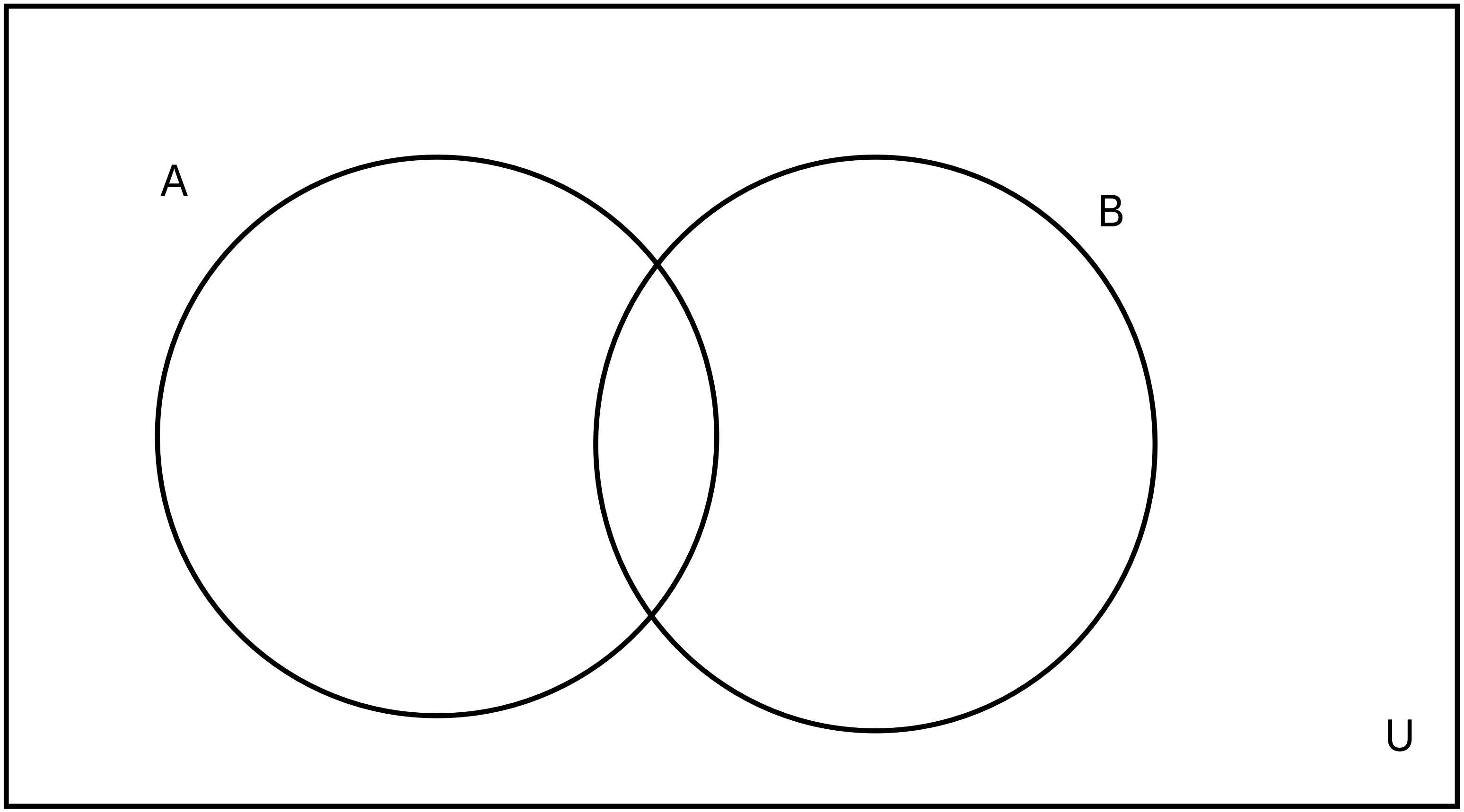
Mathematical Preliminaries (Hein 1.1 and 1.2)

- Sets are collections in which order of elements and duplication of elements do not matter.
  - {1,a,1,1} = {a,a,a,1} = {a,1}
  - Notation for *membership*: $1 \in \{3,4,5\}$
  - *Set-former* notation: $\{x \mid P(x)\}$ is the set of all *x* which
  - satisfy the property *P*.
  - $\{x \mid x \in N \text{ and } 2 \geq x \geq 5\}$
  - $\{x \in N \mid 2 \geq x \geq 5\}$
  - Often a *universe* is specified. Then all sets are assumed to be subsets of the universe (*U*), and the notation
  - $\{x \mid P(x)\}$ stands for $\{x \in U \mid P(x)\}$

Operations on Sets

- *empty set* : $\emptyset$
- Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- Difference: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$
- Complement: $\underline{A} = U - A$

