ECS 020 Summary

1. Discrete systems and structures

Discrete: Composed of distinct, separable parts.
Structures: Objects built up from simpler objects according to some definite pattern.
Discrete Mathematics: The study of discrete, mathematical objects and structures.

2. Propositional logic

Propositional Logic: The logic of compound statements built from simpler statements using so-called Boolean connectives.
Proposition: 1) A declarative statement with some definite meaning (not vague or ambiguous), 2) having a truth value that is either true (T) or false (F), 3) it is never both, neither, or somewhere "in between".
We might know the actual truth value, and the truth value might depend on the situation or context.

3. Boolean Operators / Connectives

An operator or connective combines one or more operand expressions into a larger expression.

1) Unary operators take 1 operand (e.g., negation, −3)
2) Binary operators take 2 operands (e.g., multiplication, 3 × 4)

Propositional or Boolean operators operate on propositions (or their truth values) instead of on numbers

4. Negation Operator (NOT, ¬)

Unary operator. Truth table:

p	$\neg p$
T	F
F	T

5. Conjunction Operator (AND, ∧)

Binary operator. Truth table:

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

¬ and ∧ operations together are sufficient to express any Boolean truth table.

6. Disjunction Operator (OR, ∨)

Binary operator. Truth table:

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

¬ and ∨ operations together are sufficient to express any Boolean truth table.

7. Exclusive Or Operator (XOR, ⊕)

Binary operator. Truth table:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

8. Implication Operator (→)

Binary operator. $p \to q$ means p (hypothesis / antecedent) implies q (conclusion / consequent).

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Common phrases meaning $p \to q$:
"p implies q", "q if p", "p only if q", "p is sufficient for q", "q is necessary for p"
Converse, Inverse, Contrapositive for $p \to q$:
Converse: $q \to p$
Inverse: $\neg p \to \neg q$
Contrapositive: $\neg q \to \neg p$ (same as $p \to q$)

9. Biconditional Operator (↔)

Binary operator. $p \leftrightarrow q$ means that $p \to q$ and $q \to p$. p is true if and only if (IFF) q is true (p and q have the same truth value).

p	q	$p \to q$
F	F	T
F	T	F
T	F	F
T	T	T

This truth table is the exact opposite of ⊕'s. So $p \leftrightarrow q$ means $\neg(p \oplus q)$.
$p \leftrightarrow q$ does not imply that p and q are true, or that either of them causes the other, or that they have a common cause.

10. Boolean Operations Summary

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
F	F	T	F	F	F	T	T
F	T	T	F	T	T	T	F
T	F	F	F	T	T	F	F
T	T	F	T	T	F	T	T

Order of operation: ¬, ∧, ∨, ⊕, →, ↔.
Ex: $p \vee \neg q \to p \wedge q$ means $(p \vee (\neg q)) \to (p \wedge q)$
Precedence of ∨ or ⊕ is ambiguous and often depends on the programming language.

11. Propositional Consistency

Two different compound propositions may be True at the same time. We call them consistent.
Use truth table to solve this kind of problem.
Ex: Among four people, P1, P2, P3, P4, at least one of is truthful, and at least one is lying. One of the truthful ones has a treasure in their pocket. They each know who has the treasure and each of them makes a statement:
S1 (by P1): I don't have the treasure.
S2 (by P2): My pockets are empty.
S3 (by P3): P1 is lying.
S4 (by P4): P1 is lying.
Where is the treasure?

P1	P2	P3	P4	Consist?	Why
T	T	T	T	NO	Violating "at least one is lying".
T	T	T	L	NO	If P4 is lying, then P1 is truthful, but P3 is truthful, then P1 is lying, this violates S3.
…	…	…	…	…	…
T	T	L	T	YES	

As a result, person 3 is lying, other people are truthful.

12. Propositional Equivalence

Two syntactically (i.e., textually) different compound propositions may be the semantically identical (i.e., have the same meaning). We call them equivalent.

1) Tautology
   A tautology is a compound proposition that is always true no matter what the truth values of its atomic propositions are!
   Ex: $p \vee \neg p = T$ always
2) Contradictions
   A contradiction is a compound proposition that is false no matter what!
   Ex: $p \wedge \neg p = F$ always

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

3) Logical Equivalence
   Compound proposition p is logically equivalent to compound proposition q, written $p \Leftrightarrow q$, if and only if the compound proposition $p \leftrightarrow q$ is a taulolgy.

