... Let's assume there exists some function $F(a,b,c,...)$ 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!
Recap from last lecture: Inference proofs

Prove: “The square of every even number is even.”

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

Domain: Integers

Even\( (x) \equiv \exists y \ (x=2y) \)
Odd\( (x) \equiv \exists y \ (x=2y+1) \)
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
   
   2.1 \( \text{Even}(a) \) \quad \text{Assumpt.}
   
   2.2 \( \exists y \ (a = 2y) \) \quad \text{Def. Even}
   
   2.3 \( a = 2b \) \quad \text{Elim } \exists: \text{b special depends on } a
   
   2.4 \( a^2 = 4b^2 = 2(2b^2) \) \quad \text{Algebra}
   
   2.5 \( \exists y \ (a^2 = 2y) \) \quad \text{Intro } \exists \text{ rule}
   
   2.6 \( \text{Even}(a^2) \) \quad \text{Definition of Even}

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
English Proofs

• We often write proofs in English rather than as fully formal proofs
  – They are more natural to read

• English proofs follow the structure of the corresponding formal proofs
  – Formal proof methods help to understand how proofs really work in English...
    ... and give clues for how to produce them.
• In principle, formal proofs are the standard for what it means to be “proven” in mathematics
  – almost all math (and theory CS) done in Predicate Logic

• But they are **tedious** and impractical
  – e.g., applications of commutativity and associativity
  – Russell & Whitehead’s formal proof that $1+1 = 2$ is *several hundred pages* long
    we allowed ourselves to cite “Arithmetic”, “Algebra”, etc.

• Similar situation exists in programming...
Programming

%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d

arr[i] = arr[(i + 1) % n];

Assembly Language

High-level Language
Programming vs Proofs

\[
\begin{align*}
%a &= \text{add } %i, 1 \\
%b &= \text{mod } %a, %n \\
%c &= \text{add } %arr, %b \\
%d &= \text{load } %c \\
%e &= \text{add } %arr, %i \\
\text{store } %e, %d
\end{align*}
\]

Given

Given

\( \& \text{ Elim: 1} \)

Double Negation: 4

\( \lor \text{ Elim: 3, 5} \)

MP: 2, 6

Assembly Language for Programs

Assembly Language for Proofs
Proofs

Given

\(\land\) Elim: 1

Double Negation: 4

\(\lor\) Elim: 3, 5

MP: 2, 6

what is the “Java” for proofs?

Assembly Language for Proofs

High-level Language for Proofs
Proofs

Given
Given
∧ Elim: 1
Double Negation: 4
∨ Elim: 3, 5
MP: 2, 6

Assembly Language for Proofs
High-level Language for Proofs
Proofs

• Formal proofs follow simple well-defined rules and should be easy for a machine to check
  – as assembly language is easy for a machine to execute

• English proofs correspond to those rules but are designed to be easier for humans to read
  – also easy to check with practice
    (almost all actual math and theory CS is done this way)
  – English proof is correct if the reader believes they could translate it into a formal proof
    (the reader is the “compiler” for English proofs)
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
   1.1 $\text{Even}(a)$ Assumption
   2.1 $\exists y (a = 2y)$ Definition of Even
   2.2 $a = 2b$ Elim $\exists$: $b$ special depends on $a$
   2.3 $a^2 = 4b^2 = 2(2b^2)$ Algebra
   2.4 $\exists y (a^2 = 2y)$ Intro $\exists$ rule
   2.5 $\text{Even}(a^2)$ Definition of Even
   2.6 $\text{Even}(a) \rightarrow \text{Even}(a^2)$ Direct proof rule

2. $\forall x (\text{Even}(x) \rightarrow \text{Even}(x^2))$ Intro $\forall$: 1,2
Prove “The square of every even integer is even.”

Let $a$ be an arbitrary integer.

1. Let $a$ be an arbitrary integer.

Suppose $a$ is even.

2.1 Even($a$) Assumption

Then, by definition, $a = 2b$ for some integer $b$ (dep on $a$).

2.2 $\exists y \ (a = 2y)$ Definition

2.3 $a = 2b$ $b$ special depends on $a$

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

2.4 $a^2 = 4b^2 = 2(2b^2)$ Algebra

So $a^2$ is, by definition, even.

