Math 100 Spring 2015

David Ross, Department of Mathematics

Revised:

May 1, 2015

1 Some notation:

$\mathbb{N} = 0, 1, 2, 3, \ldots$ (The **natural numbers**) **Note⇓**

$\mathbb{Z} = 0, \pm 1, \pm 2, \pm 3, \ldots$ (The **integers**)

$\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ (The **rational numbers**)

$\mathbb{R}$ =the **real numbers**

$\mathbb{Z}^+ = 1, 2, 3, \ldots$ (The *positive* integers, or **whole numbers**) (also $\mathbb{N}^+$) **Note⇓**

$\mathbb{Q}^+ = \{r \in \mathbb{Q} : r > 0\}$ (The *positive* rational numbers)

$\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$(The *positive* real numbers)

Warning⇑ The text exactly reverses the meanings of "whole number" and "natural number". From now on, I'll (reluctantly) conform to the text's horrible use, ie

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$
$$\text{Whole numbers} = \{0, 1, 2, 3, 4, \ldots\}$$

A bit more notation (useful shorthand):

$\forall$ means "for all" or "for every"

$\forall$ is never used in isolation, but together with a *variable*, i.e. $\forall x$ or $\forall n$

$\exists$ means "there exists" or "there is at least one"; also not used alone

Examples:

$\forall x(x = x)$

"For every x, $x = x$" (In other words, every number equals itself.)

$\exists n \in \mathbb{Z}(n + 1 = 0)$

"For some integer n, $n + 1 = 0$"... but note that it is *not* true that $\exists n \in \mathbb{N}(n + 1 = 0)$

$\forall x \exists y(x < y)$

"For every x there is at least one larger y." Note true for $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, etc.

$\exists x \forall y(x < y)$

"There exists an x such that for every y, $y > x$." This is always false, since no x is bigger than itself.

2 Sets

- A *set* is a collection of objects.
- This seems to be a vague and circular definition: what is an object? what is a collection?
- It *is* too vague; see Russell's paradox below.
- We'll worry about this later (though not much), not now.

How do we indicate a set?

By explicitly listing all elements:
$\{1, 2, 3\}$;
$\{a, b, Harvey\}$
$\{\}$

By implicitly listing all elements:
$\{1, 2, 3, \ldots, 1000\}$;
$\{a, b, \ldots, z\}$;
{Oahu, Maui, Kauai,. . . }

By name: $\mathbb{R}$; $\mathbb{N}$; $\mathbb{Q}$; $\emptyset$

By description, using set-builder notation:
$\{n \in \mathbb{N} \mid n \text{ prime}\}$;
$\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$;
$\{n \in \mathbb{N} \mid n \neq n\}$

Note the use of the symbol ϵ, meaning "in" or "element of."

This is the only 'primitive' set operation; everything else will be defined in terms of ϵ.

We will say synonymously: $x \in A$; "x is an element of A"; "A contains x"

Notation and operations:

Extensionality: A set is completely determined by its contents, not how that set is presented. So, the following sets are all equal:

1. $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
2. $\{5, 4, 3, 2, 1, 6, 7, 8, 9\}$ (order doesn't matter)
3. $\{1, 1, 1, 1, 1, 2, 3, 4, 5, 4, 3, 2, 1, 9, 6, 7, 8, 9\}$ (duplication doesn't matter)
4. $\{1, 2, 3, \ldots, 9\}$ (as long as the ellipsis is unambiguous)
5. $\{x \in \mathbb{N} \ : \ 1 \leq x \leq 9\}$ (but note how important specifying the $\mathbb{N}$ is!)

When we write $A = B$ (where A and B are sets) we mean the following synonymous things:

1. Every element of A is an element of B and vice versa.
2. $\forall x \ (((x \in A) \Rightarrow (x \in B)) \wedge ((x \in B) \Rightarrow (x \in A)))$

Subsets

Definition: $A \subseteq B$ (A is a *subset* of B) if every element of A is an element of B.

Equivalently: $A \subseteq B$ if $\forall x\ (x \in A \Rightarrow x \in B)$

Equivalently: $A \subseteq B$ if $\forall x \in A\ (x \in B)$

Examples :

1. $\{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5\}$
2. $\{1, 2, 3, 4, 5\} \not\subseteq \{1, 2, 3\}$
3. To show that $A \subseteq B$ you need to show that *every* element of A is an element of B. To show that $A \not\subseteq B$ you need only find *one* element of A that is not in B.
4. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subset \mathbb{R}$
5. $\{1, 2, 3, 4, 5\} \subseteq \{1, 2, 3, 4, 5\}$
6. In fact, for *any* set A, $A \subseteq A$
7. $\{\} \subseteq \{1, 2, 3, 4, 5\}$ (!)
8. In fact, for *any* set A, $\emptyset \subseteq A$
9. List all the subsets of $\{1, 2, 3\}$

Graphical representations often help our intuition (class)

Proper Subset: Say that A is a *proper* subset of B, $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Notation: Sometimes you'll see proper subset written as $A \subsetneq B$ or $A \subsetneqq B$ or $A \subsetneqq B$.

Examples :

1. $\mathbb{N} \subset \mathbb{Z}$
2. $\mathbb{N} \subseteq \mathbb{N}$, but $\mathbb{N} \not\subset \mathbb{N}$
3. List proper subsets of {1,2,3}

Some Useful Properties:

$\emptyset \subseteq A$ for any set A (Tricky!)

$A \subseteq A$ for any set A

Transitivity: If $A \subseteq B$ and $B \subseteq C$ than $A \subseteq C$

(Alternate definition of equality) If A and B are sets, then $A = B$ if and only if ($A \subseteq B$ and $B \subseteq A$)

If A is finite with N elements then A has 2^N subsets.

2.2 Set Operations (union, intersection, set difference, complement)

Intersection: The *intersection* of two sets is the set of elements common to both of them.

Equivalently,

$$A \cap B =_{\text{def}} \{x \mid x \in A \text{ and } x \in B\}$$

Equivalently,

$$x \in (A \cap B) \text{ provided } (x \in A) \wedge (x \in B)$$

Union: The *union* of two sets is the set of elements appearing in either of them.

Equivalently,

$$A \cup B =_{\text{def}} \{x \mid x \in A \text{ or } x \in B\}$$

Equivalently,

$$x \in (A \cup B) \text{ provided } (x \in A) \vee (x \in B)$$

Examples :

1. $\{1, 2, 3, 4\} \cap \{2, 4, 6, 8\} =$

2. $\{1, 2, 3, 4\} \cup \{2, 4, 6, 8\} =?$

3. $\{2k | k \in \mathbb{N}\} \cap \{3k | k \in \mathbb{N}\} =?$

4. $\{2k | k \in \mathbb{N}\} \cup \{2k + 1 | k \in \mathbb{N}\} =?$

Set Difference: The *difference* of two sets is the set of elements in one but not the other.

Equivalently,

$$A - B =_{\text{def}} \{x \mid x \in A \text{ and } x \notin B\}$$

Equivalently,

$$x \in (A - B) \text{ provided } (x \in A) \wedge (x \notin B)$$

Examples :

1. $\{1, 2, 3, 4\} - \{2, 4\} =?$
2. $\{1, 2, 3, 4\} - \{2, 4, 6, 8\} =?$
3. $\{2, 4\} - \{1, 2, 3, 4\} =?$
4. $\{2, 4, 6, 8\} - \{1, 2, 3, 4\} =?$
5. $\{1, 2, 3, 4\} - \{1, 2, 3, 4\} =?$
6. In fact, for *any* set A, $A - A = \emptyset$
7. $\mathbb{N} - \{2k | k \in \mathbb{N}\} =?$
8. $\{2k | k \in \mathbb{N}\} \cup \{2k - 1 | k \in \mathbb{N}\} =?$

Complement: If $A \subset B$ then $B - A$ is the *complement* of A in B.

If all sets A under consideration are assumed to be subsets of some particular set U (*universe of discourse*) then $U - A$ is just the *complement* of A, and we denote it by $A^{\complement}$ (or A' in some texts, including ours).

Example The complement of the set of even natural numbers in $\mathbb{N}$ is the set of odd natural numbers.

Pictures:

2.3 Some useful properties

Associative laws:

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

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

Distributive laws:

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

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

DeMorgan laws:

$(1)\ A - (B \cup C) = (A - B) \cap (A - C)$

$(1')\ (B \cup C)^{\complement} = B^{\complement} \cap C^{\complement}$

$(2)\ A - (B \cap C) = (A - B) \cup (A - C)$

$(2')\ (B \cap C)^{\complement} = B^{\complement} \cup C^{\complement}$

Misc.

(1) If $A \subseteq B$ then $A \cap B = A$ and $A \cup B = B$

(2) (In fact, if $A \cap B = A$ or $A \cup B = B$ then $A \subseteq B$)

(For the rest of the properties, assume there's a universal set U)

(3) $(A^{\complement})^{\complement} = A$

(4) $A \cap A^{\complement} = \emptyset; \quad A \cup A^{\complement} = U$

(5) If $A \subset B$ then $B^{\complement} \subset A^{\complement}$

2.4 Why rigor is necessary

Russell's Paradox:

Consider the following definition of a set:

$$W = \{x \mid x \notin x\}$$

Suppose $W \notin W$.

Then W satisfies the definition of W, so $W \in W$.

So W must be in W, $W \in W$.

But to be in W an object must not contain itself, so $W \notin W$.

Uh oh.

The real conclusion to the above *paradox* is that the formula we gave above does not properly define a set; there is no "set of all sets."