TABLE 7 Logical Equivalences Involving Conditional Statements.

$p \to q \equiv \neg p \vee q$
$p \to q \equiv \neg q \to \neg p$
$p \vee q \equiv \neg p \to q$
$p \wedge q \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \wedge \neg q$
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Exclusive or: $p \oplus q \Leftrightarrow (p \vee q) \wedge \neg(p \wedge q)$
$p \oplus q \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$

Implication: $p \to q \Leftrightarrow \neg p \vee q$

Biconditional: $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$
$p \leftrightarrow q \Leftrightarrow \neg(p \oplus q)$

p	q	$p \to q$
F	F	T
F	T	T
T	F	**F**
T	T	T

TABLE 6 Logical Equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

13. Logical Inference

Definition: An Inference Rule is a pattern establishing that if we know that a set of antecedent statements of certain forms are all true, then we can validly deduce that a certain related consequent statement is true.

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Formal proof is based on the rules above

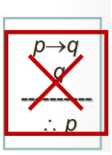
Definition: A formal proof of a conclusion C, given premises p1, p2, …, pn sequence of steps, apply inference rule to premises or previously proven statements (antecedents), and yield new true statement (the consequent)

A proof: if the premises are true, then the conclusion is true.

A fallacy is an inference rule or other proof method that is not logically valid.

Fallacy of *affirming the consequent*:

- "$p \to q$ is true, and q is true, so p must be true." (No, because **F→T** is also true.)
- p is *sufficient* but not *necessary* for q



Fallacy of *denying the antecedent*:

- "$p \to q$ is true, and p is false, so q must be false." (No, because **F→T** is also true.)
- p is *sufficient* but not *necessary* for q

14. Predicate logic

1) Propositional function $P(x)$: A statement involving the variables x.

2) A statement from $P(x_1, x_2, \dots, x_n)$ is the value of the propositional function P at the n-th tuple $(x_1, x_2, \dots, x_n)$, and P is called the predicate.

3) The domain of discourse, denote U, is the set of values x that x is allowed to take in $P(x)$.

4) The universal quantification of $P(x)$ is the proposition "$P(x)$ is true for all value of x in U".

Notation: $\forall x P(x)$, $\forall$ is called the universal quantifier.

"$\forall x P(x)$"=True, when $P(x)$ is true for every x in U.

"$\forall x P(x)$"=False, when there is an x in U for which $P(x)$ is false.

Examples:

"for all integers n, 2n is even" (True)

"for all real numbers x, $x^2 - 1 > 0$" (False, $x = 0$)

"for all CS major students S, S must take discrete math" (True)

5) The existential quantification of $P(x)$ is the proposition "There exists an element x in U such that $P(x)$ is true."

Notation: $\exists x P(x)$, $\exists$ is called the existential quantifier.

"$\exists x P(x)$"=True, when there is an x in U for which $P(x)$ is true.

"$\exists x P(x)$"=False, when $P(x)$ is false for every x in U.

Examples:

"there exists an integer n, $2 * n$ is even" (True)

"there exists a student S, S works hard" (True)

"there exists a real number x, $x^2 < 0$" (False)

6) Quantifier equivalence laws

$\forall x P(x) \Leftrightarrow \neg\exists x \neg P(x)$

$\exists x P(x) \Leftrightarrow \neg\forall x \neg P(x)$

$\forall x \forall y P(x, y) \Leftrightarrow \forall y \forall x P(x, y)$

$\exists x \exists y P(x, y) \Leftrightarrow \exists y \exists x P(x, y)$

$\forall x (P(x) \wedge Q(x)) \Leftrightarrow (\forall x P(x)) \wedge (\forall x Q(x))$

$\exists x \big(P(x) \vee Q(x)\big) \Leftrightarrow \big(\exists x P(x)\big) \vee (\exists x Q(x))$

7) Negations

Negating the universal: $\neg\forall x P(x) \Leftrightarrow \exists x \neg P(x)$

Example:

"All mathematicians wear glasses."

Negation: "There is at least one mathematician who does not wear glasses."

Negating the existential: $\neg\exists x P(x) \Leftrightarrow \forall x \neg P(x)$

Example:

"Some snowflakes are the same."

Negation: "No snowflakes are the same." Or "All snowflakes are different."

