The University of New Mexico

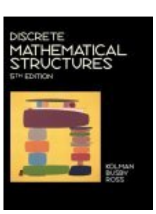
CS 261
Mathematical Foundations of Computer Science
University of New Mexico
Computer Science Department

Summer 2005

Taught by:
Joel Castellanos
FEC 319
e-mail joel@cs.unm.edu
web: http://cs.unm.edu/~joel/

Course Description

- This course is an introduction to the formal mathematical concepts of computer science for the beginning student. Topics include elementary logic, set theory, relations, deduction, induction, algorithmic processes, graph theory, and models of computation.
- Prerequisites:
  - CS-152L (Computer Programming Fundamentals)
  - Math-162L (Calculus I).



Discrete Mathematical Structures, 5th Edition.
By Kolman, Busby, and Ross

Grading

- Homework:
  - Problem sets assigned Mondays, Tuesdays, and Wednesdays.
  - Neither turned in nor graded.
  - Students are highly encouraged to work together.

- Quizzes:
  - Each Monday covering pervious week's homework.
  - Total of 7 quizzes.
  - Lowest two quiz grades dropped.
  - Each quiz counts as 10% of final course grade.

- Final Exam:
  - Two hour compressive exam
  - 50% of the final course grade.

What is Discrete Mathematics?

Discrete mathematics, is the study of mathematical structures that are fundamentally discrete, in the sense of not supporting or requiring the notion of continuity. Most of the objects studied in discrete mathematics are countable sets, such as the integers. For example, discrete mathematics uses summations rather than integrals used in calculus.

Discrete mathematics has become popular in recent decades because of its applications to computer science. Concepts and notations from discrete mathematics are useful to study or express objects or problems in computer algorithms and programming languages.

Discrete Mathematics usually includes the study of logic, set theory, number theory, combinatorial analysis, graph theory, algorithms, information theory, the theory of computability and complexity (a study on theoretical limitations on algorithms), elementary probability theory, Markov chains, linear algebra (matrix manipulations and related linear equations), and cryptology.

Sets

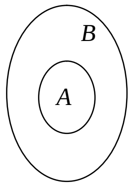
- Definitions:
  - A **set** is any well-defined collection of objects.
  - The objects in a set are called the **elements** or **members** of the set.
  - The order of elements in a set is not important.
  - Repeated elements in a set are ignored.
  - **Cardinality** of set A, $|A|$, is the number of elements contained in A.

- Examples:
  - People with brown hair enrolled at UNM (not well-defined).
  - Set of even integers greater than zero.

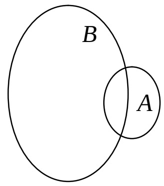
Set Notation

- Let $A = \{1, 3, 5, 7\}$. Then $1 \in A$, $3 \in A$, $2 \notin A$
- $Z = \{x \mid x \text{ is an integer}\}$
- $Z^+ = \{x \mid x \text{ is a positive integer}\}$.
- $N = \{x \mid x \text{ is a positive integer or zero}\}$.
- Empty set: { } or $\emptyset$.
- A is a subset of B: $A \subseteq B$, $A \subseteq A$.
- A is a proper subset of B: $A \subset B$, $A \not\subset A$.
- $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
- $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
- Universal Set (U): Assumed to contain all objects for which the discussion is meaningful.
- Cardinality of set A: $|A|$

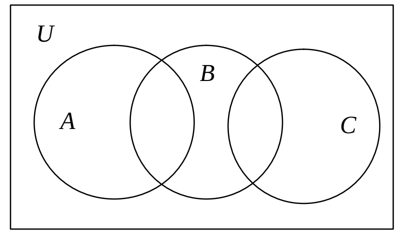
Venn Diagrams



$A \subseteq B$



$A \not\subseteq B$



$A \cup B = ?$

$A \cup B \cup C = ?$

$A \cap B = ?$

$A \cap B \cap C = ?$

Complement of A: $\overline{A} = \{x \mid x \notin A\}$

Symmetric difference: $A \oplus B = \{ x \mid (x \in A$ and $x \notin B)$ or $(x \in B$ and $x \notin A)$

Using Symmetric difference, write an expression for the elements of B that are not in A and not in C.

Exercise 1.1-15

Let $A = \{ 1,2,5,8,11 \}$.