So, how do we know whether the things we write down are really sets?

The Modern Approach: wrote down formal properties for sets corresponding to our intuition, try not to include enough properties to construct something paradoxical.

For this class we will focus on basic set operations and try not to worry too much whether the the things we have written down are actually sets. However, the defining properties should always be clear enough that *if* the thing we define is a set, *then* there is no doubt what the elements of that set would be.

2.5 Ordered pairs, triples, n-tuples, Cartesian products

Definition: An *ordered pair* is an object (a, b) with the property:
$(a, b) = (c, d)$ if and only if $a = c$ and $b = d$

EG: If $x, y \in \mathbb{R}$ then (x, y) is a point in the plane (and vice versa)

Note that order counts: if $(a, b) = (b, a)$ then $a = b$

So $(2, 3) \neq (3, 2)$ but $(3, 3) = (3, 3)$

Remark: Difference between $(2, 3)$ and $\{2, 3\}$

Can have ordered pairs of things other than numbers numbers, eg (Taylor Swift, Aloha Tower)

Definition: If A and B are sets, the *Cartesian product* of A and B is

$$A \times B =_{def} \{(a, b) \colon a \in A, b \in B\}$$

EG: Famous Dogs $\times$ Transcendental Numbers $=$

$\{(\text{Lassie}, \pi), (\text{Rin Tin Tin}, e), (\text{Cujo}, \pi), \dots\}$

More generally: Can generalize to *ordered triples* (a, b, c), or ordered $n-$tuples $(x_1, x_2, \dots, x_n)$

EG: $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (or $\mathbb{R}^3$) $=$
$\{(a, b, c) \colon a, b, c \in \mathbb{R}\}$ =3-dimensional space

The 4-tuple (Cujo, David Ross, Eiffel Tower, 17) is an element of
Famous Dogs $\times$ UH Math Professors $\times$ French Buildings $\times$ Primes

Counting principle: If A, B are finite sets, A has n elements, and B has m elements, then $A \times B$ has mn elements.

More generally, if $A_1, A_2, \ldots, A_k$ are finite with (respectively) $n_1, n_2, \ldots, n_k$ elements then $A_1 \times A_2 \times \cdots \times A_k$ is finite with $n_1 n_2 n_3 \cdots n_k$ elements.

EG: Roll 4 dice, number of different throws =?

EG: From a deck of cards, how many ways are there to pick one card from each suit?

2.6 Cardinality

Start simple: How many elements are there in the following sets?

1. $\{\}$
2. $\{2, 4, 6, 4, 2\}$
3. $\{0, 1, 2\}$

What about $\mathbb{N}$? $\mathbb{R}$?

What if we don't know what "how many" means?

Start simpler: Define what it means for two sets to be the same size:

Definition: A set A is *conumerous* with B provided A and B can be put into a one-to-one correspondence. (Picture)

Other, equivalent notation/terminology for "A is conumerous with B":

a. A and B *have the same number of elements*

b. A and B *have the same cardinality*

c. $\text{card}(A) = \text{card}(B)$

Examples: 1. The sets above.

2. Finite sets and von Neumann natural numbers; definition of finite.

Galileo Galilei, 1638

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, \dots\} \qquad (= \mathbb{N})$$

and

$$\{0, 1, 4, 9, 16, 25, 36, 49, 64, \dots\} \qquad (= \{n^2 : n \in \mathbb{N}\})$$

are conumerous.

More examples:

1. $\mathbb{N}$ and $\mathbb{N} - \{0\}$ (cf *Hilbert's Hotel*)
2. $\mathbb{N}$ and $\mathbb{Z}$
3. Any two line segments (in the plane)
4. The real interval $(0, 1) \subset \mathbb{R}$ and all of $\mathbb{R}$

We now have:

Finite sets: $\text{card}(A) = \text{card}(\{0, 1, 2, \ldots, n-1\})$ for some $n \in \mathbb{N}$

Infinite sets: $\mathbb{N}, \mathbb{N} - \{0\}, \mathbb{Z}$ - all have the same cardinality

More infinite sets: $(0, 1), \mathbb{R}$, any line segment in plane - all have same cardinality

Questions: 1. Do $\mathbb{N}$ and $\mathbb{R}$ have the same cardinality? (Answer: No)

2. If not - what is the relationship between these *orders of infinity*?

3. **(Continuum hypothesis)** Is there a set E such that $\mathbb{N} \subset E \subset \mathbb{R}$ and $\text{card}(\mathbb{N}) \neq \text{card}(E) \neq \text{card}(\mathbb{R})$?

Theorem (Cantor): $\text{card}(\mathbb{R}) \neq \text{card}(\mathbb{N})$

Proof:

Definition: An infinite set A is *countable* (or *denumerable*, or *enumerable*) if it has the same cardinality as $\mathbb{N}$.

So: $\mathbb{N}, \mathbb{N} - \{0\}, \mathbb{Z}$ are countable.

$\mathbb{R}$ is *not* countable.

What about $\mathbb{Q}$?

Some useful (obvious?) facts

Theorem For any sets A, B, and C:

1. A has the same cardinality as A
2. If A has the same cardinality as B then B has the same cardinality as A
3. If A has the same cardinality as B and B has the same cardinality as C then A has the same cardinality as C

Definition: *A has no greater cardinality than B* (or $\text{card}(A) \leq \text{card}(B)$) provided A has the same cardinality as some subset of B, that is, for some $C \subseteq B$, $\quad \text{card}(A) = \text{card}(C)$

Some terminology

The *cardinal number* of a set A is the collection of all sets with the same cardinality as A. (Warning!)

A set is *countable* if it is either finite or countably infinite, otherwise it is *uncountable*.

A countably infinite set is said to have cardinal number (or *cardinality*) $\aleph_0$

A set with same cardinality as $\mathbb{R}$ is said to have *cardinality of the continuum* (or cardinal number $\mathfrak{c}$, or sometimes $2^{\aleph_0}$, for reasons that will be clear later).

Two statements that show that $\aleph_0$ is the smallest infinite cardinality

I. Every infinite set contains a countably infinite subset.

II. Every subset of a countably infinite set is countable.

(Proof of I)

(Cantor-Schröder-Bernstein) If $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(A)$ then $\text{card}(A) = \text{card}(B)$

Examples:

$(0, 1) \subseteq [0, 1] \subset \mathbb{R}$, so...

Property II from previous page.

Remark on Axiom of Choice

We know that for every infinite set A, $\text{card}(A) < \text{card}(\mathbb{N})$ or $\text{card}(A) = \text{card}(\mathbb{N})$ or $\text{card}(\mathbb{N}) < \text{card}(A)$. (Why?)

In other words, $\mathbb{N}$ is *comparable* to all other sets.

We'd like *all* sets to be comparable, since then cardinalities would 'line up' (picture)

Zermelo's Axiom of Choice (AC): If $\mathcal{A}$ is any collection of disjoint nonempty sets, then there is a new set containing exactly one element from each of the given sets. (picture)

Theorem: If AC is true then all sets are comparable in the sense that $\forall A \forall B \big(\text{card}(A) \leq \text{card}(B) \vee \text{card}(B) \leq \text{card}(A) \big)$

Theorem (Paul Cohen) AC is independent of the other axioms of set theory.

> *To choose one sock from each of infinitely many pairs of socks requires the Axiom of Choice, but for shoes the Axiom is not needed.*
> – Bertrand Russell

More examples

I. The algebraic numbers are countable. (We'll define "algebraic" and "transcendental" later.)

Note that it follows that there exist at least one transcendental number.

II. Let S be the interior of the unit square in the plane,

$$S = \{(x, y) \colon 0 < x, y < 1\},$$

sometimes denoted by $(0, 1) \times (0, 1)$. Then S has cardinality $\mathfrak{c}$, that is, $\text{card}(S) = \text{card}((0, 1))$.

III. (Cantor) For any set A, $\text{card}(A) \neq \text{card}(\mathcal{P}(A))$ (in fact, $\text{card}(A) < \text{card}(\mathcal{P}(A))$ (Note: $\mathcal{P}(A)$ is the set of all subsets of A.)

Note that means that

$$\underset{\aleph_0}{\text{card}}(\mathbb{N}) < \underset{2^{\aleph_0}}{\text{card}}(\mathcal{P}(\mathbb{N})) < \underset{2^{2^{\aleph_0}}}{\text{card}}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \cdots$$

GCH (*General Continuum Hypothesis*) For any infinite set A, there is no cardinality between $\text{card}(A)$ and $\text{card}(\mathcal{P}(A))$

(Cohen) This is independent of the usual axioms of set theory

3 Formal/Symbolic Logic - General

- What statements are true or false by virtue of form alone?
- Formal v. informal logic

Some reasons to formalize logic:

- Make determining the truth of difficult logical statements a matter of simple calculation.
- Clarify which deductive methods (classical forms) are sound (correct) or necessary.
- Make it possible to formalize other disciplines (mathematics, computer science, others)
  - Automated theorem proving and program verification
  - Generalization through abstraction
  - Limits of mechanical thought; free will vs. determinism
- Problems with informal reasoning.
  (Ionesco, *Rhinoceros*; Schulman, *Life and loves of Dobie Gillis*)

Considerations in establishing a formal system:

- Should not be unnecessary cumbersome, difficult to use, or difficult to typeset
  (Examples: Lull et al; Lewis Carroll; Frege; Principia Mathematica; RPN; JSL)
- Should correspond to intuition.
- Should be extensive enough to cover all sitations of interest.
- Should be small enough to be tractable.
- (Propositional logic; Predicate Logic [aka First Order Logic]; Higher order logics and infinitary logics.)
- Should allow for a distinction between *syntactic* and *semantic* argument. (more later)
- Should be amenable to *metamathematical analysis*, for example, mathematical proofs about statements about the logic.