2.5 $\exists y \ (a^2 = 2y)$

2.6 Even($a^2$) Definition

Since $a$ was arbitrary, we have shown that the square of every even number is even.

2. Even($a$)$\rightarrow$Even($a^2$)

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

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

Then, by definition, \( a = 2b \) for some integer \( b \) (depending on \( a \)). Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \). So \( a^2 \) is, by definition, is even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even. \( \blacksquare \)
Prove “The sum of two odd numbers is even.”

Formally, prove  \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)
Prove “The sum of two odd numbers is even.”

**Proof:** Let $x$ and $y$ be arbitrary integers. Suppose that both are odd.

Then, $x = 2a + 1$ for some integer $a$ (depending on $x$) and $y = 2b + 1$ for some integer $b$ (depending on $x$). Their sum is $x + y = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1)$, so $x + y$ is, by definition, even.

Since $x$ and $y$ were arbitrary, the sum of any two odd integers is even. ■
**English Proof: Even and Odd**

Prove “The sum of two odd numbers is even.”

Let $x$ and $y$ be arbitrary integers.

1. Let $x$ be an arbitrary integer
2. Let $y$ be an arbitrary integer

Suppose that both are odd.

2.1 $\text{Odd}(x) \land \text{Odd}(y)$  
   Assumption

2.2 $\text{Odd}(x)$  
   Elim $\land$: 2.1

2.3 $\text{Odd}(y)$  
   Elim $\land$: 2.1

Then, $x = 2a+1$ for some integer $a$ (depending on $x$) and $y = 2b+1$ for some integer $b$ (depending on $x$).

2.4 $\exists z \ (x = 2z+1)$  
   Def of Odd: 2.2

2.5 $x = 2a+1$  
   Elim $\exists$: 2.4 ($a$ dep $x$)

2.6 $y = 2b+1$  
   Elim $\exists$: 2.5 ($b$ dep $y$)

Their sum is $x+y = ... = 2(a+b+1)$

2.7 $x+y = ... = 2(a+b+1)$  
   Algebra

2.8 $\exists z \ (x+y = 2z)$  
   Intro $\exists$: 2.4

2.9 $\text{Even}(x+y)$  
   Def of Even

Since $x$ and $y$ were arbitrary, the sum of any odd integers is even.

2. $(\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)$
3. $\forall x \ \forall y \ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$
Lecture 10 Activity

• You will be assigned to **breakout rooms**. Please:
• Introduce yourself
• Choose someone to share screen, showing this PDF
• Consider the statement:

  \[ \text{The sum of two even numbers is even.} \]

• Recall that an integer \( x \) is even if and only if there is an integer \( z \) with \( x = 2z \).

• Please do the following
  1. Write the statement in predicate logic
  2. Write an English proof

Fill out a poll everywhere for **Activity Credit**!
Go to [pollev.com/thomas311](http://pollev.com/thomas311) and login with your UW identity

---

**Prove “The sum of two odd numbers is even.”**

**Proof:** Let \( x \) and \( y \) be arbitrary integers. Suppose that both are odd. Then, \( x = 2a + 1 \) for some integer \( a \) (depending on \( x \)) and \( y = 2b + 1 \) for some integer \( b \) (depending on \( x \)). Their sum is \( x + y = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1) \), so \( x + y \) is, by definition, even. Since \( x \) and \( y \) were arbitrary, the sum of any two odd integers is even.
Rational Numbers

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

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

Predicate Definitions

Rational(x) ≡ ∃p ∃q ((x = p/q) ∧ Integer(p) ∧ Integer(q) ∧ (q ≠ 0))

Prove: “If x and y are rational, then xy is rational.”

Formally, prove ∀x ∀y ((Rational(x) ∧ Rational(y)) → Rational(x · y))
Rationality

Prove: “If x and y are rational, then xy is rational.”

Proof: Suppose that x and y are rational. Then, $x = \frac{a}{b}$ for some integers $a$, $b$, where $b \neq 0$, and $y = \frac{c}{d}$ for some integers $c, d$, where $d \neq 0$.

