... Let's assume there exists some function $F(a, b, c, \ldots)$ which produces the correct answer—hang on.

This is going to be one of those weird, dark-magic proofs, isn't it? I can tell.

What? No, no, it's a perfectly sensible chain of reasoning.

All right...

Now, let's assume the correct answer will eventually be written on this board at the coordinates $(x, y)$. If we—

I knew it!
Last class: Inference Rules for Quantifiers

\[
\begin{align*}
\text{Intro } \exists & \quad P(c) \text{ for some } c \\
\therefore & \quad \exists x \ P(x) \\
\text{Elim } \forall & \quad \forall x \ P(x) \\
\therefore & \quad P(a) \text{ for any } a
\end{align*}
\]

"Let a be arbitrary" \( \cdots \) \( P(a) \)
\[
\therefore \quad \forall x \ P(x)
\]

\[\text{Intro } \forall \]

\[\exists x \ P(x) \]
\[
\therefore \quad P(c) \text{ for some } \text{special } c
\]

* in the domain of \( P \). No other name in \( P \) depends on a

** c is a NEW name. List all dependencies for c.
Prove: “The square of every even number is even.”

Formal proof of: \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)

1. Let \( a \) be an arbitrary integer
   
   \[
   \begin{align*}
   2.1 & \quad \text{Even}(a) & \text{Assumption} \\
   2.2 & \quad \exists y \ (a = 2y) & \text{Definition of Even} \\
   2.3 & \quad a = 2b & \text{Elim } \exists: \ b \text{ special depends on } a \\
   2.4 & \quad a^2 = 4b^2 = 2(2b^2) & \text{Algebra} \\
   2.5 & \quad \exists y \ (a^2 = 2y) & \text{Intro } \exists \text{ rule} \\
   2.6 & \quad \text{Even}(a^2) & \text{Definition of Even}
   \end{align*}
   \]

2. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \) \quad \text{Direct proof rule}

3. \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \) \quad \text{Intro } \forall: 1,2
Law Proof: Even and Odd

Prove “The square of every even integer is even.”

Proof: Let \( a \) be an arbitrary even integer.  

1. Let \( a \) be an arbitrary integer \( \text{even integer.} \) \( \text{Assumption} \)

Then, by definition, \( a = 2b \) for some integer \( b \) (depending on \( a \)).

2. \( \exists y (a = 2y) \) \( \text{Definition} \)
2.3 \( a = 2b \) \( b \) special depends on \( a \)

Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \).  

2.4 \( a^2 = 4b^2 = 2(2b^2) \) \( \text{Algebra} \)

Since \( 2b^2 \) is an integer, by definition, \( a^2 \) is even.

2.5 \( \exists y (a^2 = 2y) \) \( \text{Definition} \)
2.6 \( \text{Even}(a^2) \)

Since \( a \) was arbitrary, it follows that the square of every even number is even.  

3. \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)
Prove “The square of every odd integer is odd.”

Pf. Let a be an arbitrary odd integer. Then, there exists b depending on a such that $2b + 1 = a$.

Therefore, by algebra, $(2b + 1)^2 = a^2$.

Thus, $a^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$.

Since $2b^2 + 2b$ is an integer, $a^2$ is odd.

$a^2$ is odd

Because a was arbitrary, the square of any odd integer is odd.
Prove “The square of every odd integer is odd.”

**Proof:** Let \( b \) be an arbitrary odd integer. Then, \( b = 2c+1 \) for some integer \( c \) (depending on \( b \)). Therefore, \( b^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1 \). Since \( 2c^2 + 2c \) is an integer, \( b^2 \) is odd. Since \( b \) was arbitrary, the square of every odd integer is odd. ■
Proof Strategies: Counterexamples

To *disprove* $\forall x \ P(x)$ prove $\exists_x \neg P(x)$:

- Works by de Morgan’s Law: $\neg \forall x \ P(x) \equiv \exists x \neg P(x)$
- All we need to do that is find a $c$ for which $P(c)$ is *false*
- This example is called a *counterexample* to $\forall x \ P(x)$.