Steps in practice:

- Decide on the appropriate formal system (this class: propositional logic or predicate logic)
- Translate statements from English into the formalism (3.1 in our text)
- Analyze using the logic rules

4 Logical connectives (negation, disjunction, conjunction, implication)

The following are examples of statements that have (or might have) a definite *truth value*, that is, be either true or false:

1. $5 + 7 = 12$
2. $5 + 7 = 14$
3. My dog is black.
4. The King of France is bald.
5. $x = 5$
6. $A > B$

Note that the truth value of the last two can change, depending on the values of x, or of A and B. Nevertheless, they are assertions that *might* have a truth value, and *will* do if x, A, B take on values.

Similarly, the truth value of (4) is a matter of some debate; it depends on whether you interpret the sentence as asserting the existence of a King of France.

For comparison, here are some sentences with no notion of a truth value:

1. Ouch.
2. Let x be an integer.
3. Smell the ocean!

A statement that has (or could have) a truth value is called a *proposition*; the terms 'proposition', 'assertion', and 'statement' are generally used interchangeably.

A *logical connective* is an operation we apply to one or more proposition to get a new proposition.

We will look at the following logical connectives: implication ($\Longrightarrow$), negation ($\sim$), disjunction ($\vee$), conjunction ($\wedge$ or &).

4.1 Implication

Suppose A and B are propositions. The following are all different ways of saying the same thing:

$$\begin{gathered}
\text{If } A \text{ then } B \\
A \text{ implies } B \\
A, \text{ therefore } B \\
A \text{ is sufficient for } B \\
\text{For } B \text{ it is sufficient that } A \\
B \text{ is necessary for } A \\
B \text{ follows from } A \\
A \implies B
\end{gathered}$$

Intuitively, if $A \implies B$ and A is true then this 'forces' B to be true as well. However, if A is false then it doesn't force anything about B. We therefore say that $A \implies B$ is true unless A is true and B is false.

Examples (determine the truth value if possible)

1. If $1 + 1 = 2$ then $1 + 1 = 3$.
2. If $1 + 1 = 3$ then $1 + 1 = 2$.
3. Sunlight is necessary for photosynthesis. (Equivalently, "if there is photosynthesis, then there is sunlight.")
4. For N to be composite it is sufficient that $\exists p > 1$ $(p|N)$. (Equivalently, "$\exists p > 1$ $(p|N)$ is sufficient for N to be composite;" or, "if $\exists p > 1$ $(p|N)$ then N is composite.")

Note:

- "Composite", for natural numbers, means "not prime" (so 2, 3, and 5 are prime, 4 and 6 are composite)
- $a|b$ is shorthand for "a divides b" or "b is evenly divisible by a"

4.2 Negation

Suppose A is a propositions. The following are all different ways of saying the same thing:

A is false.
A is not true.
Not A.
$\sim A$

Intuitively, $(\sim A)$ has the opposite truth value of A, and is called a *negation* of A. Given a statement, you can always find a negation by putting "not" in front of it or "is false" after it. However, recognizing that one statement is a negation of another is not always easy - in math, or in life.

Examples

1. The moon is made of green cheese.

   Some Negations:

   (a) The moon is not made of green cheese.

   (b) It is false that the moon is made of green cheese.

   (c) The moon fails to be made of green cheese.

   Some Invalid Negations

   (a) The moon is made of poi.

   (b) Mars is made of green cheese.

One way to recognize that B is a negation of A is:

If A is true then B must be false.

If A is false then B must be true.

If one or both of the "must be" statements is not a real "must" then B is not a negation of A.

2. Which are negations of $1 + 1 = 2$?

(a) $1 + 1 \neq 2$

(b) $1 + 1 = 0$

The question of whether $1 + 1 = 0$ is a negation of $1 + 1 = 2$ is an extremely subtle one. They certainly have opposite truth values, but one can imagine a universe in which they are both true. (Can't you? How about $6 + 6 = 0$? Hint: clock arithmetic.)

We will generally only use the term *negation* when referring to "syntactic" opposites.

3. Which are negations of "All mathematics professors eat kittens"?

   (a) No mathematics professors eat kittens.

   (b) Some mathematics professors don't eat kittens.

   (c) All mathematics profeesors eat only dogs.

   (d) David Ross doesn't eat kittens.

> Negating sentences beginning with "All" or "Every" or $\forall x$:
>
> A negation of "$\forall x\ \Phi(x)$" is "$\exists x(\sim \Phi(x))$"
>
> (Recall that $\exists x \cdots$ means "there exists an x such that $\cdots$" or "Some x are $\cdots$" or "For at least one $x, \cdots$", etc.)

4. Find negations:

   (a) Every good boy does fine.

   (b) All politicians are liars.

   (c) $\forall N\ 5|N$. (Note: $5|N$ means "5 divides N" or "N is evenly divisible by 5"

   (d) No mathematics professors eat kittens.

   So - to prove that a 'for all x" statement is *false*, you only need to find *one* x that makes

it false. This is sometimes called *Disproof by Counterexample.*

5. What is a negation of "If $3|N$ then N is composite"?

   (**Answer:** "$3|N$ and N is prime.")

Note that the only way $A \implies B$ can be *false* is when A is true but B is false. To negate $A \implies B$ we want something which is only *true* in this situation, and the obvious statement is then "$A \wedge \sim B$".

Two more remarks about negation:

1. $\sim\sim A$ is equivalent to A
2. Recall that

   $$A \implies B$$

   is equivalent to

   $$(\sim B) \implies (\sim A)$$

   (contrapositive)

4.3 Conjunction, disjunction

Suppose A and B are propositions. The following are all different ways of saying the same thing:

A and B are true.
Both A and B are true.
A is true and B is true.
A and B.
$A \wedge B$.
$A\&B$.

$A \wedge B$ is true when both A and B are true, and false if *either* of them is false. This connective is called *conjunction*.

Examples

1. $1 + 1 = 2$ and $2 + 2 = 4$
2. $1 + 1 = 2$ and $2 + 2 = 6$
3. Abraham Lincoln was the President of the United States and a famous cosmonaut.

Suppose A and B are propositions. The following are all different ways of saying the same thing:

A or B are true.
Either A or B are true.
Either A is true or B is true or both are true.
A is true or B is true.
A or B.
$A \vee B$.

$A \vee B$ is true when A is true or B is true *or both*, and false if *both* of them is *false*. This connective is called *disjunction*.

Examples

1. $1 + 1 = 2$ or $2 + 2 = 4$
2. $1 + 1 = 2$ or $2 + 2 = 6$
3. $1 + 1 = 3$ or $2 + 2 = 6$
4. Abraham Lincoln was the President of the United States or a famous cosmonaut.

5 Propositional (or *sentential*) Logic

5.1 Elements of the formal language; Syntax

Symbols:

- Proposition Letters: $A\ B\ C\ \cdots$ (or sometimes $A_0\ A_1\ \cdots$, or $p\ q\ r\ \ldots$)
- Logical Connectives: $\wedge\ \vee\ \implies\ \sim$
- Other ("non-logical") Symbols: ( )

Formal Definition of a *proposition* (or *sentence*, or *well-formed formula* [abbreviated WFF]):

1. If P is a proposition letter then P is a proposition.
2. If P is a proposition then $\sim P$ is a proposition.
3. If P and Q are propositions then $P \wedge Q$, $P \vee Q$, and $P \Rightarrow Q$ are propositions.
4. Nothing is a proposition unless defined via rules (1)-(3).

The importance of this formal definition is (a) it gives a mechanical way to 'recognize' a proper formula, and (b) that such a formal definition can be done at all!

Remark: The definition of WFF is an example of a *recursive definition*; it explains how to generate complex propositions from simpler ones:

Simplest: $A, B, \ldots$

Next: $\sim A, \sim B, A \wedge A, A \wedge B, B \wedge B, A \vee A, A \vee B, B \vee B, A \Rightarrow A, A \Rightarrow B, B \Rightarrow B, \ldots$

Next: $A \wedge \sim B, A \wedge A \Rightarrow A \wedge B, \ldots$

etc.

Problem: Needs Disambiguation!

Does something like

$$\sim p \vee q$$

mean we negate p then "or" with q, or do we "or" with q first then negate? Note that these give different values!

One solution: use lots of parentheses, eg

$$((\sim p) \vee q)$$

or

$$(\sim (p \vee q))$$

.

The "formal definition" of WFF can be used to make this rigorous:

1. If P is a proposition letter then P is a proposition.
2. If P is a proposition then $(\sim P)$ is a proposition.
3. If P and Q are propositions then $(P \wedge Q)$, $(P \vee Q)$, and $(P \Rightarrow Q)$ are propositions.
4. Nothing is a proposition unless defined via rules (1)-(3).

However, this can lead to horrendous expressions, like

$$(\sim (\sim (\sim (\sim (\sim (\sim (\sim p)))))))$$

instead of the (slightly) less horrific

$$\sim\sim\sim\sim\sim\sim\sim\sim p$$

Common sense tells us to only use parentheses if there is danger of misinterpretation.

5.2 Semantics of Propositional logic:

Semantics (for any logic) refers to the assignation of meaning to the symbols.