Venn Diagrams



Laws

- $A \cup A = A$
- $A \cup B = B \cup A$
- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\underline{A \cup B} = \underline{A} \cap \underline{B}$
- $A \cup \emptyset = A$

- $A \cap A = A$
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $\underline{A \cap B} = \underline{A} \cup \underline{B}$
- $A \cap \emptyset = \emptyset$

Subsets and Powerset

- A is a *subset* of B if all elements of A are elements of B as well. Notation: $A \subseteq B$.
-
- The *powerset* $\mathbb{P}(A)$ is the set whose elements are all subsets of A: $\mathbb{P}(A) = \{X \mid X \subseteq A\}$.
-
- **Fact**. If A has n elements, then $\mathbb{P}(A)$ has 2^n
- elements.
-
- In other words, $|\mathbb{P}(A)| = 2^{|A|}$, where $|X|$ denotes the number of elements (*cardinality*) of X.

Proving Equality and non-equality

- To show that two sets A and B are equal, you need to do two proofs:
  - Assume $x \in A$ and then prove $x \in B$
  - Assume $x \in B$ and then prove $x \in A$
- **Example**. Prove that $P(A \cap B) = P(A) \cap P(B)$.
- To prove that two sets A and B are not equal, you need to produce a *counterexample* : an element x that belongs to one of the two sets, but does not belong to the other.
- **Example**. Prove that $P(A \cup B) \neq P(A) \cup P(B)$.
- Counterexample: A={1}, B={2}, X={1,2}. The set X belongs to $P(A \cup B)$, but it does not belong to $P(A) \cup P(B)$.

Strings
(Hein 1.3.3, 3.1.2, 3.2.2)

- Strings are defined with respect to an *alphabet*, which is an arbitrary *finite* set of symbols. Example alphabets are {0,1} (*binary*) and ASCII.

- A *string* over an alphabet Σ is any finite sequence of elements of Σ.

- `Hello` is an ASCII string; 0101011 is a binary string.

- The *length* of a string w is denoted $|w|$. The set of all strings of length n over Σ is denoted Σ^n.

More strings

- $\Sigma^0=\{\Lambda\}$, where Λ is the *empty string* (common to all alphabets).
-
- Σ^* is the set of *all* strings over Σ:
- $\Sigma^* = \{\Lambda\} \cup \Sigma \cup \Sigma^2 \cup \Sigma^3 \cup \; \ldots$
-
- Σ^+ is Σ^* with the empty string excluded:
- $\Sigma^* = \Sigma \cup \Sigma^2 \cup \Sigma^3 \cup \; \ldots$

String concatenation

- If u=`one` and v=`two` then u • v=`onetwo` and
- v • u=`twoone`. Dot is usually omitted; just write uv for u • v.
- Laws:
- u • (v • w) = (u • v) • w
- u • Λ = u
- Λ • u = u
- |u • v| = |u| + |v|

- The n^{th} power of the string u is u^n = u • u ... u, the concatenation of n copies of u.
- E.g., One^3 = oneoneone .
- Note $u^0=\Lambda$.

Can you tell the difference?

- There are three things that are sometimes confused.

Λ – the empty string (“”)

$\varnothing$ – the empty set ({ })

$\{\Lambda\}$ – the set with just the empty string as an element

Languages

- A *language* over an alphabet Σ is any subset of Σ^*. That is, any set of strings over Σ.

- Some languages over {0,1}:
  - {Λ,01,0011,000111, … }
  - The set of all binary representations of prime numbers: {10,11,101,111,1011, … }

- Some languages over ASCII:
  - The set of all English words
  - The set of all C programs

Language concatenation

- If L and L' are languages, their concatenation L • L' (often denoted LL') is the set
- {u • v | u $\in$ L and v $\in$ L‘ }.
-
- **Example**. {0,00} • {1,11} = {01,011,001,0011}.
-
- The n^{th} power L^n of a language L is L • L ... L, n
- times. The zero power L^0 is the language $\{\Lambda\}$, by definition.
-
- **Example**. $\{0,00\}^4=\{0^4,0^5,0^6,0^7,0^8\}$

Kleene Star

- Elements of L^* are Λ and all strings obtained by concatenating a finite number of strings in L.
  - $L^* = L^0 \cup L^1 \cup L^2 \cup L^3 \cup \ldots$
  - $L^+ = L^1 \cup L^2 \cup L^3 \cup \ldots$
  - Note: $L^* = L^+ \cup \{\Lambda\}$
- **Example**. $\{00,01,10,11\}^*$ is the language of all even length binary strings.

