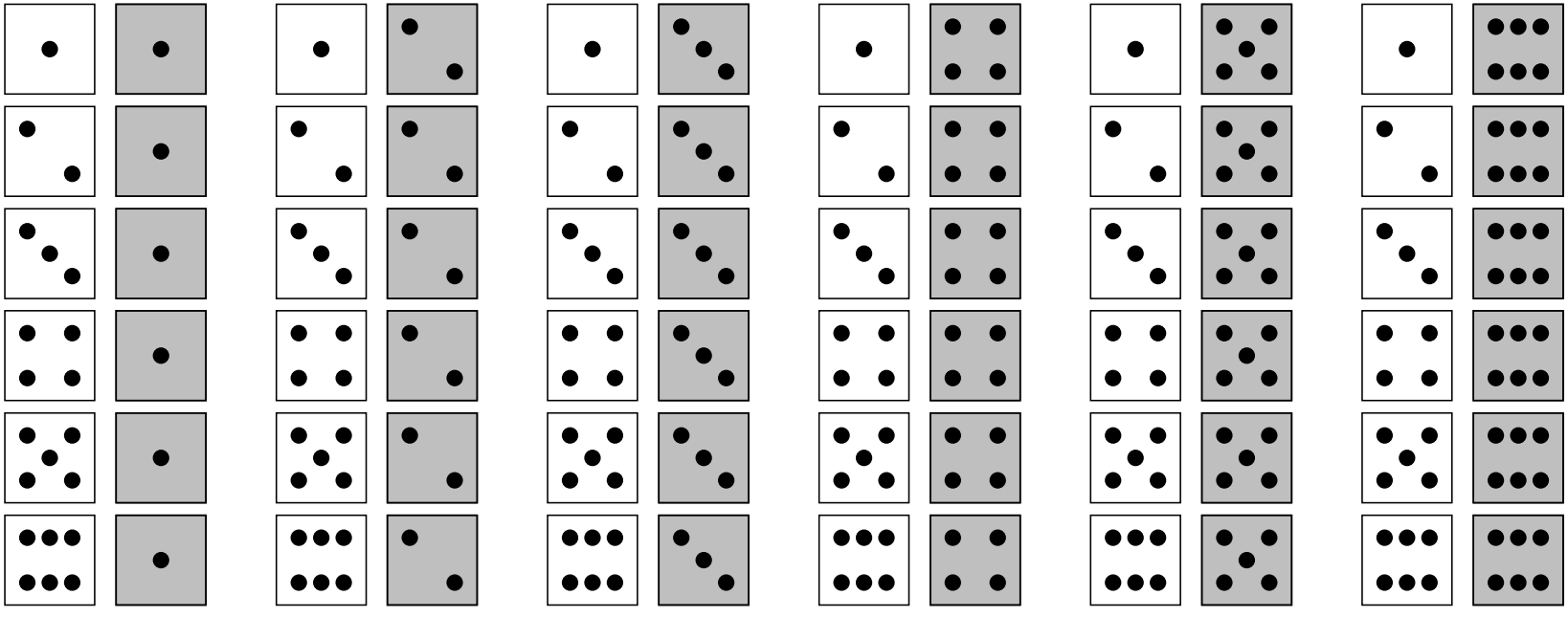
[c] The probability of a black face card is given by

$$P(E) = \frac{n(E)}{n(S)} = \frac{6}{52} = \frac{3}{26} \approx 11.5\%.$$

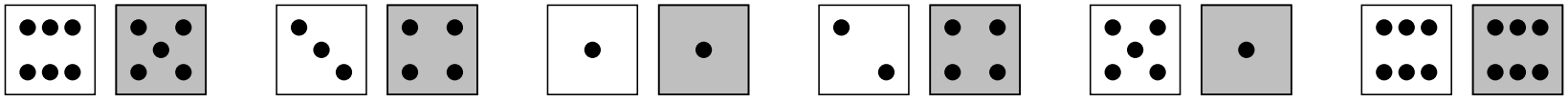
Example: Rolling a Pair of Dice 1 of 3

A **die** is one of a ***pair of dice***. It is a cube with six sides, each containing a marking of one thru six dots, called ***pips***.