In propositional logic, the 'meaning' of a formula is just a truth value.

Use **T** to represent 'True', **F** to represent 'False'

Consider a typical formula: $A \vee B$

We know that intuitively that the English sentence this represents, "Either A is true or B is true (or both)" is either true or false depending on the truth values of A and B. So, a formula won't be simply "true" or "false", but rather true or false relative to some fixed assignment of truth values to the most basic subformulas, the proposition letters.

Definition: A *model* for a propositional logic is an assignment of truth values to the proposition letters.

Remark: Synonyms for *model* are *interpretation* and *structure*.

Formally, if $\mathcal{B}$ is the set of proposition letters of our logic, then a model is a function $\mathcal{M} : \mathcal{B} \to \{\mathrm{T}, \mathrm{F}\}$.

Example: Suppose our logic has only the proposition letters A, B, and C. One model might be to make A true, and both B and C false. We might denote this by $\mathcal{M}(A) = T, \mathcal{M}(B) = F, \mathcal{M}(C) = F$. Or we could write: "$\mathcal{M}$ is the model $A = T, B = F, C = F$." Whatever is easier!

We already have rules telling us how to piece together the truth values of complex formulas from those for simpler ones. For example, with the model $\mathcal{M}$ we just defined, the formula

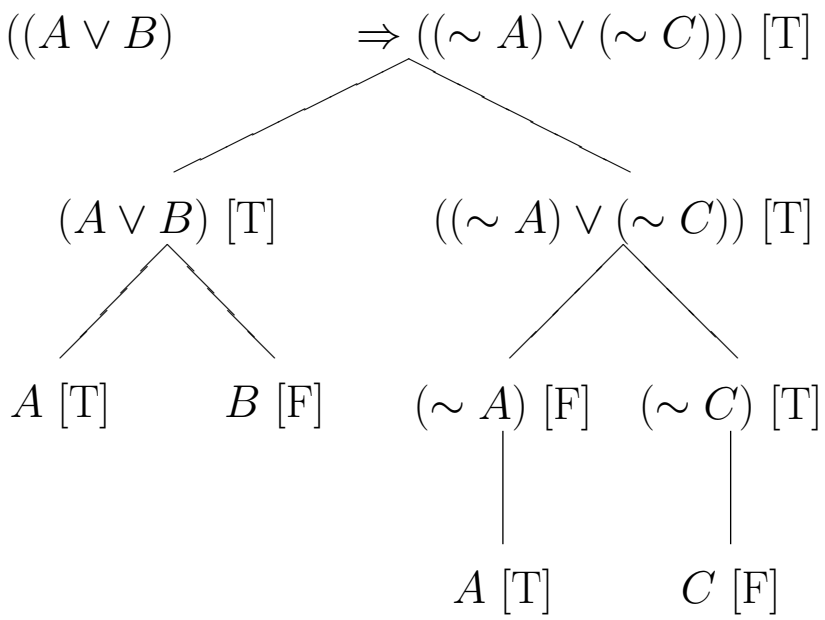
$$(A \vee (\sim (\sim B)))$$

would have the truth value T, since A is true and it is a disjunction of A with something.

For more complicated formulas, it is useful to break it down by subformula:

Example - using trees Consider the formula: $((A \vee B) \Rightarrow ((\sim A) \vee (\sim C)))$

Here is a "tree" representation we label the tree nodes (from the bottom-up) with truth values:



We can also do this using the other method of parsing formulas:

Consider: $\underbrace{(\underbrace{(A \vee B)} \Rightarrow (\underbrace{(\sim A)} \vee \underbrace{(\sim C)}))}$

Instead of underbracing, let's assign truth values, in the same order:

First: $((\underset{T}{A} \vee \underset{F}{B}) \Rightarrow ((\sim \underset{T}{A}) \vee (\sim \underset{F}{C})))$

Then: $((\underset{T}{A} \underset{T}{\vee} \underset{F}{B}) \Rightarrow ((\underset{F}{\sim} \underset{T}{A}) \vee (\underset{T}{\sim} \underset{F}{C})))$

Then: $((\underset{T}{A} \underset{T}{\vee} \underset{F}{B}) \Rightarrow ((\underset{F}{\sim} \underset{T}{A}) \underset{T}{\vee} (\underset{T}{\sim} \underset{F}{C})))$

Therefore: $((\underset{T}{A} \underset{T}{\vee} \underset{F}{B}) \underset{T}{\Rightarrow} ((\underset{F}{\sim} \underset{T}{A}) \underset{T}{\vee} (\underset{T}{\sim} \underset{F}{C})))$

Exercise: verify that in the model with A, B, and C all True, this formula is false.

Remark on *truth tables*

A formula could be true in some models, not true in others.

In particular, *without specifying a model it makes no sense to say that a WFF is true or false!*

Some formulas are true in *every* model.

Example: $(A \vee (\sim A))$

Definition: A WFF ϕ is *valid* if it is true in every model, i.e., if $\mathcal{M} \models \phi$ for every assignment of truth values to proposition letters.

5.2.1 Truth tables

Truth tables are useful tools to look at the behavior of a formula in all possible models. Each column is headed by a subformula of the formula being considered, with the simplest formulas (the proposition letters that appear in this formula). The rows contain all possible assignments of truth values to the proposition letters, and then the corresponding truth values of the subformulas are determined in increasing order of complexity.

If the column of truth values below the final formula consists entirely of **T**, then the formula is valid (or - in the book's terminology, a "tautology")

$$(A \vee (\sim A))$$

A	$(\sim A)$	$(A \vee (\sim A))$
T	F	T
F	T	T

(A tautology - the *law of excluded middle*)

The Basic Connectives

A	$(\sim A)$
T	F
F	T

A	B	$(A \Rightarrow B)$
T	T	T
T	F	F
F	T	T
F	F	T

A	B	$(A \vee B)$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$(A \wedge B)$
T	T	T
T	F	F
F	T	F
F	F	F

Equivalence

A	B	$(\sim B)$	$(\sim A)$	$((\sim B) \Rightarrow (\sim A))$
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

Note that $(A \Rightarrow B)$ and its contrapositive

$$((\sim B) \Rightarrow (\sim A))$$

have the same truth values in all combinations of the proposition letters.

When two formulas have the same truth values - in other words, behave the same under all assignments of truth values - they are called *logically equivalent* (or just *equivalent*). We could use the $\equiv$ symbol for this, for example,

$$(A \Rightarrow B) \equiv ((\sim B) \Rightarrow (\sim A)).$$

An implication is logically equivalent to its contrapositive.

Everyone should look at the text for a discussion of the relationship of the statement $A \Rightarrow B$, its contrapositive, and its *converse*

$$B \Rightarrow A$$

More Examples

1. Show $(\sim (A \vee B)) \equiv (\sim A \wedge \sim B)$
   (a "DeMorgan Law")

2. $A \Rightarrow (B \Rightarrow A)$

3. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

4. $\sim\sim A \Rightarrow A$

5. Which of the following are valid? For those that are *not*, give a model in which they do not hold.

   (a) $(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$

   (b) $(((A \vee B) \wedge \sim A) \Rightarrow B)$

   (c) $(A \Rightarrow (\sim A \vee B))$

Question: If a formula has N proposition letters, how many rows will the truth table have?

Remark: More compact truth tables.

5.2.2 Applications: Deduction Rules

The text (3.6) introduces a way to test the validity of some *argument forms*.

These provide a template, where, from certain hypotheses (called here *premises*), a *conclusion* can be drawn.

Example: If I am a mathematician then I eat kittens. I am a mathematician. Therefore I eat kittens.

This is an example of *modus ponens*.

It can be represented in a general way as follows:

$$\begin{array}{l} A \Rightarrow B \\ \underline{A \qquad\qquad} \\ \therefore B \end{array}$$

Here $A \Rightarrow B$ and A are the premises, B is the conclusion.

A and B can just be proposition letters, or could stand for more complex well-formed-formulas.

When written in this "propositional logic" form, we sometimes call such an argument form a *deduction rule*.

You **will not** be required to know these deduction rules by name, or even at all (except maybe modus ponens, which every educated human should know by name).

Another common rule is *modus tollens*:

$A \Rightarrow B$

$\underline{\sim B \qquad\qquad}$

$\therefore \sim A$

This is the basis of what we sometimes call *Proof By Contradiction*

There are a couple of ways to use truth tables to check the validity of such arguments.

Text: Test validity of

$$Premise1 \wedge Premise2 \wedge Premise2 \cdots \wedge PremiseN) \Rightarrow Conclusion$$

Here's another way:

- Form a truth table containing all premises, the conclusion, and all subformulas of these formulas.
- Delete rows in which any premise fails, leaving all and only rows where every premise is true.
- If the conclusion is true in *all* of the remaining rows, then it is a valid deduction rule, otherwise it is not.

(Note the resemblance to the tennis example!)

Example: Verify that modus ponens is valid:

A	B	$(A \Rightarrow B)$	
T	T	T	
T	F	F	$\longleftarrow$ (delete this row)
F	T	T	$\longleftarrow$ (delete this row)
F	F	T	$\longleftarrow$ (delete this row)

Example: Verify that the following nameless deduction rule is sound:

$A \Rightarrow B$

$\sim B \vee C$

$\underline{\sim C \qquad\qquad}$

$\therefore \sim A$

A	B	C	$\sim B$	$\sim B \vee C$	$\sim C$	$\sim A$
T	T	T				
T	T	F				
T	F	T				
T	F	F				
F	T	T				
F	T	F				
F	F	T				
F	F	F				

Example: Is this deduction rule valid?

