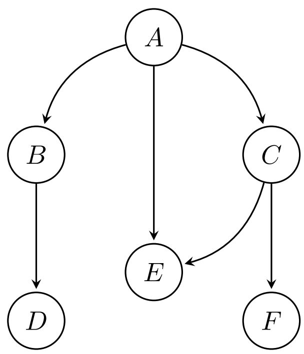
1 Formal Systems

1.1

A formal system has states $\{A, \ldots, F\}$ and rules R_1. Below is a graph showing all possible transitions between states.



1. Is derivation $A \Rightarrow^*_{R_1} F$ possible in the system? [1]
2. Is transition $A \Rightarrow_{R_1} D$ possible in the system? [1]
3. Express as a set the states that can be derived from A by a derivation of length 2 [1]

1.2

A string rewriting system is defined with the following rules R_2.

- $ba \curvearrowright ab$
- $ca \curvearrowright ac$
- $cb \curvearrowright bc$
- $da \curvearrowright ad$
- $db \curvearrowright bd$
- $dc \curvearrowright cd$
- $cba \curvearrowright abc$
- $dcba \curvearrowright abcd$

Let S_a be the string *cbadbd*

1. List all the strings S_b that can be derived from S_a in one step: $S_a \Rightarrow_{R_2} S_b$ [1]
2. Give strings S_b, S_c, S_t (where S_t is a terminal string), such that $S_a \Rightarrow_R S_b \Rightarrow_R S_c \Rightarrow_R S_t$. A terminal string is one from which no rule applications are possible. [1]

1.3

Give the terminal string for each string below (using rules R_2 defined above).

1. *cbabc* [1]
2. *badbba* [1]
3. *dabcbabad* [1]

1.4

For the following binary relations, state whether they are reflexive, symmetric, and/or transitive.

1. $\equiv$ [1]
2. $<$ [1]
3. $\geq$ [1]
4. $\neq$ [1]
5. taller than [1]

1.5

For the following table of binary operators, state whether they are commutative and/or associative.

1. $-$ (subtraction) [1]
2. $\cup$ [1]
3. $\setminus$ (set difference) [1]
4. $+$ (mod n) [1]
5. $\wedge$ [1]

2 Modular Arithmetic

2.1

Solve the following modular arithmetic questions

1. $[(12 \mod 5) + (14 \mod 5)] \mod 5$ [1]
2. $[(4 \mod 9) \times (0 \mod 9)] \mod 9$ [1]
3. $\left([(66 \mod 34) - (23 \mod 34)] \mod 34\right) \times (130 \mod 34)$ [1]
4. $9 \div 7 \pmod{13}$ [1]
5. $7 \div 5 \pmod{11}$ [1]

2.2

For each number below, give its modular inverse (if defined) under a modulus of 6, or answer 'undefined'

1. $0^{-1} \pmod 6$ [1]
2. $1^{-1} \pmod 6$ [1]
3. $2^{-1} \pmod 6$ [1]
4. $3^{-1} \pmod 6$ [1]
5. $4^{-1} \pmod 6$ [1]
6. $5^{-1} \pmod 6$ [1]

2.3

If subtraction under modulus were associative, which of the following statements would be true? [1]

1. $a - b \equiv b - c \pmod n$
2. $(b - a) - c \equiv bc - ac \pmod n$
3. $a - (b - c) \equiv (a - b) - c \pmod n$
4. $a - c - b \equiv b - (c - a) \pmod n$

2.4

What is the additive inverse of:

1. 14 [1]
2. $7 \pmod{13}$ [1]

2.5

Write the following as products of their prime factors in the form $f_1 \times f_2 \times f_3 \times \ldots$

1. 66 [1]
2. 95 [1]
3. 49 [1]
4. 154 [1]

2.6

Assume a string is encrypted using the encryption function $E(X) = (aX + b) \mod n$, where X is the index (starting at 0) of an element drawn from the alphabet [abcdefghijklmnopqrstuvwxyz0123456789], and n is the length of that alphabet.

1. Encrypt the string "hello" with keys $a = 7$, $b = 11$ [1]
2. Decrypt the string "8qvv fshq" with keys $a = 11$, $b = 16$ [1]

2.7

Let $p = 17$, $g = 11$. Alice generates a public key $A = 16$ using the following formula: $A = g^a \mod p$, where A is the public key and a is a private key.