- (a) $\{5,1\} \subseteq A$ True
- (b) $\{8,1\} \in A$ False
- (c) $\{1, 8, 2, 11, 5 \} \not\subset A$ False
- (d) $\varnothing \subseteq A$ True
- (e) $\{1, 6\} \not\subset A$ True
- (f) $\{2\} \subseteq A$ True
- (g) $\{3\} \notin A$ True
- (h) $A \subseteq \{11, 2, 5, 1, 8, 4 \}$ True

Exercise 1.1-17

Let A = {1},

B = {1, a, 2, b, c},

C = {b, c},

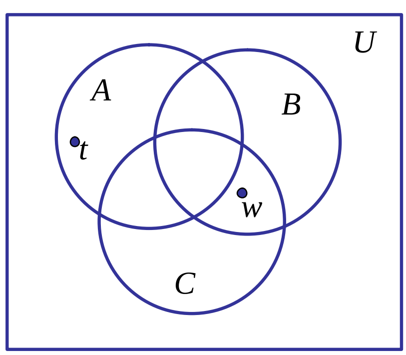
D = {a, b},

E = {1, a, 2, b, c, d }

(a) A Í B (b) ∅ Í A (c) B Ë C

(d) C Í E (d) D Ë C (e) B Í E

Exercise 1.1-23



(a) B Í A False

(b) A Í C False

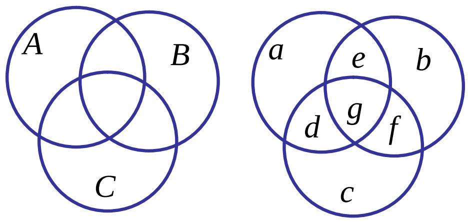
(c) C Í B False

(d) $w \in A$ False

(e) $t \in A$ True

(f) $w \in B$ True

Theorem 1.2-3



Where each lower case letter represents the cardinality of the elements within each non-overlapping area.

Theorem: Let A, B, and C be finite sets. Then
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Proof:

$$|A \cup B \cup C| = [a] + [b] + [c] + d + e + f + g$$
$$= [|A| - d - e - g] + [|B| - e - f - g] + [|C| - d - f - g] + d + e + f + g$$
$$= |A| + |B| + |C| - d - e - f - 2g$$
$$= |A| + |B| + |C| - (d+g) - (e+g) - (f+g) + g$$
$$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Exercise 1.2-24 – page 1 of 3

A survey of 500 television watchers produced the following information: $|U| = 500$

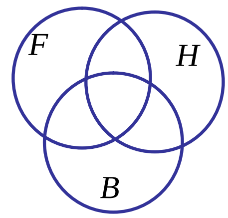
- 285 watch football games, $|F| = 285$
- 195 watch hockey games, $|H| = 195$
- 115 watch basketball games, $|B| = 115$
- 45 watch football and basketball games, $|F \cap B| = 45$
- 70 watch football and hockey games, $|F \cap H| = 70$
- 50 watch hockey and basketball games, $|H \cap B| = 50$
- 50 do not watch any of the games. $|\overline{F \cup H \cup B}| = 50$

(a) How many people in the survey watch all three kinds of games?

(b) How many people watch exactly one of the sports?

Exercise 1.2-24 – page 2 of 3

(a) How many people in the survey watch all three kinds of games?
That is, find $|F \cap H \cap B|$



From Theorem 1.2-3, we have

$|F \cup H \cup B| = |F| + |H| + |B| - |F \cap H| - |F \cap B| - |H \cap B| + |F \cap H \cap B|$

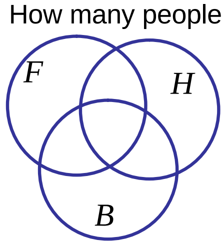
$500 - 50 = 285 + 195 + 115 - 70 - 45 - 50 + |F \cap H \cap B|$

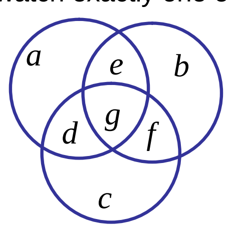
$450 = 595 - 165 + |F \cap H \cap B|$

$20 = |F \cap H \cap B|$

Exercise 1.2-24 – page 3 of 3

(b) How many people watch exactly one of the sports? [a + b + c]





Where each lower case letter represents the cardinality of the elements within each non-overlapping area.