$A \Rightarrow B$

$\underline{B \qquad\qquad}$

$\therefore A$

A	B	$(A \Rightarrow B)$
T	T	T
T	F	F
F	T	T
F	F	T

A Lewis Carroll example

a) All babies are illogical.

b) Nobody is despised who can manage a crocodile.

c) Illogical persons are despised.

Let proposition letters stand for propositions within the syllogism:

B= one is a baby

L= one is logical

M= one can manage a crocodile

D= one is despised

Carroll's words can now be translated into formulas:

a') $B \Rightarrow (\sim L)$

b') $M \Rightarrow (\sim D)$

c') $(\sim L) \Rightarrow D$

And (next page) a truth table:

B	L	M	D	$(\sim L)$	$(\sim D)$	$B \Rightarrow (\sim L)$	$M \Rightarrow (\sim D)$	$(\sim L) \Rightarrow D$
T	T	T	T					
T	T	T	F					
T	T	F	T					
T	T	F	F					
T	F	T	T					
T	F	T	F					
T	F	F	T					
T	F	F	F					
F	T	T	T					
F	T	T	F					
F	T	F	T					
F	T	F	F					
F	F	T	T					
F	F	T	F					
F	F	F	T					
F	F	F	F					

6 Divisibility and prime numbers

> God may not play dice with the universe, but something strange is going on with the prime numbers. (Paul Erdoš)

For $a, b \in \mathbb{Z}$, say that a *divides* b, or b is *divisible* by a, if $b = an$ for some $n \in \mathbb{Z}$.

Notation: Write $a|b$ if a divides b

We sometimes say that b is a *multiple* of a, or a is a *divisor* of b

In the logic shorthand:

$$\forall a, b \in \mathbb{Z}\big(a|b \text{ if and only if } \exists n \in \mathbb{Z}(an = b)\big)$$

Convention: 0 is divisible by everything, but does not divide anything: $\forall a\ a|0$ but $\forall a\ 0 \nmid a$

Examples: $3|27,\ 4 \nmid 10,\ 2|$any even number

1 has only one divisor, 2 has two divisors (1 and 2), 20 has 6 divisors $\{1, 2, 4, 5, 10, 20\}$, 0 has infinitely many divisors.

Definition 6.1. *A natural number $p > 1$ is a* prime number *provided it is only divisible by itself and* 1

In other words,

$$p > 1 \text{ is prime } \iff \forall n(n|p \implies n = 1 \text{ or } n = p)$$

Equivalently, a prime is a natural number with exactly two divisors.

A natural number > 1 which is not prime is called *composite* (or simply *nonprime*).

Examples: $2, 3, 5, 7, 11, 13, 17$ are all prime. So is $2^{24036583} - 1$ (this has 7235733 digits, and is a *Mersenne* prime).

Convention 0 and 1 are not prime numbers, but we usually don't call them composite numbers either.

Some important facts about primes:

Euclid's theorem There are infinitely many primes. (Book IX, Proposition 20)

Fundamental Theorem of Arithmetic Every natural number greater than 1 can be written as the product of primes numbers; moreover, this *prime representation* is unique in

the sense that any other such representation is just obtained by writing the same primes in a different order.

Prime Number Theorem The number of primes between 2 and N is "asymptotically"

$$\frac{N}{\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{N}}$$

Equivalently, if P_N is the N^{th} prime, then P_N is asymptotically approximately

$$N \times (\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\cdots+\frac{1}{N})$$

Division Algorithm: Suppose a and d are positive integers; then there is a unique $k \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$.

(a is the *dividend*, d the *divisor*, k the *quotient* of a by d, and r the *remainder*)

Euclidean Algorithm: Later (needs more terminology!)

Some things to look up on your own: Illegal primes, Sieve of Eratosthenes, Primality test, Prime Number Bear (NSFW!)

7 Some useful facts about divisibility

Recall: $a|b$ means a divides b, or b is divisible by a

Lemma 7.1. *Let $a, b, c \in \mathbb{Z}$. Then:*

1. *If $a|b$ and $a|c$ then $a|(b+c)$*
2. *If $a|b$ and $a|c$ then $a|(b-c)$*
3. *If $a|b$ then $a|(bc)$*
4. *If $a|b$ and $b|c$ then $a|c$*
5. *If $a|b$ and $b|a$ then $a = \pm b$*
6. *If $a|b$ and a and b are both > 0 then $a \leq b$*
7. *If $m \neq 0$ and $a|b$ then $(am)|(bm)$*

Questions:

Why did we avoid division? (Or *did* we?)

What properties of arithmetic are used in the proofs?

Discuss the path from definition to assertion to proof.

What is the difference between a 'Lemma' and a 'Theorem'?

Lemma 7.2. *Let $a \in \mathbb{Z}, a > 1$. Then a has at least one prime divisor.*

Remark: A prime divisor is sometimes called a *factor*.

Proof. Class. □

8 Euclid's theorem

This will be an example of *Proof by Contradiction* (or *reductio ad absurdum*).

Idea: To prove a statement **S**, first assume that **S** is *false*.

Next: Show that this assumption (of **S**'s falsity) leads to something which is *indisputably* false (eg, "0=1"). At this point we often say "This is a contradiction"

Conclude: That **S** must in fact be true.

Remarks:

Let P, Q, R be statements

Modus Tollens: From $P \implies Q$ and $\sim Q$ infer $\sim P$. (In this case, put $P = \sim S$ and $Q =$ the contradiction.)

Contrapositive: The statement $P \implies Q$ is logically equivalent to its contrapositive $(\sim Q) \implies (\sim P)$.

Theorem 8.1. *(Euclid) There are infinitely many primes.*

Proof. Suppose instead there are only *finitely* many primes: $2, 3, 5, 7, 11, \ldots, p_N$

Form the number

$$M = (2 \times 3 \times 5 \times 7 \times 11 \times 13 \times \cdots \times p_N) + 1$$

M has a prime factor, p.

p must be one of the primes in the list, so

$$p|(2 \times 3 \times 5 \times \cdots \times p_N)$$

Then $p|(M - (2 \times 3 \times 5 \times \cdots \times p_N))$, i.e., $p|1$

This is a contradiction (since the only positive divisor of 1 is itself).

□

Corollary 8.1. *Let* $\{p_1, p_2, p_3, \ldots, p_N\}$ *be any finite set of primes. Then any prime factor of* $(p_1 \times p_2 \times p_3 \times p_4 \times p_5 \cdots \times p_N) + 1$ *is different from* $p_1, \ldots, p_n$

Proof. This is the 'middle part' of the proof of Euclid's Theorem. □

9 Digression: Theorems and Proofs

Comments on mathematical THEOREMS:

A *theorem* is a declarative assertion of a mathematical truth.

It generally has some initial statements, called *hypotheses*, which we assume are true just for this context of the theorem. These typically take forms such as: "Let p be a prime number..." or "If m and n are integers..." or "Suppose $x^2 + 2x + 1 = 0$..." (etc.)

Note that the hypotheses might assert something about some variables or other mathematical objects.

It ends with one or more statements, called *conclusions*.

Sometimes the statemet of a theorem is hard to parse into hypotheses and conclusions.

Conceptually, the form is:

IF *hypotheses* THEN *conclusion*(*s*).

The terms THEOREM, LEMMA, PROPOSITION, COROLLARY are all roughly synonymous; the difference is the depth or difficulty of the argument:

theorems are major assertions

lemmas are less major assertions, usually just used as tools in proving theorems

propositions are relatively simple assertions, sometimes nearly obvious

corollaries follow in a straightforward way either from the statement or proof of another statement (theorem, lemma, proposition, or other corollary)

Theorems are usually introduced with word 'Theorem' (or 'Lemma' etc) and are set off from the subsequent *proof* by means of space, different fonts, or some other way.

Comments on mathematical PROOF:

We will see several kinds of proofs this term. The simplest is *direct proof*

A direct proof takes the form of a sequence of assertions.

Sometimes these assertions are just a succession of sentences in English, sometimes they are equations or other statements expressible in purely mathematical notation, sometimes a mixture.

Every assertion should be either:

1. A hypothesis of the theorem.
2. A 'basic' fact of mathematics, property of arithmetic or geometry or logic, etc. (An *axiom*.)
3. Something that follows 'logically' from the earlier assertions.

The last assertion should be the theorem's conclusion.

Most proofs are variants of direct proof.

Corollary 10.1. *If N is composite than N has a prime factor $\leq \sqrt{N}$*

Proof. Class □

Lemma 10.1. *If p is a prime number and m, n are positive integers and $p|mn$ then either $p|m \vee p|n$*

(Recall: If P and Q are assertions [="propositions"] then "$P \vee Q$" means: either P is true OR Q is true *OR BOTH*.)

Proof. Class □

11 GCF, LCM, Division and Euclidean Algorithms

Definition 11.1. *Let* $A, B \in \mathbb{N}$

LCM: *The least common multiple of* A *and* B, $LCM(A, B)$, *is the smallest* M *such that* $A|M$ *and* $B|M$.

GCF: *The greatest common divisor of* A *and* B, $GCF(A, B)$, *is the largest* D *such that* $D|A$ *and* $D|B$.

Examples (and finding LCM, GCF using Fund. Thm. of Arith.)