8) Notational Conventions:

Quantifiers bind as loosely as needed:

$\forall x P(x) \wedge Q(x)$

Consecutive quantifiers of the same type can be combined:

$\forall x \forall y \forall z P(x, y, z) \Leftrightarrow \forall x, y, z P(x, y, z) \Leftrightarrow \forall xyz P(x, y, z)$

All quantified expressions can eb reduced to the canonical alternating form:

$\forall x_1 \exists x_2 \exists x_3 \exists x_4 \dots P(x_1, x_2, x_3, x_4, \dots)$

Sometimes the universe of discourse is restricted within the quantification:

$\forall x > 0 P(x) \Leftrightarrow \forall x (x > 0 \to P(x))$

Meaning: For all x that are greater than zero, P(x).

$\exists x > 0 P(x) \Leftrightarrow \exists x (x > 0 \wedge P(x))$

Meaning: There is an x greater than zero such that P(x).

9) Deduction Example

Definitions:

s: ≡Socrates (ancient Greek philosopher)

$H(x)$: ≡ "x is human"

$M(x)$: ≡ "x is mortal"

Premises:

H(s): Socrates is human.

$\forall x H(x) \to M(x)$: All humans are mortal.

15. Proof

1) Direct proof (Assume p is true, and prove q)

The implication $p \to q$ can be proved by showing that if p is true then q must also be true. A proof of this kind is called a direct proof.

2) Indirect proof (Assume $\neg q$, and prove $\neg p$)

Proof by contraposition: Since the implication $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$, the implication $p \to q$ can be proved by showing that $\neg q \to \neg p$ is true. This related implication is usually proved directly. An argument of this type is called an indirect proof.

A **vacuous proof** is established by showing $\neg p$. (Prove $\neg p$ by itself.)

A **trivial proof** is established by showing q is true. (Prove q by itself.)

3) Proof by contradiction

For proposition p: Assume $\neg p$ is true and show this leads to both r and $\neg r$ for some independent proposition r; in other words $\neg p \to (r \wedge \neg r)$.

For implication $p \to q$: By assuming that the hypothesis p is true and that the conclusion q is false, then using p and $\neg q$ as well as other axioms, definitions, and previously derived theorems, derives a contradiction.

Proofs are based on noting that $\big(((p \to q) \wedge p) \wedge \neg q\big) \equiv (q \wedge \neg q)$

likewise $\big(p \wedge (\neg q \to \neg p)\big) \equiv (p \wedge \neg p)$.

4) Equivalence proof

To prove a theorem that is an equivalence $(p \leftrightarrow q$, the tautology), $(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$ can be used. That is, the proposition "p if and only if q" can be proved if both the implication "if p then q" and "if q then p" are proved.

5) Proof by cases/Exhaustive proof

Exhaustive proof: Proof by showing it holds for all possible x in U. (Truth table)

Proof by case: Proof by showing it holds for all possible cases. (Useful when direct proof not simple but the extra information in the cases let you move forward.)

Without loss of generality (WLOG): Same proof holds for all cases. Quite useful but gets one into trouble (a common mistake in a proof).

6) Constructive existence proof

It is the proof of statement of the form $\exists x P(x)$. Just find one value of x in U for which $P(x)$ is true. (Hence "constructive").

7) Nonconstructive existence proof

Don't pinpoint the exact values that satisfy, just show they must exist.

8) Proof by counterexample

The goal of such a proof is to show $\forall x P(x)$ is false. Note, showing $\exists x P(x)$ is false is counterexample for $\forall x P(x)$, but this is not a counterexample for the conjecture $\exists x P(x)$.

16. Set Theory

1) Definition: A set is a type of structure, representing an unordered collection of zero or more distinct objects.

Set theory deal with operations between, relations among, and statements about sets.

2) Notation

We can use variables such as S,T,U,... to denote a set.

We can explicitly listing a set by specifying all of its elements in curly braces.

Example:

S={a,b,c,d}

For any proposition P(x) over some specified universe of discourse, {x|P(x)} is the set of all x such that P(x).

Example:

S={x|x>0} means the set of numbers x, which are positive.

3) Properties of Sets

Unordered

{a,b,c} = {a,c,b} = {b,a,c} = {b,c,a} = {c,a,b} = {c,b,a}

Distinct

If a=b, then {a,b,c} = {a,c} = {b,c} = {a,a,b,a,b,c,c,c}. This set contains (at most) 2 elements.

Cardinality (size) of a set

If there are n distinct elements in the set S, where n is a nonnegative integer, we say that S is a finite set.

|S| is the cardinality (size) of S.

A set is said to be infinite if it is not finite.