Suppose a white and a gray die are tossed together, and the number of dots that occur face up on each is recorded — the following are the possible outcomes (the sample space):



We can introduce a more compact notation by describing each possibility with a pair of numbers, *e.g.*



"6-5" "3-4" "1-1" "2-4" "5-1" "6-6"

Questions:

[a] Use the compact notation to write the sample space S of possible outcomes.

[b] Use the set notation to write the event E that the face numbers sum to six.

[c] What is the probability that the face numbers have a sum of six?

[a] Use the compact notation to write the sample space S of possible outcomes.

$$\mathbf{S} = \left\{ \begin{array}{l} \text{1-1, 1-2, 1-3, 1-4, 1-5, 1-6, 2-1, 2-2, 2-3, 2-4, 2-5, 2-6,} \\ \text{3-1, 3-2, 3-3, 3-4, 3-5, 3-6, 4-1, 4-2, 4-3, 4-4, 4-5, 4-6,} \\ \text{5-1, 5-2, 5-3, 5-4, 5-5, 5-6, 6-1, 6-2, 6-3, 6-4, 6-5, 6-6} \end{array} \right\}$$

[b] Use the set notation to write the event E that the face numbers sum to six.

$$\mathbf{E} = \left\{ \text{ 1-5, 2-4, 3-3, 4-2, 5-1 } \right\}$$

[c] What is the probability that the face numbers have a sum of six?

$$\mathbf{P(E)} = \frac{\mathbf{n(E)}}{\mathbf{n(S)}} = \frac{\mathbf{5}}{\mathbf{36}} \approx \mathbf{13.9\%}$$

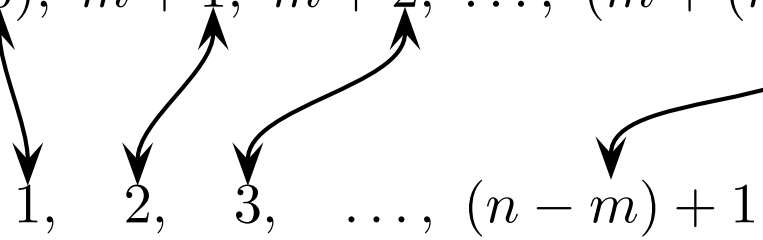
Example: Counting Element of a List

Question: If m and n are integers ($m \leq n$), how many integers are there from m through n (including m and n)?

We write down the list:

$$m = (m+0),\ m+1,\ m+2,\ \ldots,\ (m+(n-m)) = n$$

and count



Theorem: If m and n are integers and $m \leq n$, then there are $(n - m + 1)$ integers from m to n inclusive.

Example: Counting the Elements of a Sublist

Questions:

[a] How many 3-digit integers are divisible by 5?

[b] What is the probability that a given 3-digit integer is divisible by 5?

Solutions:

[a] The smallest 3-digit integer divisible by 5 is $100 = 5 \cdot 20$. The largest 3-digit integer divisible by 5 is $995 = 5 \cdot 199$. Clearly, there are as many 3-digit integers divisible by 5 as there are integers in the range from $m = 20$ to $n = 199$, *i.e.* $\mathbf{199 - 20 + 1 = 180}$.

[b] There are $999 - 100 + 1 = 900$ 3-digit integers. By [a] 180 of these are divisible by 5; the probability that a randomly chosen 3-digit integer is divisible by 5 is given is $\mathbf{180/900 = 1/5 = 20\%}$.

Convergence of the World Series?