Remember the Division Algorithm:

Lemma 11.1. *Suppose a and d are positive integers; then there are unique $k, r \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$*

Proof. 'Sketch' in class. □

Lemma 11.2. *Suppose $a, k, d, r \in \mathbb{N}$ and $a = kd + r$. Then GCF(a, d)=GCF(d, r)*

Proof. Every common divisor of a and d is also a divisor of $a-kd$ (why?), which is r. Every common divisor of d and r is also a divisor of $kd+r$ (why?), which is a. Thus the largest common divisor of a and d must be the largest common divisor of d and r □

This lemma has remarkable consequences if we iterate the Division Algorithm. For example:

$$100 = (70)(1) + 30$$
$$70 = (30)(2) + 10$$
$$30 = (10)(3) + 0$$

At this point we have to stop, but see:

$$GCF(100, 70) = GCF(70, 30) = GCF(30, 10) = 10$$

This procedure for finding the GCF of two positive integers is called the **Euclidean Algorithm**.

12 Number Theory Concluded

Let's review the progression of the results so far:

- We defined the notion of *prime* and *composite* numbers, and set out to understand how numbers are constructed in terms of primes (ultimate goal: the Fundamental Theorem of Arithmetic)
- Introduced the basic notion of divisibility, introduced the notation $|$, and enumerated a list of properties for the operation $|$.
- Started proving increasingly "deep" results about primes and divisibility. The proof of a given result often relied on ones that came before. Often of the results were useful for concrete operations.

  Some of the results:

  1. Every positive integer has at least one prime divisor.
  2. Every positive number N has at least one prime divisor $\leq \sqrt{N}$. (This one is useful in practice, for testing primality.)
  3. There are infinitely many primes. (Intro-

duced the notion of *proof by contradiction.*)

4. Division algorithm: *Suppose a and d are positive integers; then there are unique $k, r \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$.*
5. Defined LCM and GCF. Showed how the division algorithm could be turned into a procedure for finding the GCF of two numbers (*Euclidean Algorithm*)
6. For any $M, N \in \mathbb{Z}^+$, there is $r, s \in \mathbb{Z}$ such that $rM + sN = GCF(M, N)$. (This followed by tracing the Euclidean algorithm backwards.)
7. Used this fact to prove: If p prime and $p|(mn)$ then $p|m$ or $p|n$
8. Did some applications (clock arithmetic, irrationality of $\sqrt{2}$).

General observations:

Only the proof of the Fundamental Theorem of Arithmetic is left.

The progression from *definition* (which is meant to make an intuition rigorous) to the final result had no holes or guesses; everything was proved rigorously. This process of *Deductive Proof* is what sets mathematical reasoning apart from most other forms of reasoning.

While the final goal (FTA) has no obvious applications, along the way it spun off a useful algorthm (Euclidean Algorithm), and results like the one in line (6) which are at the heart of RSA cryptography.

13 The hierarchy of number systems

God made the integers, all else is the work of man.

– Leopold Kronecker (1823-1891)

- Start with 0
- As soon as we can add 1 (the successor function) we get all of $\mathbb{N}$
- In $\mathbb{N}$ we can define addition and multiplication, but we can't subtract (without sometimes leaving $\mathbb{N}$)
- So: to get subtraction we move to $\mathbb{Z}$, the integers. (Axioms later.)
- In $\mathbb{Z}$ we can add, subtract, and multiply.
- $\mathbb{Z}$ is the smallest set of numbers extending $\mathbb{N}$ in which we can do this.
- However in $\mathbb{Z}$ we can't divide. (For example $5 \div 3$ is not an integer.)

- So: to get division we move to $\mathbb{Q}$, the rational numbers. (Axioms later.)
- In $\mathbb{Q}$ we can add, subtract, multiply, and divide (except by 0).
- $\mathbb{Q}$ is the smallest set of numbers extending $\mathbb{Z}$ in which we can do this.

Question: What can't we do in $\mathbb{Q}$?

Answer (if you're an electronic calculator): Nothing.

Answer (if you're not a calculator): Plenty

Example: $\sqrt{2}$ is irrational (="not rational").

(Equivalently: there is no rational number whose square is 2.)

(Pythagoras: "The side of a square and its diagonal are not commensurate.")

Ubiquity of rationals: Between any two distinct numbers (rational or irrational) there is another rational number. (That is, $\mathbb{Q}$ is *dense*.)

Ubiquity of irrationals: Between any two distinct numbers there is an irrational number. (That is, $\mathbb{R} - \mathbb{Q}$ is dense.)

14 Digression: what are natural numbers really

We all know how to use natural numbers, integers, etc., but what are they?

Modern solution: write down axioms we believe they satisfy, then produce a 'model' of the set of numbers which shows that the axioms are consistent.

For example, here is a formal definition of the Natural Numbers; it uses two special symbols, a symbol for 0 and a symbol s where $s(x)$ is meant to be the 'successor' of x (i.e., $x + 1$):

Peano Postulates

1. (0 is not the successor of anything)
   $\forall x\ (0 \neq s(x))$
2. (different natural numbers have different successors)
   $\forall x \forall y\ ((x \neq y) \Rightarrow (s(x) \neq s(y)))$
3. (every natural number other than 0 has an immediate predecessor)
   $\forall x\ ((x \neq 0) \Rightarrow \exists y\ (x = s(y)))$
4. (dominos[1]) For *any* predicate $P(x)$, we have the axiom:

   $((P(0) \wedge \forall x(P(x) \Rightarrow P(s(x))) \Rightarrow \forall x P(x))$

[1] aka induction

Remarkably, this is enough to do anything we might want to do in $\mathbb{N}$!

Examples:

Any natural number can be represented, for example 17 is represented by

$s(s(s(s(s(s(s(s(s(s(s(s(s(s(s(s(s(0)))))))))))))))))$

Addition can be defined in terms of successor:

$x + 0 =_{def} x$

$x + s(y) =_{def} s(x + y)$

For example, $1 + 1 = 2$:

$2 + 2 = 4$:

The John von Neumann Natural Numbers

To use the Peano Postulates we really need to know that these formulas are consistent. The easiest way to show that they *are* is to build a 'model' with familiar objects that satisfy these postulates.

J. von Neumann (1903-1957) proposed the following model:

All the elements of this model are sets.

For 0 we take the emptyset, $0 =_{def} \emptyset$

For s we take the function $s(x) =_{def} x \cup \{x\}$

So:

$0 = \emptyset = \{\}$

$1 = s(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$

$2 = s(1) = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$

(or - if you prefer - $\{\emptyset, \{\emptyset\}\}$)

$3 = s(2) = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$

(or - if you prefer - $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$)

More Generally:

$n+1 = n \cup \{n\} = \{0, 1, 2, \ldots, n-1\} \cup \{n\} = \{0, 1, 2, \ldots, n\}$

Every "von Neumann" natural number is the set of its predecessors.

Note that the for any m and n in this model,

$$m < n \text{ if and only if } m \in n$$

(convince yourself that this is true!), moreover in this case

$$m \subset n.$$

Rationals and Repeating Decimals

Sometimes the digits in the decimal expansion of a number start repeating after a while.

Examples: 1. $0.3333333\ldots$

2. $1.17171717171717\ldots$
3. $47.19734023402340 23\ldots$
4. -12.45

Note: all the above are rational numbers

Example: $0.99999\cdots = 1$

Theorem $\forall x$ (x is a repeating decimal $\Rightarrow x \in \mathbb{Q}$)

Equivalently: $\forall x$ (x irrational $\Rightarrow x$ not a repeating decimal)

Proof: Clearly we can do to *any* repeating decimal what we did in the examples above.

Question: Is the converse true?

Is every number whose decimal representation does *not* repeat an irrational number?

Equivalently, does every rational number have a repeating decimal representation?

Theorem Yes.

Examples: 1. 47/2

2. 47/5

3. 47/25

4. 47/15

5. 12/7

Some Famous Irrational Numbers

$\sqrt{2}$

$\sqrt{p}$ (for any prime p)

$\pi \quad (= 3.14159265358979323846 \ldots)$

$e \quad (= 2.71828182845904523536028747135266249775 72 \ldots)$

ϕ (Phi, the *Golden ratio*) The positive solution to the following remarkable quadratic equation:

$$\phi^2 - \phi - 1 = 0$$

$(= 1.61803398874989484820458683436563811772030 9 \ldots)$

Any number of the form $p+qz$ where z irrational, $p, q \in \mathbb{Q}$ and $q \neq 0$

$0.10100100010000100000100000010000000 1 \ldots$

$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \frac{1}{5^3} + \cdots$ ("Zeta of 3")

$(= 1.20205690315959428539973816151144999076 \ldots)$

$\zeta(n) = \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \cdots$ is *Riemann's Zeta Function*, and is connected to one of the most important open problems (the *Riemann Hypothesis*, formulated in 1859).

That $\zeta(3)$ is irrational has only been known since 1979

We still don't know many things about $\zeta(3)$, including whether it is *algebraic* (next lecture)

14.1 Algebraic numbers

Two of our main examples were irrational because they solved simple equations:

$$\sqrt{2} \text{ satisfies } x^2 = 2$$

$$\phi \text{ satisfies } \phi^2 - \phi - 1 = 0$$

Question: Is *this* why we need the reals? To be able to solve equations?

Recall: A *polynomial* is a function that looks like:

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0$$

$a_0, a_1, \ldots, a_n$ are the *coefficients* of the polynomial. Usually assume the *leading coefficient* $a_n \neq 0$

Question: If $p(x)$ is a polynomial, when does the equation $p(x) = 0$ have a solution?

$p(x) = ax + b$ (*linear* polynomial), then always.