**e.g. Disprove “Every prime number is odd”**

Find a prime number that is not odd

$\neg \forall x, \ \text{Prime}(x) \Rightarrow \text{odd}(x)$

$\equiv \exists x \neg (\text{Prime}(x) \Rightarrow \text{odd}(x))$

$\equiv \exists x \neg (\neg \text{Prime}(x) \vee \text{odd}(x))$
Proof Strategies: Proof by Contrapositive

If we assume \( \neg q \) and derive \( \neg p \), then we have proven \( \neg q \rightarrow \neg p \), which is equivalent to proving \( p \rightarrow q \).

1.1. \( \neg q \) Assumption

... 

1.3. \( \neg p \) 

1. \( \neg q \rightarrow \neg p \) Direct Proof Rule

2. \( p \rightarrow q \) Contrapositive: 1
Proof by Contradiction: One way to prove $\neg p$

If we assume $p$ and derive $F$ (a contradiction), then we have proven $\neg p$.

1. $p$ Assumption

\[ \neg \neg p \equiv T \rightarrow F \]

2. $\neg p \lor F$ Law of Implication: 1

3. $\neg p$ Identity: 2
Prove: “No integer is both even and odd.”

English proof:

\[ \neg \exists x (\text{Even}(x) \wedge \text{Odd}(x)) \equiv \forall x \neg (\text{Even}(x) \wedge \text{Odd}(x)) \]

pf. Let \( a \) be an arbitrary integer. We prove by contrapositive.

Assume \( a \) is even and odd. (*)

Since \( a \) is even, \( a = 2b \) for some \( b \) depending on \( a \).

Since \( a \) is odd, \( a = 2c + 1 \) for some \( c \) depending on \( a \).

Thus, \( 2b = 2c + 1 \). So, \( b = c + \frac{1}{2} \).

No two integers differ by \( \frac{1}{2} \). Contradiction. (*) is False.

\( a \) is not both even and odd.

Since \( a \) was arbitrary, no integer is both even and odd.
Prove: “No integer is both even and odd.”

English proof:  ¬ ∃x (Even(x) ∧ Odd(x))

≡ ∀x ¬(Even(x) ∧ Odd(x))

Proof: We work by contradiction. Let c be an arbitrary integer and suppose that it is both even and odd. Then c=2a for some integer a (depending on c) and c=2b+1 for some integer b (depending on c). Therefore 2a=2b+1 and hence a=b+½.

But two integers cannot differ by ½ so this is a contradiction. So, no integer is both even and odd. ■
Rational Numbers

- A real number $x$ is *rational* iff there exist integers $p$ and $q$ with $q \neq 0$ such that $x = p/q$.

Rational($x$) $\equiv \exists p \exists q \ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land q \neq 0)$

\[
\frac{2}{3} \quad \frac{10}{5} \quad \frac{3}{0}
\]
Prove: “If $x$ and $y$ are rational then $xy$ is rational.”

Predicate Definitions

\[
\text{Rational}(x) \equiv \exists p \ \exists q \ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))
\]
Prove: “If x and y are rational then xy is rational.”

**Proof:** Let x and y be rational numbers. Then, $x = a/b$ for some integers $a$, $b$, where $b \neq 0$, and $y = c/d$ for some integers $c,d$, where $d \neq 0$.

Multiplying, we get that $xy = (ac)/(bd)$.

Since $b$ and $d$ are both non-zero, so is $bd$; furthermore, $ac$ and $bd$ are integers. It follows that $xy$ is rational, by definition of rational.
Proofs

• Formal proofs follow simple well-defined rules and should be easy to check
  – In the same way that code should be easy to execute

• English proofs correspond to those rules but are designed to be easier for humans to read
  – Easily checkable in principle

• Simple proof strategies already do a lot
  – Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)
Set Theory

Sets are collections of objects called **elements**.

Write $a \in B$ to say that $a$ is an element of set $B$, and $a \notin B$ to say that it is not.