Class Exercise

- Fill in the blanks to define some laws:

$L^{*} \cup \{\Lambda\}$ = ____________

$L^{+} \bullet \{\Lambda\}$ = ____________

$\{\Lambda\} \bullet \{\Lambda\}$ = ____________

$\varnothing \bullet L$ = ____________

$L^{*} \bullet L^{*}$ = ____________

$(L^{*})^{*}$ = ____________

$L \bullet L^{*}$ = ____________

$\varnothing^{*}$ = ____________

$\{\Lambda\}^{*}$ = ____________

$L \bullet L^{*}$ = ____________

Mathematical Statements (Hein 6.1, 6.2, 6.3, 7.1)

- *Statements* are sentences that are true or false:
  - [1.] $0=3$
  - [2.] `ab` is a substring of `cba`
  - [3.] Every square is a rectangle
-
- *Predicates* are parameterized statements; they are true or false depending on the values of their parameters.
  - [1.] $x>7$ and $x<9$
  - [2.] $x+y=5$ or $x-y=5$
  - [3.] If $x=y$ then $x^2=y^2$

Logical Connectives

- *Logical connectives* produce new statements from simple ones:
  - Conjunction; $A \wedge B$; A and B
  - Disjunction; $A \vee B$; A or B
  - Implication; $A \Rightarrow B$; if A then B
  - Negation; $\neg A$ not A
  - Logical equivalence; $A \Leftrightarrow B$
  - A if and only if B
  - A iff B

Quantifiers

- The *universal quantifier* (∀ "for every") and the *existential quantifier* (∃ "there exists") turn predicates into other predicates or statements.
  - There exists x such that x+7=8.
  - For every x, x+y > y.
  - Every square is a rectangle.

- **Example**. True or false?
  - $(\forall x)(\forall y)\ x+y=y$
  - $(\forall x)(\exists y)\ x+y=y$
  - $(\exists x)(\forall y)\ x+y=y$
  - $(\forall y)(\exists x)\ x+y=y$
  - $(\exists y)(\forall x)\ x+y=y$
  - $(\exists x)(\exists y)\ x+y=y$

Proofs
(Hein 1.1, 1.2, 4.4, 7.1)

- There are many ways to structure proofs
  - Implications
  - Proof by contradiction
  - Proof by exhaustive case analysis
  - Proof by induction

You should be able to use all these techniques

Proving Implications

- Most theorems are stated in the form of (universally quantified) implication: if A, then B
- To prove it, we *assume* that A is true and proceed to derive the truth of B by using logical reasoning and known facts.
- **Silly Theorem**. If 0=3 then 5=11.
- *Proof*. Assume 0=3. Then 0=6 (why?). Then 5=11 (why?).

- Note the implicit universal quantification in theorems:
- **Theorem A**. If x+7=13, then x^2=x+20.
- **Theorem B**. If all strings in a language L have even length, then all strings in L* have even length.

Converse (Hein 1.1)

- The *converse* of the implication $A \Rightarrow B$ is the implication $B \Rightarrow A$. It is quite possible that one of these implications is true, while the other is false.
- E.g., $0=1 \Rightarrow 1=1$ is true,
- but $1=1 \Rightarrow 0=1$ is false.
  - Note that the implication $A \Rightarrow B$ is true in all cases except when A is true and B is false.
-
- To prove an equivalence $A \Leftrightarrow B$, we need to prove a pair of converse implications:
  - (1) $A \Rightarrow B$,
  - (2) $B \Rightarrow A$.

Contrapositive (Hein 1.1)

- The *contrapositive* of the implication $A \Rightarrow B$ is the implication $\neg B \Rightarrow \neg A$. If one of these implications is true, then so is the other. It is often more convenient to prove the contrapositive!

- **Example**. If L_1 and L_2 are non-empty languages such that $L_1^* = L_2^*$ then $L_1=L_2$.

- *Proof*. Prove the contrapositive instead. Assume $L_1 \neq L_2$. Let w be the shortest possible non-empty string that belongs to one of these languages and does not belong to the other (e.g. $w \in L_1$ and $w \notin L_2$). Then $w \in L_1^*$ and it remains to prove $w \notin L_2^*$. [Finish the proof. Why is the assumption that $L_1, L_2 \neq \varnothing$ necessary?]

Reductio ad absurdum- Proof by Contradiction

- Often, to prove $A \Rightarrow B$, we assume both A and $\neg$ B, and then proceed to derive something absurd (obviously non-true).
-
- **Example**. If L is a finite language and L • L =L, then L=$\varnothing$ or L={Λ}.
- *Proof*. Assume L is finite, L • L =L, L$\neq \varnothing$, and L$\neq \{\Lambda\}$. Let w be a string in L of maximum length. The assumptions imply that $|w|>0$. Since $w^2 \in L^2$, we must have $w^2 \in L$. But $|w^2|=2|w|>|w|$, so L contains strings longer than w. Contradiction.
- qed
-