Example:

S={a,a,b,a,b,c,c,c,c}, then |S|=3.

4) Membership

Definition:

x∈S ("x is in S") is the predicate that object x is an element or member of set S.

Example:

3∈{1,2,3,4}

3∈{x|x is an integer}

"a" ∈{x|x is a letter of the alphabet}

Negation: x∈S:≡¬(x∈S) "x is not in S"

5) Equality

Two sets are declared to be equal if and only if they contain exactly the same elements: A=B⇔∀x(x∈A↔x∈B).

It does not matter how the set is defined or denoted.

Example:

The set {1,2,3,4}

= {x|x is an integer where x>0 and x<5}

= {x|x is a positive integer whose square is >0 and <25}

6) Infinite Sets

Conceptually, sets may be infinite, which means not finite, without end, unending.

Symbols for some special infinite sets:

N={0,1,2,...} The natural numbers

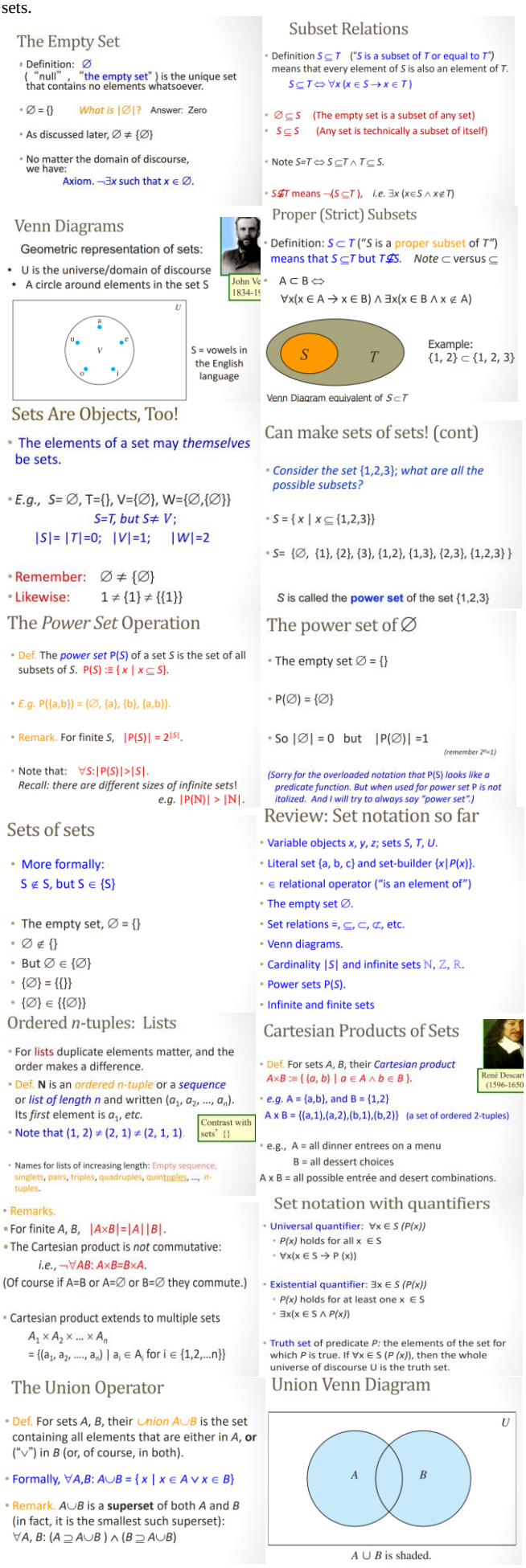
Z={...,−2,−1,0,1,2,...} The integers

Z+={1,2,3,4,...} The positive integers

Q={12,34,11,7123,...}

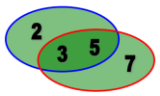
R= The "real" numbers, such as 374.182847192949881943125...,π, and so on.

Double-struck font (N, Z, Z+, R) is also often used for these special number sets.



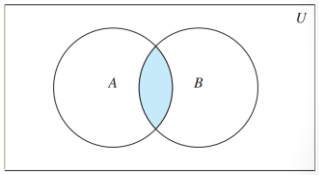
Union Examples

- {a,b,c}∪{2,3} = {a,b,c,2,3}
- {2,3,5}∪{3,5,7} = {2,3,5,3,5,7} ={2,3,5,7}



E.g., "The set of people who may owe income tax to the US Government includes every person who worked in any U.S. state last year."