Multiplying, we get that $xy = \frac{ac}{bd}$. Since $b$ and $d$ are both non-zero, so is $bd$. Furthermore, $ac$ and $bd$ are integers. By definition, then, $xy$ is rational.
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let \( x \) and \( y \) be arbitrary.
Suppose that \( x \) and \( y \) are rational. Then, \( x = \frac{a}{b} \) for some integers \( a, b \), where \( b \neq 0 \), and \( y = \frac{c}{d} \) for some integers \( c, d \), where \( d \neq 0 \).
Multiplying, we get that \( xy = \frac{ac}{bd} \). Since \( b \) and \( d \) are both non-zero, so is \( bd \). Furthermore, \( ac \) and \( bd \) are integers. By definition, then, \( xy \) is rational.
Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. ■
English Proofs

• High-level language let us work more quickly
  – should not be necessary to spill out every detail
  – reader checks that the writer is not skipping too much
  – examples so far
    skipping Intro ∧ and Elim ∧
    not stating existence claims (immediately apply Elim ∃ to name the object)
    not stating that the implication has been proven ("Suppose X... Thus, Y." says it already)
  – (list will grow over time)

• English proof is correct if the reader believes they could translate it into a formal proof
  – the reader is the “compiler” for English proofs
Proof Strategies
Proof Strategies: Counterexamples

To prove $\neg \forall x P(x)$, prove $\exists \neg P(x)$:

- 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 an $x$ where $P(x)$ is false
- This example is called a *counterexample* to $\forall x P(x)$.

E.g. Prove “Not every prime number is odd”

Proof: 2 is prime but not odd, a counterexample to the claim that every prime number is odd. ■
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 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 \( p \rightarrow q \).

We will prove the contrapositive.

Suppose \( \neg q \).

\[ \begin{align*}
1.1. \quad & \neg q & \text{Assumption} \\
\ldots & \\
1.3. \quad & \neg p & \\
\text{1.} \quad & \neg q \rightarrow \neg p & \text{Direct Proof Rule} \\
\text{2.} \quad & p \rightarrow q & \text{Contrapositive: 1}
\end{align*} \]

Thus, \( \neg p \).
Proof by Contradiction: One way to prove $\neg p$

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

1.1. $p$ Assumption

1.3. $F$

1. $p \rightarrow F$ Direct Proof rule
2. $\neg p \lor F$ Law of Implication: 1
3. $\neg p$ Identity: 2
Proof Strategies: Proof by Contradiction

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

We will argue by contradiction.

Suppose \( p \).

\[
\begin{align*}
1. & \quad p & \text{Assumption} \\
2. & \quad \neg p \lor F & \text{Law of Implication: 1} \\
3. & \quad \neg p & \text{Identity: 2}
\end{align*}
\]

This shows \( F \), a contradiction.
Prove: “No integer is both even and odd.”

Formally, prove \( \neg \exists x \ (\text{Even}(x) \land \text{Odd}(x)) \)
Prove: “No integer is both even and odd.”

Formally, prove \[ \neg \exists x (\text{Even}(x) \land \text{Odd}(x)) \]

Proof: We work by contradiction. Suppose that \( x \) is an integer that is both even and odd.

Then, \( x = 2a \) for some integer \( a \) and \( x = 2b + 1 \) for some integer \( b \). This means \( 2a = 2b + 1 \) and hence \( a = b + \frac{1}{2} \).

But two integers cannot differ by \( \frac{1}{2} \), so this is a contradiction. \( \blacksquare \)
A proof with multiples

**Definition:** An integer \( y \) is a **strict multiple** of \( x \), if \( y = a \cdot x \) for some integer \( a \) with \( a \geq 2 \).

**Predicate Definitions**

\[
\text{SMul}(x, y) \equiv \exists a \ (a \geq 2 \land y = ax)
\]

**Domain of Discourse**

Positive Integers

**Example:** \( \text{SMul}(7, 21) = T, \text{SMul}(7, 22) = F, \text{SMul}(5, 5) = F \)
A proof with multiples

**Definition:** An integer \( y \) is a **strict multiple** of \( x \), if \( y = a \cdot x \) for some integer \( a \) with \( a \geq 2 \).