Some simple examples

- $A = \{1\}$
- $B = \{1, 3, 2\}$
- $C = \{\Box, 1\}$
- $D = \{\{17\}, 17\}$
- $E = \{1, 2, 7, \text{cat, dog, } \emptyset, \alpha\}$
Some Common Sets

\[\mathbb{N}\] is the set of **Natural Numbers**; \(\mathbb{N} = \{0, 1, 2, \ldots\}\)

\[\mathbb{Z}\] is the set of **Integers**; \(\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\)

\[\mathbb{Q}\] is the set of **Rational Numbers**; e.g. \(\frac{1}{2}, -17, 32/48\)

\[\mathbb{R}\] is the set of **Real Numbers**; e.g. \(1, -17, 32/48, \pi, \sqrt{2}\)

\([n]\) is the set \(\{1, 2, \ldots, n\}\) when \(n\) is a natural number

\(\{}\) = \(\emptyset\) is the **empty set**; the *only* set with no elements
Sets can be elements of other sets

For example
A = \{\{1\}, \{2\}, \{1, 2\}, \emptyset\}
B = \{1, 2\}

Then B \in A.
Definitions

• A and B are equal if they have the same elements

\[ A = B \equiv \forall x (x \in A \iff x \in B) \]

• A is a subset of B if every element of A is also in B

\[ A \subseteq B \equiv \forall x (x \in A \rightarrow x \in B) \]

• Note: \( (A = B) \equiv (A \subseteq B) \land (B \subseteq A) \)
Definition: Equality

A and B are **equal** if they have the same elements

\[ A = B \equiv \forall x (x \in A \leftrightarrow x \in B) \]

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

Which sets are equal to each other?
Definition: Subset

A is a *subset* of B if every element of A is also in B

\[ A \subseteq B \equiv \forall x (x \in A \rightarrow x \in B) \]

\[
\begin{align*}
A &= \{1, 2, 3\} \\
B &= \{3, 4, 5\} \\
C &= \{3, 4\}
\end{align*}
\]

**QUESTIONS**

- \( \emptyset \subseteq A? \) \( \checkmark \)
- \( A \subseteq B? \) \( \times \)
- \( C \subseteq B? \) \( \checkmark \)
Building Sets from Predicates

\[ S = \text{the set of all}^* x \text{ for which } P(x) \text{ is true} \]

\[ S = \{ x : P(x) \} \]

\[ S = \text{the set of all } x \text{ in } A \text{ for which } P(x) \text{ is true} \]

\[ S = \{ x \in A : P(x) \} \]

*in the domain of \( P \), usually called the “universe” \( U \)
Set Operations

\[ A \cup B = \{ x : (x \in A) \lor (x \in B) \} \]  \hspace{1cm} \text{Union}

\[ A \cap B = \{ x : (x \in A) \land (x \in B) \} \]  \hspace{1cm} \text{Intersection}

\[ A \setminus B = \{ x : (x \in A) \land (x \notin B) \} \]  \hspace{1cm} \text{Set Difference}

\begin{align*}
A &= \{1, 2, 3\} \\
B &= \{3, 5, 6\} \\
C &= \{3, 4\}
\end{align*}

**QUESTIONS**

Using A, B, C and set operations, make...

\[ [6] = A \cup B \cup C \]
\[ \{3\} = A \cap C \]
\[ \{1, 2\} = A \setminus B \]
More Set Operations

\[ A \oplus B = \{ x : (x \in A) \oplus (x \in B) \} \]

\[ \overline{A} = \{ x : x \notin A \} \]

(with respect to universe U)

A = \{1, 2, 3\}
B = \{1, 2, 4, 6\}
Universe:
U = \{1, 2, 3, 4, 5, 6\}

\[ A \oplus B = \{3, 4, 6\} \]
\[ \overline{A} = \{4, 5, 6\} \]

Symmetric Difference

Complement
It’s Boolean algebra again

• Definition for $\cup$ based on $\lor$

• Definition for $\cap$ based on $\land$

• Complement works like $\neg$
De Morgan’s Laws

\[ \overline{A \cup B} = \overline{A} \cap \overline{B} \]

\[ \overline{A \cap B} = \overline{A} \cup \overline{B} \]

Proof technique:
To show \( C = D \) show
\[ x \in C \rightarrow x \in D \] and
\[ x \in D \rightarrow x \in C \]
Distributive Laws