$p(x) = ax^2 + bx + c$ (*quadratic* polynomial), then

$$p(x) = 0$$

is 'solved' by the *quadratic formula*:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

What about cubic? quartic? quintic?

A brief history of solving polynomial equations

much stolen from:
http://www-history.mcs.st-andrews.ac.uk/history/index.html

Quadratic equation:

$$a_2x^2 + a_1x + a_0 = 0$$

400BC Babylonians could solve some problems that *we* would formulate as quadratic equations.

300BC Euclid: geometric solutions of some problems involving roots, that (again) *we* would formulate as quadratic equations.

628 Brahmagupta (in *Brahmasphutasiddhanta*, or The Opening of the Universe): solves relatively general quadratic equations

830 Abu Ja'far Muhammad ibn Musa al-Khwarizmi (member of the Banu Musa, scholars at the House of Wisdom in Baghdad), in *Hisab al-jabr w'al-muqabala*: specific (numerical) examples of several categories of quadratic equations, using geometric and algebraic methods (though all in words).

> *That fondness for science,...that affability and condescension which God shows to the learned, that promptitude with which he protects and supports them in the elucidation of obscurities and in the removal of difficulties, has encouraged me to compose a short work on calculating by al-jabr and al-muqabala , confining it to what is easiest and most useful in arithmetic.*

[al-jabr means "restoring", referring to the process of moving a subtracted quantity to the other side of an equation; al-muqabala is "comparing" and refers to subtracting equal quantities from both sides of an equation.]

113?CE Abraham bar Hiyya Ha-Nasi (aka Savasorda), in Hibbur ha-Meshihah ve-ha-Tishboret (Treatise on Measurement and Calculation); first published complete solution of the quadratic.

Cubic equations:

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \quad (a_3 \neq 0)$$

Quartic equations:

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \quad (a_4 \neq 0)$$

(c.f.
www.sosmath.com/algebra/factor/fac111/fac111.html
to see what cubic solution looks like)

1494 Fra Luca Pacioli *Summa de arithmetica, geometrica, proportioni et proportionalita*, shows the *quartic* $x^4 = a + bx^2$ can be solved by quadratic methods...

...but asserts $x^4+ax^2 = bandx^4+a = bx^2$ are impossible (why?), also says that the *cubic* cannot be solved in general.

1515 Scipione dal Ferro, University of Bologna, solves equations of form $x^3 + mx = n$, but keeps solution secret.

(This can be used to solve *all* cubics if you are comfortable with manipulating negative numbers.)

1526 dal Ferro dies, reveals solution on deathbed to his student Antonio Fior, who is evidently a braggart.

1535 Nicolo of Brescia, known as Tartaglia, thus learns that dal Ferro had the solution, and figures out what it must be. He then announces that he too can solve the cubic (without revealing his solution). Fior challenges him to a competition, each posing 30 problems to the other. Fior cannot solve any of the problems Tartaglia sets, but Tartaglia figures out a generalization of the basic solution, and solves all of Fior's problems instantly.

1539 Girolamo Cardano (illegitimate son of a lawyer/geometer who was a friend of da Vinci, and himself a doctor/mathematician) tries to get the solution from Tartaglia for a book in progress. He agrees he will only publish the method after Targaglia has a chance to publish it first, and swears:

> *I swear to you, by God's holy Gospels, and as a true man of honour, not only never to publish your discoveries, if you teach me them, but I also promise you, and I pledge my faith as a true Christian, to note them down in code, so that after my death no one will be able to understand them.*

1545 Cardano published *Ars Magna*, including solutions of both cubics and quartics (the latter mainly due to his student Lodovico Ferrari).

1673 Gottfried Wilhelm von Leibniz gives the easiest possible proof that the Cartan solutions actually work. (Class: show idea for quadratic.)

Casus Irreducibilis: Fior, Tartaglia, especially Cartan all noticed: even if a cubic has all three real roots, to solve for them algebraically you must take roots of nonreal numbers numbers at some point. Cartan called this the *casus irreducibilis*. Modern methods show that this is unavoidable.

Quintic: The 5th degree equation

$$a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=0, \qquad a_5\neq 0$$

definitely has a solution:

1799 Paolo Ruffini announces the general quintic *cannot* be solved algebraically. Proof contains gaps, and announcement is largely ignored, but estabishes many mathematical facts that are later used.

1824 Niels Henrik Abel produces first correct proof of this unsolvability. Not published until well after his death.

1830++ Evariste Galois establishes a general algebraic theory which not only includes Abel's proof, but also a general framework for determining whether a given equation has an algebraic solution. His various papers on the subject get lost, rejected for spurious reasons, etc.

1831 French revolution. Galois arrested, tried, acquitted. Arrested again on Bastille day, while in prison learns his most important paper rejected for being badly written.

1832 Galois falls in love with daughter of prison physician. After release from prison tries to pursue her, is apparently rebuffed. Fights duel, possibly connected with her, is killed.

1843 French Academy of Science finally acknowledges Galois work as important, his papers get published in 1848.

Galois Theory and Impossibility:

Impossibility of solving the quintic.

Impossibility of trisecting an angle.

Definition: A number is *algebraic* if it is a solution to an equation of the form $p(x) = 0$, where $p(x)$ is a polynomial with integer coefficients.

A real number is *transcendental* if it is not algebraic.

Examples: 1. $-13/17$

2. $\sqrt{2}; \quad \phi; \quad 2^{\frac{1}{4}}$
3. $\sqrt{3-\sqrt{2}}$
4. $\sqrt{5}+\sqrt{7}$

So....why $\mathbb{R}$?

Start with a 'typical' real number, say $\pi = 3.1415926\ldots$

Approximate: $3, 3.1, 3.14, 3.141, 3.1415, \cdots$

Note that these rational approximations are *increasing*, and *bounded above* (by 4, for example).

Another example (*continued fraction*):

$$\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}$$

Approximate: $1, \frac{1}{1+1}, \frac{1}{1+\frac{1}{1+1}}, \frac{1}{1+\frac{1}{1+\frac{1}{1+1}}}, \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+1}}}}, \ldots$

These rational approximations are *increasing*, and *bounded above* (by 1, for example).

This motivates the following operational definition:

The set $\mathbb{R}$ of *real numbers* is the smallest set which contains $\mathbb{Q}$ and satisfies the following property, the *least upper bound* (LUB) property:

If $\emptyset \not\subset A \subset \mathbb{R}$ and A is bounded above then there is a number a such that

(i) $\forall x(x \in A \Rightarrow x \leq a)$

(ii) $\forall y((\forall x(x \in A \Rightarrow x \leq y)) \Rightarrow a \leq y)$

Example $\frac{1}{1+\frac{1}{1+\frac{1}{1+\ldots}}}$ must be a real number. What number is it?

Problem: Even in $\mathbb{R}$ we can't solve some simple equations, such as:

$$x^2 + 1 = 0$$

Solution: Extend the system yet again, to the *Complex Numbers* $\mathbb{C}$

$\mathbb{C}$ will be is the smallest extension of $\mathbb{R}$ that satisfies the usual algebraic properties of $\mathbb{R}$ and also contains an 'imaginary' element representing $\sqrt{-1}$.

Remarkably, just throwing $\sqrt{-1}$ into the system makes it possible to solve *all* polynomial equations; this is the *Fundamental Theorem of Algebra*.

15 Probability and Statistics

15.1 Overview

The idea that probability is something we can study, analyze, and come to understand, is something relatively new:

> *Fate laughs at probabilities.*
> Bulwer Lytton

> *How dare we speak of the laws of chance? Is not chance the antithesis of all law?*
> Joseph Bertrand, Calcul des probabilités

While basic probability theory grew out of investigations by gamblers in the late 18th century, a modern, rigorous foundation is fairly new:

> *The theory of probability as a mathematical discipline can and should be developed from axioms in exactly the same way as geometry and algebra.*
> Andrey Kolmogorov

> *All possible definitions of probability fall short of the actual practice.*
> William Feller

Besides helping us gamble if we are so inclined, understanding probability can help avoid jumping to conclusions:

> *Coincidences, in general, are great stumbling blocks in the way of that class of thinkers who have been educated to know nothing of the theory of probabilities—that theory to which the most glorious objects of human research are indebted for the most glorious of illustrations.*
>
> Edgar Allen Poe, The Murders in the Rue Morgue

> *Lottery: A tax on people who are bad at math.*
>
> Anonymous

> *LAST NIGHT'S CHILLING LOTTERY WINNER: 9-1-1*
>
> NY Post Headline, 12 September 2002

Statistics is historically less-respected than probability:

> *There are three kinds of lies: lies, damned lies, and statistics.*
> Benjamin Disraeli

> *USA Today has come out with a new survey - apparently, three out of every four people make up 75% of the population.* David Letterman

> *Smoking is one of the leading causes of statistics.*
> Fletcher Knebel

What's the difference between probability and statistics?

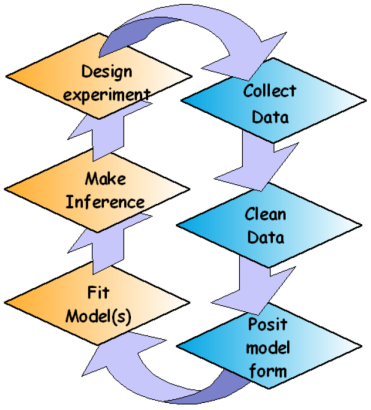
Assumption: Data Generating Mechanism (or model) $\longrightarrow$ Data (sample)

Probability Given complete knowledge about data generating mechanism, make assertions about the data.