In many situations a ***tree structure*** is a useful tool for accounting for all possibilities when events happen ***in order***. Consider the World Series in baseball... To teams A and B play until one team has won 4 games... There are many ways this can happen:

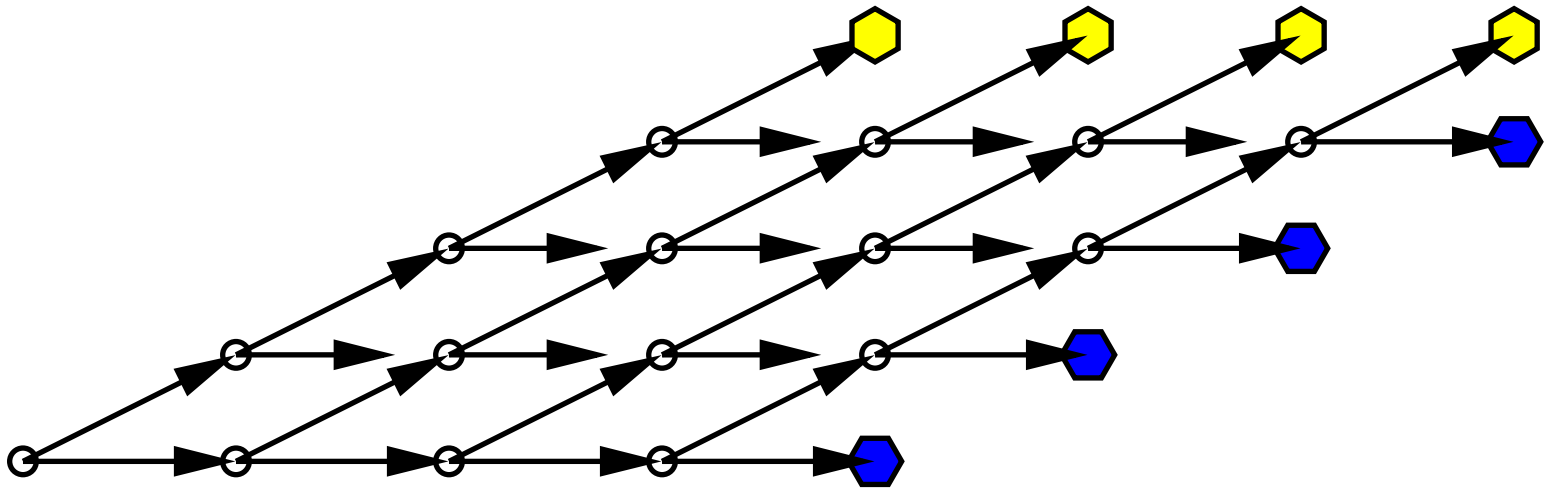


Figure: Playing the world series. Here an arrow to the right corresponds to a win for team A, and an arrow up/right corresponds to a win for team B. Team A wins the world series if we reach one of the terminal boxes to on the right (blue hexagons), and team B wins if we reach one of the terminal boxes on top (yellow hexagons).

Possibility Trees

The previous figure shows all the possible ways the world series can play out, ***but*** there are multiple ways to reach some (most) states; *e.g.* the scenario "A wins, B wins" and "B wins, A wins" end up in the same **state** (one win for each team).

In a possibility tree, these two paths are differentiated; the possibility tree for the first 5 games looks like this:

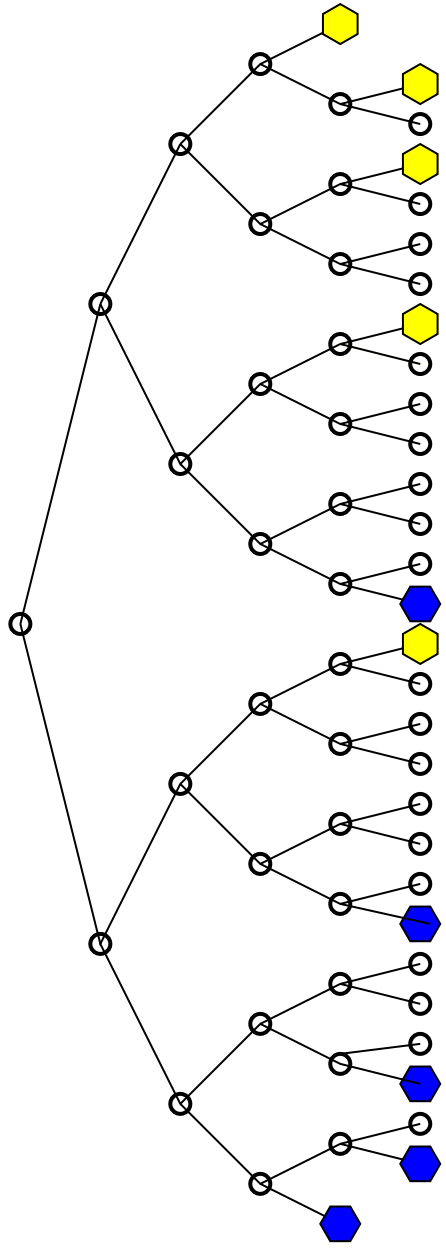


Figure (to the right:) The possibility tree for the first 5 games of the world series. Note that 2 (out of 16) paths terminate after 4 games. An additional 8 paths terminate after 5 games...

[a] How many ways can the world series be played? — We must add the two remaining games to the possibility tree to answer this question.

[b] Assuming all outcomes are equally likely, what is the probability that the world series will terminate in no more than five games?

Solutions:

[a] Let 0 denote a win for team A and 1 a win for team B, then we can write the sample space as a string of games. Let S_A be the outcomes where team A wins, and S_B be the outcomes where team B wins ($S = S_A \cup S_B$)

$$S_A = \left\{ \begin{array}{l} 0000, 00010, 00100, 01000, 10000, 000110, 001010, 001100, 010010, \\ 010100, 011000, 100010, 100100, 101000, 110000, 0001110, 0010110, \\ 0011010, 0011100, 0100110, 0101010, 0101100, 0110010, 0110100, \\ 0111000, 1000110, 1001010, 1001100, 1010010, 1010100, 1011000, \\ 1100010, 1100100, 1101000, 1110000 \end{array} \right\}$$

$$S_B = \left\{ \begin{array}{l} 1111, 11101, 11011, 10111, 01111, 111001, 110101, 110011, 101101, \\ 101011, 100111, 011101, 011011, 010111, 001111, 1110001, 1101001, \\ 1100101, 1100011, 1011001, 1010101, 1010011, 1001101, 1001011, \\ 1000111, 0111001, 0110101, 0110011, 0101101, 0101011, 0100111, \\ 0011101, 0011011, 0010111, 0001111 \end{array} \right\}$$

Hence, the world series can be played in 70 different ways.

[b] With the same notation E_A is the event that team A wins in no more than 5 games, and E_B is the event that team B wins in no more than 5 games ($E = E_A \cup E_B$):

$$E_A = \left\{ \; 0000, 00010, 00100, 01000, 10000 \; \right\}$$

$$E_B = \left\{ \; 1111, 11101, 11011, 10111, 01111 \; \right\}$$

and we have

$$P(E) = \frac{n(E)}{n(S)} = \frac{10}{70} = \frac{1}{7} \approx 14.3\%$$

Independent Events and the Multiplication Rule

If we have a sequence of events which are ***independent*** (note that this does not apply to the world series, since depending on the outcome of previous games, games #5, #6, and #7 may not be played) the multiplication rule applies:

Theorem: ***Multiplication Rule*** **—**
If an operation consists of k steps and step $\#i$ can be performed in n_i ways $i = 1, 2, \ldots, k$, then the entire operation can be performed in $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ ways.

If all 7 games of the world series were played no matter what the outcome of the previously played games:

$$k = 7, \quad n_1 = n_2 = n_3 = n_4 = n_5 = n_6 = n_7 = 2$$

$$\mathbf{2^7 = 128} \ \textbf{possibilities.}$$

Example: Selecting an Alphanumeric Password

You are to select an 8-digit alphanumeric { **a–z, A–Z, 0–9** } password.

This can be viewed as an 8-step operation where each symbol is selected independently from the 62 possible digits.

There are $\mathbf{62^8 = 218,340,105,584,896}$ possible passwords.

Swedish has 3 additional vowels {**å, ä, ö**}, so each alphanumeric digit in a Swedish password has 68 possibilities, hence there are $\mathbf{68^8 = 457,163,239,653,376}$ Swedish passwords.

It is (vaguely) interesting to note that by adding 6 more possibilities for the digits, we doubled the password space!

Example: Selecting a Password Without Repetition

The department-of-good-ideas^{TM} has announced that no passwords are allowed to contain the same character twice.