From Theorem 1.2-3, we have

$|F \cup H \cup B| = a + b + c + d + e + f + g$

$500\text{-}50 = [a + b + c] + d + e + f + g$

$450 - d - e - f - g = [a + b + c]$

$450 - (d+g) - (e+g) - (f+g) + 2g = [a + b + c]$

$450 - 45 - 70 - 50 + 2(20) = [a + b + c]$

$325 = [a + b + c]$

Exercise 1.2-25 – page 1 of 3

The Journalism 101 class recently took a survey to determine where the city's people obtained their news. Unfortunately, some of the reports were damaged. What we know is that 88 people said they obtained their news from television, 73 from the local paper, and 46 from a news magazine. Thirty-four people reported that they obtained news from television and the local paper, 16 said they obtained their news from television and a news magazine, and 12 obtained theirs from the local paper and a news magazine. A total of five people reported that they used all three media. If 166 people were surveyed, how many use none of the three media to obtain their news? How many obtain their news from a news magazine exclusively?

$|T| = 88$ $\quad |P| = 73$ $\quad |M| = 46$

$|T \cap P| = 34$ $\quad |T \cap M| = 16$ $\quad |P \cap M| = 12$

$|T \cap P \cap M| = 5$ $\quad |U| = 166$

Exercise 1.2-25 – page 2 of 3

(a) How many use none of the three media to obtain their news?

Find: $|U| - |T \cup P \cup M|$

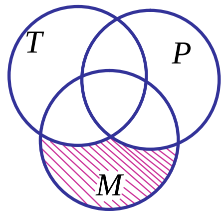
From Theorem 1.2-3, we have

$$|T \cup P \cup M| = |T| + |P| + |M| - |T \cap P| - |T \cap M| - |P \cap M| + |T \cap P \cap M|$$
$$= 88 + 73 + 46 - 34 - 16 - 12 + 5$$
$$= 150$$

$$|U| - |T \cup P \cup M| = 166 - 150$$
$$= 16$$

Exercise 1.2-25 – page 3 of 3

(b) How many obtain their news from a news magazine exclusively?



Fine the cardinality of the shaded area, m.

$m = |M| - |T \cap M| - |P \cap M| + |T \cap M \cap P|$

$|T \cap M \cap P|$ needs to be added on because it was subtracted twice.

m = 46 – 16 – 12 + 5

= 23

Exercise 1.2-27

In a psychology experiment, the subjects under study were classified according to body type and gender as follows:

	Endomorph	Ectomorph	Mesomorph
Male	72	54	36
Female	62	64	36

(a) How many male subjects were there? (72 + 54 + 36) = 162

(b) How many subjects were ectomorphs? (54 + 64) = 118

(c) How many subjects were either female or endomorphs?

(62 + 64 + 38) + 72 = 236

(d) How many subjects were not male mesomorphs?

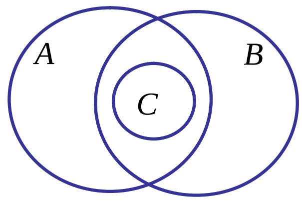
(62 + 64 + 36) + (72) + (54) = 290

(e) How many subjects were either male, ectomorph, or mesomorph?

(72 + 54 + 36) + (64) + (36) = 264

Exercise 1.2-32

(a) Draw a Venn diagram to represent the situation $C \subseteq A$ and $C \subseteq B$.



(b) To prove $C \subseteq A \cup B$, we should choose an element from which set?

Pick an element from C.

(c) Prove that if $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cup B$.

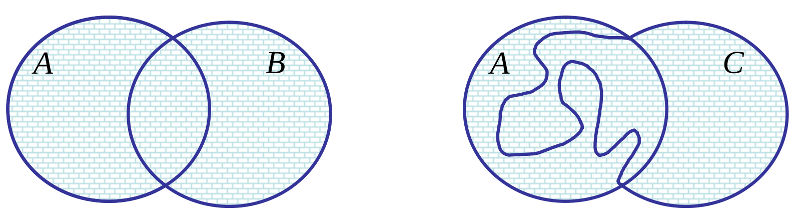
Let $x \in C$.

Then, $x \in A$ since $C \subseteq A$, and hence $x \in A \cup B$.

Note: we do not need that $C \subseteq B$.

Exercise 1.2-37

If $(A \cup B) = (A \cup C)$, must $B = C$? Explain.



No, B and C and are not necessarily equal. Just the elements of B and C that are outside of A must be equal.