**Example:** \( SMul(7,21) = T, SMul(7,22) = F, SMul(5,5) = F \)

**Prove:** For all positive integers \( x \) there is a positive integer \( y \) that is a strict multiple of \( x \) and for all positive integer \( z \) it is not true that \( z \) is a multiple of \( x \) and \( y \) is a multiple of \( z \).
Definition: An integer $y$ is a **strict multiple** of $x$, if $y = a \cdot x$ for some integer $a$ with $a \geq 2$.

<table>
<thead>
<tr>
<th>Predicate Definitions</th>
<th>Domain of Discourse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{SMul}(x,y) \equiv \exists a \ (a \geq 2 \land y = ax)$</td>
<td>Positive Integers</td>
</tr>
</tbody>
</table>

Example: $SMul(7,21) = T$, $SMul(7,22) = F$, $SMul(5,5) = F$

Prove: For all positive integers $x$ there is a positive integer $y$ that is a strict multiple of $x$ and for all positive integer $z$ it is not true that $z$ is a multiple of $x$ and $y$ is a multiple of $z$.

$$\forall x \ \exists y \ (SMul(x,y) \land \forall z \ \neg(SMul(x,z) \land SMul(z,y)))$$
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
A proof with multiples

\[ \forall x \exists y \ (SMul(x, y) \land \forall z \neg (SMul(x, z) \land SMul(z, y))) \]

Prove: For all positive integers \( x \) there is a positive integer \( y \) that is a strict multiple of \( x \) and for all positive integer \( z \) it is not true that \( z \) is a multiple of \( x \) and \( y \) is a multiple of \( z \).

Proof:
Let \( x \) be an arbitrary positive integer.
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose y = 2x which is a strict multiple of x.
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer. Choose y = 2x which is a strict multiple of x. Let z be an arbitrary positive integer.
A proof with multiples

\[ \forall x \exists y (SMul(x, y) \wedge \forall z \neg (SMul(x, z) \wedge SMul(z, y))) \]

Prove: For all positive integers \( x \) there is a positive integer \( y \) that is a strict multiple of \( x \) and for all positive integer \( z \) it is not true that \( z \) is a multiple of \( x \) and \( y \) is a multiple of \( z \).

Proof:
Let \( x \) be an arbitrary positive integer.  
Choose \( y = 2x \) which is a strict multiple of \( x \).  
Let \( z \) be an arbitrary positive integer.  
Assume for the sake of contradiction that \( z \) is a strict multiple of \( x \) and \( y \) is a strict multiple of \( z \).
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose y = 2x which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence z = ax and y = bz for some integers a, b with a ≥ 2 and b ≥ 2.
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose y = 2x which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence z = ax and y = bz for some integers a, b with a ≥ 2 and b ≥ 2.
Then 2x = y = bz = abx.
A proof with multiples

∀x ∃y (SMul(x, y) ∧ ∀z ¬(SMul(x, z) ∧ SMul(z, y)))

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose y = 2x which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence z = ax and y = bz for some integers a, b with a ≥ 2 and b ≥ 2.
Then 2x = y = bz = abx. Dividing by x ≠ 0 gives 2 = ab ≥ 4. That is a contradiction. ■
Strategies

• Simple proof strategies already do a lot
  – counter examples
  – proof by contrapositive
  – proof by contradiction

• Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)
Applications of Predicate Logic

• Remainder of the course will use predicate logic to prove important properties of interesting objects
  – start with math objects that are widely used in CS
  – eventually more CS-specific objects

• Encode domain knowledge in predicate definitions

• Then apply predicate logic to infer useful results

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>Even(x) \equiv \exists y \ (x = 2 \cdot y)</td>
</tr>
<tr>
<td></td>
<td>Odd(x) \equiv \exists y \ (x = 2 \cdot y + 1)</td>
</tr>
</tbody>
</table>
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

- $A = \{1\}$
- $B = \{1, 3, 2\}$
- $C = \{\square, 1\}$
- $D = \{17\}, 17\}$
- $E = \{1, 2, 7, \text{cat, dog, } \emptyset, \alpha\}$
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. \(\frac{1}{2}, -17, \frac{32}{48}\)

\(\mathbb{R}\) 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

\(\emptyset\) = \(\varnothing\) 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