If we are building an 8-digit password from the the digits { **a–z, A–Z, 0–9** } we have 62 possibilities for the first digit, then 61 for the second, 60 for the third, etc... All in all there are

$$\mathbf{62 \cdot 61 \cdot 60 \cdot 59 \cdot 58 \cdot 57 \cdot 56 \cdot 55 = 136,325,893,334,400}$$

possible 8-digit passwords without repetition. The probability the a random 8-digit password does not repeat any character is:

$$\mathbf{P(\text{no repetition}) = \frac{136,325,893,334,400}{218,340,105,584,896} \approx 62.4\%}$$

Example: The Number of Elements in a Cartesian Product

Suppose A_1, A_2, ..., A_k are sets with n_1, n_2, ..., n_k elements respectively.

Now consider the set $A = A_1 \times A_2 \times \ldots \times A_k$ [The Cartesian Product of the sets]; each element in A is an ordered k-tuple of the form $(a_1, a_2, \ldots, a_k)$ where $a_i \in A_i$, $i = 1, 2, \ldots, k$.

We can view the construction of the k-tuple as a k-step process of independent operations:

for i=1,..., k
Choose the i^{th} element of the k-tuple.
end

In step #i there are n_i ways to make the choice, so by the multiplication rule there are

$\mathbf{n_1 \cdot n_2 \cdot \ldots \cdot n_k}$ ***ways to perform the entire operation***

The Multiplication Rule is NOT Always Applicable

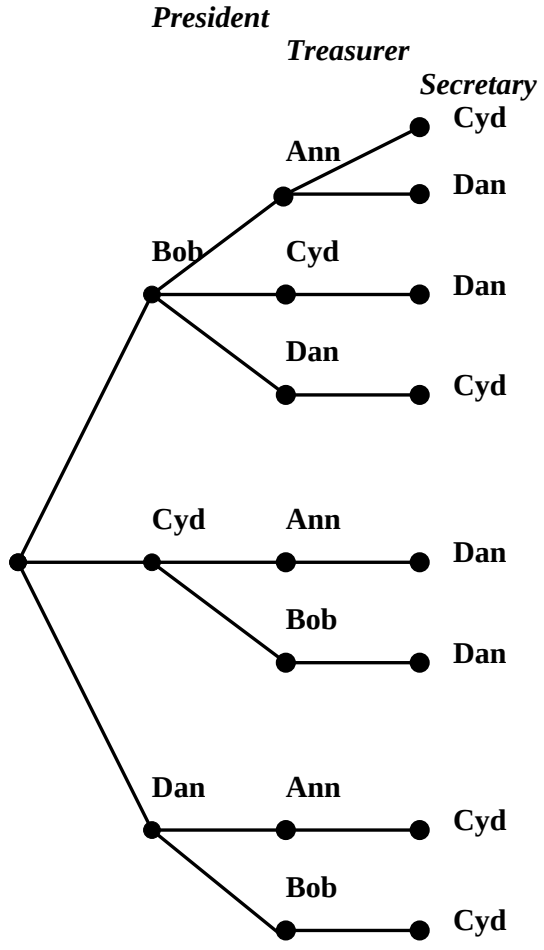
We are to select a ***president***, ***treasurer***, and a ***secretary*** for an organization — there are four eligible candidates {**Ann, Bob, Cyd, Dan**}; further these restrictions apply:

Ann cannot be president

Cyd or Dan must be secretary

To the right we see the ***possibility tree*** associated with selecting the president, treasurer, and secretary (in that order).

We notice that the number of choices in each step ***depends*** on the previous choices — therefore the multiplication rule does not apply!



Epp v3.0

Epp-5.2.1, Epp-5.2.5, Epp-5.2.17, Epp-5.2.37

Epp-5.3.20, Epp-5.3.39

Epp-6.1.3, 6.1.10, 6.1.31

Epp-6.2.1, Epp-6.2.12

Epp v2.0

Epp-5.2.1, Epp-5.2.5, Epp-5.2.24, Epp-5.2.26

Epp-5.3.45, —

Epp-6.1.3a, —, —

Epp-6.2.1, —