Let $A = \{1, 2, 3\}$, $B = \{4\}$, and $C = \{3, 4\}$.

Then $A \cup B = \{1, 2, 3, 4\}$ and $A \cup C = \{1, 2, 3, 4\}$, yet $B \neq C$.

Comparing Cardinality of Infinite Sets

- Setting one-to-one a correspondence.
- Countably infinite, $\aleph_0$
- Set of Integers : Set of Positive Integers.
- Set of Positive Integers : Set of odd Integers.

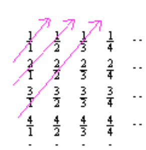
  $\aleph_0 = 2\ \aleph_0$
- Set of Positive Integers : Set of positive integers divisible by 1000.

  $\aleph_0 = 1000\ \aleph_0$

Cardinality of Set of all Rational Numbers

- First consider devising a one-to-one correspondence between N+ and the set of positive rationals.
- Recall that a positive rational number can be expressed as a quotient of two positive integers, consider this listing:

$$\begin{array}{ccccc} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \cdots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \cdots \\ \frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$



Clearly every positive rational number would be somewhere in this list. (some are listed many times, but that's OK.)

Correspondence: $1 \rightarrow 1/1$

$2 \rightarrow 2/1$

$3 \rightarrow 1/2$

$4 \rightarrow 3/1$

Sequences

A **Sequence** is a list of objects arranged in a definite order.

Powers of 2:

The **explicit** formula: $b_n = 2^{(n-1)}$, gives the sequence:

$b_1=1$, $b_2=2$, $b_3=4$, $b_4=8$, $b_5=16$, $b_6=?$, ...

Fibonacci sequence:

The **recursive formula** $f_n = f_{n-1} + f_{n-2}$, $f_1 = 1$, $f_2 = 1$, gives the sequence:

1, 1, 2, 3, 5, 8, 13, 21, ?, ?, ...

What is the value of f_{128}? - it is not easy to find.

Exercise 1.3

Write out the first four terms (begin with n=1) of the sequences whose general term is given.

8) $b_n = 3n^2 + 2n - 6$

$b_1 = 3(1)^2 + 2(1) - 6$	$= 3 + 2 - 6$	$= -1$
$b_2 = 3(2)^2 + 2(2) - 6$	$= 12 + 4 - 6$	$= 10$
$b_3 = 3(3)^2 + 2(3) - 6$	$= 27 + 6 - 6$	$= 27$
$b_4 = 3(4)^2 + 2(4) - 6$	$= 48 + 8 - 6$	$= 50$

14) $f_1 = 4$, $f_n = n \cdot f_{n-1}$

$f_2 = 2 \cdot f_{2-1}$	$= 2(4)$	$= 8$
$f_3 = 3 \cdot f_{3-1}$	$= 3(8)$	$= 24$
$f_4 = 4 \cdot f_{4-1}$	$= 4(24)$	$= 96$

Exercise 1.3

Write a formula for the n^{th} term of the sequence. Identify your formula as recursive or explicit.

18) 0, 2, 0, 2, 0, 2, ...

16) 0, 3, 8, 15, 24, 35, ...

20) 1, 1/2, 1/4, 1/8, 1/16, ...

22) 2, 5, 7, 12, 19, 31, 50, ...

Integer Divisors

Theorem 1.4-1: If n and m are integers and $n > 0$, we can write $m=kn+r$ for integers k and r with $0 \le r \le n$. Moreover, there is just one way to do this.

Theorem 1.4-2: Let a, b, and c be integers.

(a) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

Proof: If $a \mid b$ and $a \mid c$, then $b = k_1 a$ and $c = k_2 a$ for integers k_1 and k_2.
So $b + c = (k_1 + k_2)a$ and $a \mid (b + c)$

(b) If $a \mid b$ and $a \mid c$, where $b > c$, then $a \mid (b - c)$

Proof: See part (a)

(c) If $a \mid b$ or $a \mid c$, then $a \mid bc$.

Proof: We have $b = k_1 a$ or $c = k_2 a$. Then either $bc = k_1 ac$ or $bc = k_2 ab$.
In Either case, bc is a multiple of a and $a \mid bc$.