Intersection Venn diagram



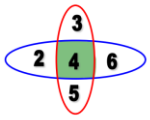
$A \cap B$ is shaded.

The Intersection Operator

- Def. For sets *A*, *B*, their *intersection* $A \cap B$ is the set containing all elements that are simultaneously in *A* **and** ("$\wedge$") in *B*.
- Formally, $\forall A,B: A \cap B = \{ x \mid x \in A \wedge x \in B \}$
- Remark. $A \cap B$ is a **subset** of both A and B (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \wedge (A \cap B \subseteq B)$

Intersection Examples

- {a,b,c}∩{2,3} = ?
- {2,4,6}∩{3,4,5} = ?

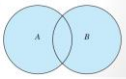


E.g., "The **intersection** of 2nd Ave. and 3rd St. is just that part of the road surface that lies on *both* streets."

Inclusion-Exclusion Principle

- How many elements are in $A \cup B$?
  $|A \cup B| = |A| + |B| - |A \cap B|$
- Example: How many students are math or CS majors? Consider set $S = A \cup B$,
  A = { *s* | *s* is a CS major}
  B = { *s* | *s* is a Math major}
- Some students double major! (We only want to count each once)
- $|S| = |A \cup B| = |A| + |B| - |A \cap B|$

Subtract out items in intersection, to compensate for double-counting them!



Disjointedness

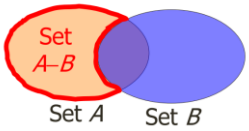
- Def. Two sets *A*, *B* are called *disjoint* (*i.e.*, unjoined) iff their intersection is empty. ($A \cap B = \varnothing$)
- Example: the set of even integers is disjoint with the set of odd integers.

Set Difference

- Def. For sets *A*, *B*, the *difference of A and B*, written *A–B*, is the set of all elements that are in *A* but not *B*.
- Formally:
  $A - B := \{ x \mid x \in A \wedge x \notin B \}$
- Also called:
  The *complement of B with respect to A*.
- Note, |A-B| ≤ |A| (regardless of the size of B)

Set Difference - Venn Diagram

- *A–B* is what's left after *B* "takes a bite out of *A*"



Set Difference Examples

- {1,2,3,4,5,6} – {2,3,5,7,9,11} = {1,4,6}
- Z – N = {... , −1, 0, 1, 2, ... } – {0, 1, ... }
  = {*x* | *x* is an integer but not a nat. #}
  = {*x* | *x* is a negative integer}
  = {... , −3, −2, −1}

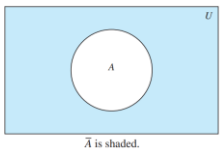
Set Complements, $\overline{A}$

- Def. The *universe of discourse* can itself be considered a set, call it *U*.
- When the context clearly defines *U*, we say that for any set $A \subseteq U$, the *complement* of *A*, written $\overline{A}$ is the complement of *A* w.r.t. *U*, *i.e.*, it is *U*–*A*.
- *E.g.*, If $U = \mathbf{N}$,
  $\overline{\{3,5\}} = \{0,1,2,4,6,7,...\}$

More on Set Complements

- An equivalent definition, when *U* is given:

$$\overline{A} = \{x \mid x \notin A\}$$



$\overline{A}$ is shaded.

Set Identities

- Identity: $A \cup \varnothing = A = A \cap U$
- Domination: $A \cup U = U$, $A \cap \varnothing = \varnothing$
- Idempotent: $A \cup A = A = A \cap A$
- Double complement: $\overline{(\overline{A})} = A$
- Commutative: $A \cup B = B \cup A$, $A \cap B = B \cap A$
- Associative: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$

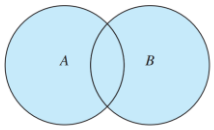
You can see these are analogous to the logical equivalences that we studied for propositions (Table 6) .

DeMorgan's Law for Sets

- Exactly analogous to (and provable from) DeMorgan's Law for propositions.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$



$A \cup B$ is shaded.

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \varnothing = A$	Identity laws
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$	Complement laws

Generalized Unions & Intersections

- Since union & intersection are commutative and associative, we can extend them from operating on *ordered* sequences of sets ($A_1,...,A_n$), or even on unordered *sets* of sets, $X = \{A \mid P(A)\}$.