\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]
Power Set

• Power Set of a set $A = \text{set of all subsets of } A$

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

• e.g., let $\text{Days}=\{M,W,F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days})=?$$

$$\mathcal{P}(\emptyset)=?$$
Power Set

- **Power Set of a set** $A$ = set of all subsets of $A$

  \[ \mathcal{P}(A) = \{ B : B \subseteq A \} \]

- e.g., let $\text{Days}=$\{M,W,F\} and consider all the possible sets of days in a week you could ask a question in class

  \[ \mathcal{P}(\text{Days})=\{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \emptyset\} \]

  \[ \mathcal{P}(\emptyset)=\{\emptyset\} \neq \emptyset \]
Cartesian Product

\[ A \times B = \{ (a, b) : a \in A, b \in B \} \]

\( \mathbb{R} \times \mathbb{R} \) is the real plane. You’ve seen ordered pairs before.

These are just for arbitrary sets.

\( \mathbb{Z} \times \mathbb{Z} \) is “the set of all pairs of integers”

If \( A = \{1, 2\}, B = \{a, b, c\} \), then \( A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\} \).

\( A \times \emptyset = \{(a, b) : a \in A \land b \in \emptyset\} = \{(a, b) : a \in A \land F\} = \emptyset \)
Representing Sets Using Bits

- Suppose universe $U$ is $\{1, 2, \ldots, n\}$
- Can represent set $B \subseteq U$ as a vector of bits:
  \[ b_1 b_2 \ldots b_n \text{ where } b_i = 1 \text{ when } i \in B \]
  \[ b_i = 0 \text{ when } i \notin B \]
  - Called the *characteristic vector* of set $B$

- Given characteristic vectors for $A$ and $B$
  - What is characteristic vector for $A \cup B$? $A \cap B$?
UNIX/Linux File Permissions

• `ls -l`
  
  drwxr-xr-x ... Documents/
  -rw-r--r-- ... file1

• Permissions maintained as bit vectors
  – Letter means bit is 1
  – “–” means bit is 0.
## Bitwise Operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Binary</th>
<th>Java:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>⊕</code> (Exclusive OR)</td>
<td>01101101 ⊕ 00110111 = 01011010</td>
<td><code>z=x^y</code></td>
</tr>
<tr>
<td><code>∨</code> (OR)</td>
<td>01101101 ∨ 00110111 = 01111111</td>
<td>`z=x</td>
</tr>
<tr>
<td><code>∧</code> (AND)</td>
<td>00101010 ∧ 00001111 = 00001010</td>
<td><code>z=x &amp; y</code></td>
</tr>
</tbody>
</table>

**Explanation:**
- `⊕` (Exclusive OR) results in a 1 if the bits are different, and a 0 if they are the same.
- `∨` (OR) results in 1 if either of the bits is 1.
- `∧` (AND) results in 1 only if both bits are 1.
A Useful Identity

• If $x$ and $y$ are bits: $(x \oplus y) \oplus y = ?$

• What if $x$ and $y$ are bit-vectors?
Private Key Cryptography

- **Alice** wants to communicate message secretly to **Bob** so that eavesdropper **Eve** who hears their conversation cannot tell what **Alice**’s message is.
- **Alice** and **Bob** can get together and privately share a secret key **K** ahead of time.
One-Time Pad

- Alice and Bob privately share random n-bit vector \( K \)
  - Eve does not know \( K \)
- Later, Alice has n-bit message \( m \) to send to Bob
  - Alice computes \( C = m \oplus K \)
  - Alice sends \( C \) to Bob
  - Bob computes \( m = C \oplus K \) which is \( (m \oplus K) \oplus K \)
- Eve cannot figure out \( m \) from \( C \) unless she can guess \( K \)
Russell’s Paradox

\[ S = \{ x : x \not\in x \} \]

Suppose for contradiction that \( S \in S \)...
Russell’s Paradox

\[ S = \{ x : x \notin x \} \]

Suppose for contradiction that \( S \in S \). Then, by definition of \( S \), \( S \notin S \), but that’s a contradiction.

Suppose for contradiction that \( S \notin S \). Then, by definition of the set \( S \), \( S \in S \), but that’s a contradiction, too.

This is reminiscent of the truth value of the statement “This statement is false.”