(d) If $a \mid b$ and $b \mid c$, then $a \mid c$.

```
public int GCD_decrementAlgorithm(int a, int b)
{ int i, k, r;
  int gcd = 0;
  if (a<b) i=a; else i=b;
  while (gcd == 0)
  {   k = a/i;
      r = a - k*i;
      if (r == 0)
      {   k = b/i;
          r = b - k*i;
          if (r == 0) gcd = i;
      }
      i--;
  }
  print("  Greatest Common Divisor = " + gcd);
  return i;
}
```

Euclidean Algorithm for Finding Greatest Common Divisor

Find GCD(a, b).

Suppose that $a > b > 0$

Then, by theorem 1, we may write:

$a = k_1 b + r_1$, where k_1 is in Z^+ and r with $0 \leq r_1 \leq b$.

Now Theorem 2 tells us that if n divides a and b, then it must divide r_1, since $r_1 = a - k_1 b$. Similarly, if n divides b and r_1, then it must divide a.

Therefore, the common divisors of a and b are the same as the common divisors of b and r_1, so GCD(a,b) = GCD(b, r_1).

This creates an iterative method for finding the GCD(a,b):

$k_1 = \text{int}(a/b)$ $\quad$ $r_1 = a - k_1 b$

$k_2 = \text{int}(b/r_1)$ $\quad$ $r_2 = b - k_2 r_1$

....

with $a > b > r_1 > r_2 > r_3 >$ ...., the remainder will eventually become zero.

```
public int GCD_EuclideanAlgorithm(int a, int b)
{ if (b > a)
  { int tmp = a;  a = b;  b = tmp;
  }
  int k = a/b;
  int r2 = a - k*b;
  int r1 = b;
  int r0 = 1;
  while (r2>0)
  { r0 = r1;
    r1 = r2;
    k = r0/r1;
    r2 = r0 - k*r1;
  }
  print("  Greatest Common Divisor = " + r1);
  return r1;
}
```

Decimal	Binary	Hexadecimal
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F
16	10000	10

Homework due Wednesday, June 8th

- Read Section 1.5
- Exercises 1.3:

  #7, #9, #11, #13,

  #15, #17, #19, #37, #39
- Exercises 1.4:

  #7, #11, #15, #24, #25, #33, #41, #42

Exercise 1.5 - #16

(a) Show that if **A** has a row of zeros, then **AB** has a corresponding row of zeros.

Generic element definition of **AB**:

If **A** = $[a_{ik}]$ is an m x p matrix and **B** = $[b_{ik}]$ is a p x n matrix, then the product of **A** and **B**, denoted **AB**, is the m x n matrix **C** = $[c_{ij}]$ defined by:

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{ip}b_{pk} \quad 1 \le i \le m, \quad 1 \le k \le n.$$

Let row z of **A** be a row of zeros. Then, $a_{z1}, a_{z2}, \dots, a_{zp} = 0$, and

$$c_{zk} = 0b_{1k} + 0b_{2k} + \dots + 0b_{pk} \quad 1 \le k \le n.$$

(b) Show that if **B** has a column of zeros, then **AB** has a corresponding column of zeros.

Let column z of **B** be a column of zeros. Then, $b_{1z}, b_{2z}, \dots, b_{pz} = 0$,

$$c_{iz} = a_{i1}0 + a_{i2}0 + \dots + a_{ip}0 \quad 1 \le i \le m,$$

Theorem 1.5 – 3 Proof

(a) $(\mathbf{A}^T)^T = \mathbf{A}$

Proof: $(a_{ik})^T = a_{ki}$, $(a_{ki})^T = a_{ik}$

(b) $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$

Proof: Let $\mathbf{C} = [c_{ik}] = (\mathbf{A} + \mathbf{B})^T$, and $\mathbf{D} = [d_{ik}] = \mathbf{A}^T + \mathbf{B}^T$

$$c_{ik} = a_{ki} + b_{ki} \qquad d_{ik} = a'_{ik} + b'_{ik} = a_{ki} + b_{ki} = c_{ik}$$

(c) $(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T$

Proof: Let $\mathbf{C} = [c_{ik}] = (\mathbf{AB})^T$, and $\mathbf{D} = [d_{ik}] = \mathbf{A}^T \mathbf{B}^T$, then

$$c_{ik} = \sum_{h=1}^{n} a_{kh} b_{hi}$$

$$d_{ik} = \sum_{h=1}^{n} b'_{ih} a'_{hk} = \sum_{h=1}^{n} b_{hi} a_{kh} = \sum_{h=1}^{n} a_{kh} b_{hi} = c_{ik}$$