Generalized Union

- Binary union operator: $A \cup B$
- *n*-ary union:
  $A \cup A_2 \cup ... \cup A_n := ((...((A_1 \cup A_2) \cup ...) \cup A_n)$
  (grouping & order is irrelevant)
- "Big U" notation: $\bigcup_{i=1}^{n} A_i$
- or for infinite sets of sets: $\bigcup_{A \in X} A$

Generalized Intersection

- Binary intersection operator: $A \cap B$
- *n*-ary intersection:
  $A_1 \cap A_2 \cap ... \cap A_n \equiv ((...((A_1 \cap A_2) \cap ...) \cap A_n)$
  (grouping & order is irrelevant)
- "Big Arch" notation: $\bigcap_{i=1}^{n} A_i$
- or for infinite sets of sets: $\bigcap_{A \in X} A$

Proving Set Identities

- To prove statements about sets, of the form $E_1 = E_2$ (where the *E*s are set expressions), here are three different and useful methods:
  1. Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.
  2. Use set builder notation & logical equivalences.
  3. Use a *membership table*.

Method 1: Mutual subsets

- Example:
- Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- Part 1: Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
  - Assume $x \in A \cap (B \cup C)$, & show $x \in (A \cap B) \cup (A \cap C)$.
  - We know that $x \in A$, and either $x \in B$ or $x \in C$.
    - Case 1: $x \in B$. Then $x \in A \cap B$, so $x \in (A \cap B) \cup (A \cap C)$.
    - Case 2: $x \in C$. Then $x \in A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. ...

Method 2: Direct proof

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement}\\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol}\\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection}\\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equival}\\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol}\\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement}\\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union}\\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}$$

Method 3: Membership Tables

- Just like truth tables for propositional logic.
- Columns for different set expressions.
- Rows for all combinations of memberships in constituent sets.
- Use "1" to indicate element is a member of the specified set, and "0" for non-membership.
- Prove equivalence with identical columns.

Membership Table Example

- Prove $(A \cup B) - B = A - B$.

A	*B*	$A \cup B$	$(A \cup B) - B$	$A - B$
0	0	0	0	0
0	1	1	0	0
1	0	1	1	1
1	1	1	0	0

Introduction

- A binary relation from set A to set B is a *subset* of A x B.
- Let R be a relation, $R \subseteq A \times B$. If (a, b) ∈ R, we write a R b.

- Example: S, a set of students; C, a set of courses @ UCD.
  - Let R = { (s, c) | student s is taking course c in SQ'2022}.
    - (Ashley, ECS020) ∈ *R* or Ashley R ECS020.
    - Many students may take the same course.
    - A single student may take many courses.

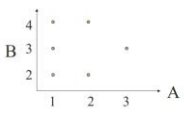
Relations *on* a Set

- A relation *on* a set A is a relation from A to A.

- Examples of relations *on* **R**:
  - $R_1 = \{ (a, b) \mid a \leq b \}$. $R_1 = \{ (0, 0), (0, 2), (1, \frac{7}{3}), (e, \pi), ... \}$
  - $R_2 = \{ (a, b) \mid b = +\text{sqrt}(a) \}$. $R_2 = \{ (1, 1), (3, \sqrt{3}), ... \}$
  - Are R_1 & R_2 functions? Put a pin in this for now...

Graph a Relation from A to B

- The word graph above is used as a verb.
- Let A = { 1, 2, 3 } and B = { 2, 3, 4 }.
- Let R be a relation from A to B where { (a, b) | a divides b }.



Properties of Relations

A relation R on A is:

- *Reflexive:* ∀a (aRa).

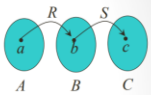
  Are either R_1 or R_2 reflexive?

  $R_1 = \{ (a, b) \mid a \leq b \}$.
  $R_2 = \{ (a, b) \mid b = + \sqrt{a} \}$.

- *Symmetric:* ∀a ∀b (aRb → bRa).
  - Let S be a set of people.
  - Let R & T be relations on S,

    R = { (a, b) | a is a sibling of b }.
    T = { (a, b) | a is a brother of b }.
    Is R symmetric? Is T symmetric?

Composition



- Let R be a relation from A to B.
- Let S be a relation from B to C.
- The *composition* is

  $S \circ R = \{ (a, c) \mid \exists b (aRb \wedge bSc) \}$.
- Let R be a relation *on* A.

  $R^1 = R$

  $R^n = R^{n-1} \circ R$.
- Let R = { (1, 1), (2, 1), (3, 2), (4, 3) }.

  What is R^2, R^3?