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

• 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

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

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

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

\[ A = \{1, 2, 3\} \]
\[ B = \{3, 4, 5\} \]
\[ C = \{3, 4\} \]

QUESTIONS

\[ \emptyset \subseteq A? \]
\[ A \subseteq B? \]
\[ C \subseteq B? \]
Building Sets from Predicates

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

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

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

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

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

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

\[ A = \{1, 2, 3\} \]
\[ B = \{3, 5, 6\} \]
\[ C = \{3, 4\} \]

**QUESTIONS**

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

\[ [6] = \]
\[ \{3\} = \]
\[ \{1,2\} = \]
More Set Operations

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

Symmetric Difference

\[ \overline{A} = \{ x : x \notin A \} \]
(\text{with respect to universe } U)

Complement

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

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

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

\[ A \cap B = \bar{A} \cup \bar{B} \]
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, by definition of complement, we have \(\neg(x \in A \cup B)\). The latter is equivalent to \(\neg(x \in A \lor x \in B)\), which is equivalent to \(\neg(x \in A) \land \neg(x \in B)\) by De Morgan’s law. We then have \(x \in A^C\) and \(x \in B^C\), by the definition of complement, so we have \(x \in A^C \cap B^C\) by the definition of intersection.

Proof technique:
To show \(C = D\) show
\(x \in C \rightarrow x \in D\) and
\(x \in D \rightarrow x \in C\)
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x \ (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

**Proof:** Let \(x\) be an arbitrary object.

Suppose \(x \in (A \cup B)^C\). Then, \(x \in A^C \cap B^C\).

Suppose \(x \in A^C \cap B^C\). Then, by definition of intersection, we have \(x \in A^C\) and \(x \in B^C\). That is, we have \(\neg(x \in A) \land \neg(x \in B)\), which is equivalent to \(\neg(x \in A \lor x \in B)\) by De Morgan’s law. The last is equivalent to \(\neg(x \in A \cup B)\), by the definition of union, so we have shown \(x \in (A \cup B)^C\), by the definition of complement. ■
De Morgan’s Laws

Prove that \((A \cup B)^C = A^C \cap B^C\)

Formally, prove \(\forall x (x \in (A \cup B)^C \iff x \in A^C \cap B^C)\)

Proof: Let \(x\) be an arbitrary object.

The stated bi-condition holds since:

\[
x \in (A \cup B)^C \equiv \neg(x \in A \cup B) \quad \text{def of } -^C
\]
\[
\equiv \neg(x \in A \lor x \in B) \quad \text{def of } \cup
\]
\[
\equiv \neg(x \in A) \land \neg(x \in B) \quad \text{De Morgan}
\]
\[
\equiv x \in A^C \land x \in B^C \quad \text{def of } -^C
\]
\[
\equiv x \in A^C \cap B^C \quad \text{def of } \cap
\]

Chains of equivalences are often easier to read like this rather than as English text.
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 $A = \text{set of all subsets of } A$

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

• 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

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

$$\mathcal{P}(\emptyset)=\{\emptyset\} \neq \emptyset$$
**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 \(A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}\).
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 \( A \times B = \{(1,a), (1,b), (1,c),
(2,a), (2,b), (2,c)\} \).

What is \( A \times \emptyset \)?
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 $A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$.

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

• Suppose universe \( U \) is \( \{1,2, \ldots, n\} \)

• Can represent set \( B \subseteq U \) as a vector of bits:

\[
\begin{align*}
  b_1 b_2 \ldots b_n \\
  \text{where} \quad b_i = 1 \text{ when } i \in B \\
  b_i = 0 \text{ when } i \not\in B
\end{align*}
\]

– Called the characteristic vector of set \( B \)

• Given characteristic vectors for \( A \) and \( B \)

  – What is characteristic vector for \( A \cup B \)? \( A \cap B \)?
Bitwise Operations

01101101
\textbf{\lor} 00110111
\hline
01111111

00101010
\textbf{\land} 00001111
\hline
00001010

01101101
\textbf{\oplus} 00110111
\hline
01011010

\textbf{Java: }\ z=x \mid y

\textbf{Java: }\ z=x \& y

\textbf{Java: }\ z=x ^ y
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

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

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.”