Statistics Given the data, make inference about the data generating mechanism.

In practice, we move back and forth between data and model:

Model Creation Process



15.2 Elements of Probability

Probability space: $(\Omega, \mathcal{A}, P)$

Three basic elements: Sample Space Ω, Collection $\mathcal{A}$ of Events, Probability measure P

Sample Space:

Ω =Sample Space=set of all possible "elementary outcomes"

Events:

An *event* is a subset of Ω, so (usually) $\mathcal{A}$ =the set of all subsets of Ω (which we often denote by $\mathcal{P}(\Omega)$, the "power set" of Ω)

Probability:

$P\colon \mathcal{A} \to [0,1]$ assigns values between 0 (completely improbable) and 1 (certain) to events.

Examples:

1. Roll one die, 'obvious' sample space is

$\Omega = \{1,2,3,4,5,6\}$

Take $\mathcal{A}$ =all subsets of Ω

Typical event: "Roll is even"$= \{2,4,6\}$

If die is 'fair', reasonable to take $P(A) = \frac{n(A)}{6}$

Recall: $n(A)$ = the number of elements in A

$P(even) = P(\{2,4,6\}) = 3/6 = 1/2;$

$P(greater\ than\ 4) = P(\{5,6\}) = 2/6 = 1/3$

If die is 'loaded', might have some numbers more likely than others.

One way to assign probabilities is to assign each number i a probability $p_i,\ 1 \leq i \leq 6$

Then let

$$P(A) = \text{the sum of all the } p_i\text{'s with } i \text{ in } A$$

(later we'll see a notation for this, $\sum_{i \in A} p_i$)

EG: If we have the following assignment:

$i:$	1	2	3	4	5	6
$p_i:$	.1	.2	.1	.1	.1	.4

then:

$P(even) = .2 + .1 + .4 = .7;$

$P(greater\ than\ 4) = .1 + .4 = .5;$

$P(\Omega) = .1 + .2 + .1 + .1 + .1 + .4 = 1$

2. Throw *two* dice; some possible sample spaces are:

$$\Omega_1 = \begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\ (3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) \\ (4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) \\ (5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) \\ (6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) \end{array}$$

or

$$\Omega_2 = \begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\ & & (3,3) & (3,4) & (3,5) & (3,6) \\ & & & (4,4) & (4,5) & (4,6) \\ & & & & (5,5) & (5,6) \\ & & & & & (6,6) \end{array}$$

or

$$\Omega_3 = \{2, 3, 4, \ldots, 12\}$$

What are reasonable probability assignments for these different sample spaces?

Note: Look back at the notes from early in the semester for a review of ordered pairs, triples, n-tuples, and Cartesian products

EG: Roll 4 dice, number of different throws =?

EG: Roll 4 fair dice, what is the probability of them adding to 5?

EG: From a deck of cards, how many ways are there to pick one card from each suit?

EG: Four cards are dealt from a deck, what is P(all from different suits)

3. Throw a dart at a dartboard of radius R.

Ω =all points in a circle (including interior) of radius R

An event will be any subset A of Ω for which "area of A" makes sense.

$P(A) =_{def}$(area of A)$/(\pi R^2)$

EG: P(hit upper half of dartboard) $= 1/2$

EG: If 'bull's-eye' of dartboard is circle of radius r, where $r < R$, then P(hit bull's-eye) $= \frac{\pi r^2}{\pi R^2} = (\frac{r}{R})^2$

Properties of a probability measure. In the definition of "probability space", we impose the following additional requirements on the probability function P:

$P(\emptyset) = 0$

$P(\Omega) = 1$

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$ (picture)

Definition Events A, B are *disjoint* if $A \cap B = \emptyset$

Note: If A and B are disjoint then

$$P(A \cup B) = P(A) + P(B)$$

EG: A pair of fair dice are thrown, what is P(sum is odd or sum is 6)?

EG: A pair of fair dice are thrown, what is P(at least one die shows a 4)?

Definition: two events A and B are *independent* provided $P(A \cap B) = P(A)P(B)$

EG: Throw two dice, A =1st die even, B=2nd die even; independent?

EG: Throw two dice, A =1st die< 3, B ="sum of dice=11"; independent?

EG: In a class of 220, assuming that for a given person all birth dates are equally likely (and assuming leap years do not exist), find the probability that at least one student in the class has a birthday today.

Do the same for a class of 30.

For these two class sizes, find probability that two or more students share a birthday.

Odds ratios: If an event E has a probability $P(E) = p$ so the complement of E has probability $P(E') = 1 - p$, then the *odds ratio* (or just the *odds*) in favor of E is

$$\frac{P(\text{E happens})}{P(\text{E doesn't happen})} = \frac{p}{1-p}.$$

Sometimes we say something like "The odds in favor of E is p to $1 - p$."

Example: 8 of the 28 players on the roster of the Hull City Tigers Football Club (a soccer team in the English Premier League) are English. If you pick one of the players at random, what are the odds that he's English?

Answer: 8 to 20 (or 2 to 5).

Example: If you pick one of the players at random, what are the odds *against* him being English?

Example: What is the *probability* that a randomly selected player is not English?

Note: Probabilities are always between 0 and 1, odds ratios can be any positive number.

Example: If you pick a player at random from the roster of the Newcastle United Football

Club (aka *the Toon*) the probability of his being English is 0.15. What are the *odds* of a randomly selected player being English?

A final application of probability: DNA testing

Statements from the news:

"The stain on White House intern Monica Lewinsky's dress was tested for DNA. Only 1 in 8 trillion people have this DNA profile."

"The most astronomical figures involved a pair of socks found near Simpson's bed. Cotton said one sock contained the DNA type of Simpson's slain ex-wife, Nicole Brown Simpson. Asked how many other whites shared that DNA type, Cotton said one in 9.7 billion. Prosecutor George Clark noted the figure was larger than the Earth's population, estimated at 5.5 billion, meaning that Ms. Simpson was literally the only person whose blood could be on that sock." (*USA Today*, 10-18-96)

What do such statements mean? Can we really use them to determine guilt from a DNA match?

Overview of DNA testing: DNA, Loci, markers (VNTR, STR, etc), profile

Procedure: Choose sites.

Estimate probability distributions at sites based on broad data (blood banks, etc)

Assumption: sites distant enough so measurements are independent.

Use independence (product rule) to determine probability of any given profile.

Example. If specify 4 sites, and each has 100 equally probable allele values, then probability of any given profile is $(1/100)^4$, or one in 100 million. If specify 10 sites, each with 20 equally probably values, then probability of any given profile is $(1/20)^{10}$, or about one in 10^{26}.

Note: The probablities for any locus are actually "confidence intervals" (whatever those are), so you might get a range of values, eg between $.009^4$ and $.011^4$ (or between one in $68,301,346$ and one in $152,415,790$).

The "Prosecutor's Fallacy"

A DNA sample from a crime is typed, and profile computed to have a one in one million probability. Then DNA from the defendant is typed, and has this same profile. Consider two statements:

(1) "There is only a 1 in a million chance the defendant is innocent"

(2) "The probability of obtaining this DNA profile from a randomly selected individual is 1 in a million."

These are *not* the same!

Statement (2) is correct (if our other estimates and assumptions are correct). Statement (1) is false.

Actual computation requires *conditional probability*:

$P(A|B)$ = The probability of A given that you know B is true

Statement (1) is really the assertion that
$P(\text{Defendant innocent} \mid \text{blood profile matched}) = 1/1000000$

but we don't yet know this conditional probability.

Bayes Theorem If A, B are events, then

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}$$

Let:

A =Defendant is innocent

A^c =Defendant is guilty

B =Defendant's blood matches the crime scene profile

and let $p = P(A^c)$ (which we don't know, but might have a preconception about). We know that $P(B|A) = 1/1000000, P(B|A^c) = 1$, so plug into Bayes Theorem, get:

$$P(A|B) = \frac{(1/1000000)(1-p)}{(1/1000000)(1-p) + p}$$
$$= \frac{1-p}{1 + 999999p}$$

this varies depending on what is the 'prior' probability p of guilt:

Measures of Central tendency

Suppose we have data points $x_1, x_2, x_3, \ldots, x_n$

There are three common ways to estimate the "middle" of the data:

Mean: The mean (or average) of $x_1, \ldots, x_n$ is

$$\bar{x} = \frac{x_1 + x_2 + \cdots + x_n}{n} = \frac{\sum_i x_i}{n}$$

Example:

Data: $6.2, 6.1, 8.2, 3.1, 8.7$

$$\bar{x} = \frac{6.2 + 6.1 + 8.2 + 3.1 + 8.7}{5} = \frac{32.3}{5} = 6.46$$

Median: The "middlemost" number:

i) If n is odd then the median=the value x_i such that half the numbers are $\geq x_i$, half $\leq x_i$
= the k^{th} largest number, where $k = \frac{n+1}{2}$

ii) If n is even then the median=the average of the two numbers in the middle

iii) Normally you need to sort the data to find the median.

Example:

Data: $6.2, 6.1, 8.2, 3.1, 8.7$; sorted: $3.1, 6.1, 6.2, 8.2, 8.7$

$$\text{median} = 6.2$$

Example:

Data: $6.2, 6.1, 9, 8.2, 3.1, 8.7$; sorted: $3.1, 6.1, 6.2, 8.2, 8.7, 9$

$$\text{median} = \frac{6.2 + 8.2}{2} = 7.2$$

Mode: The most common data point. (Normally not very interesting.)