1. Find a value for Alice's private key by brute force [1]
2. You pick a private key $b = 15$. Calculate your public key, $B = g^b \mod p$ [1]
3. A shared secret s can be calculated with the formula $s = A^b \mod p$, where A is Alice's public key, and b is your private key. Find s. [1]

2.8

jxu qdimuh veh jxyi gkuijyed yi 'qfhysej' [1]

3 Number Systems

3.1

Convert all the following values into each of: Binary, Octal, Decimal, and Hexadecimal

1. $(10101101)_2$ [1]
2. $(6346)_8$ [1]
3. $(953)_{10}$ [1]
4. $(1AA)_{16}$ [1]

3.2

Answer the following binary arithmetic questions. All numbers given are in binary. You can only store 8 bit numbers, higher bits overflow. Negative values should use twos complement. Give all your answers in binary with 8 bits.

1. $11100101 + 01100100$ [1]
2. $11010101 - 00001011$ [1]
3. $00110011 - 11000111$ [1]
4. 00011101×00001011 [1]
5. 11101001×00101001 [1]
6. $00111001 \div 00011100$ (report both quotient and remainder) [1]
7. $01001011 \div 000000111$ (report both quotient and remainder) [1]

3.3

Give the Ones' Complement of the following 8-bit binary number

1. 01010111 [1]

3.4

Give the Two's Complement for each of the following 8-bit binary numbers

1. 11101111 [1]
2. 00000000 [1]

3.5

The following signed numbers are represented in binary using 4 bits and sign and magnitude representation.

1. What is the additive inverse of 1011? [1]
2. What is 1110 in decimal? [1]
3. What is $1001 + 0101$ in binary (4 bits, sign and magnitude)? [1]

3.6

Give the greatest common divisor for each of the following pairs of numbers.

1. $(8, 13)$ [1]
2. $(34, 56)$ [1]
3. $(21, 29)$ [1]

3.7

What is the radix complement of the following numbers (assuming representation with 4 digits)?

1. $(9283)_{10}$ [1]
2. $(3321)_4$ [1]
3. $(BAA2)_{16}$ [1]

3.8

Assume base 32 is written with the alphabet $abcdefghijklmnopqrstuvwxyz012345$ Convert $(DBACA)_{16}$ into base 32 [1]

3.9

A national database assigns individuals a unique 10-character string of lower case letters. How many individuals could be recorded in this database before two would be assigned the same string? [1]

Marks on this page: 26

3.10

An online video host gives encodes video IDs using as few characters as possible, but all IDs are the same length. It can safely use numbers and upper and lowercase letters. What is the smallest number of characters that can encode the id 5730? [1]

4 Sequences and Summation

4.1

For each of the following, state whether the sequence is arithmetic or geometric, and give the next 3 values in the sequence

1. 19, 14, 9 [1]
2. 13, 39, 117 [1]

4.2

Give the first 5 elements of the following sequences:

1. $\{\frac{n!}{n}\}_{n=1}^{\infty}$ [1]
2. $\{i^i\}_{i=1}^{\infty}$ [1]
3. $a_n = a_{n-2} + 1$ where $a_1 = 1$ and $a_2 = 6$ [1]
4. $a_n = 5 \times 2^{n-1}$ [1]
5. $a_n = a_{n-1} \times a_{n-2}$ where $a_1 = 1$ and $a_2 = 2$ [1]

4.3

An arithmetic sequence has 10 terms and a common difference of $\frac{1}{2}$ and it's final term is 20.

1. Is this sequence increasing, decreasing, monotonic, and/or bounded? (List all that apply) [1]
2. Is 15.5 a lower bound for this sequence? [1]
3. Is $\frac{1}{20}$ an upper bound for this sequence? [1]

4.4

Solve the following summations

1. $\sum_{i=1}^{4} 7$ [1]
2. $\sum_{i=6}^{9} i + 2$ [1]
3. $\sum_{i=1}^{4} \frac{1}{i^2}$ (give a fraction in simplest form) [1]
4. $\sum A$ where $A = \{n\}_{n=1}^{3}$ [1]

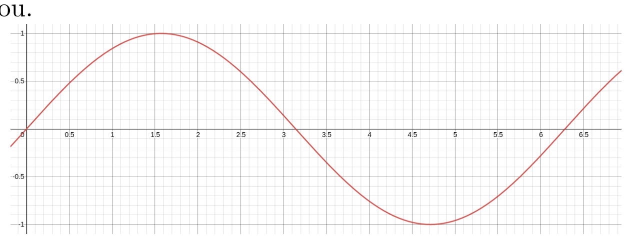
4.5

Solve the following products

1. $\prod_{k=1}^{4}(3k-2)$ [1]
2. $\prod_{k=7}^{11} 5$ [1]
3. $\prod A$ where $A = \{\frac{k}{k^2}\}_{k=1}^{5}$ (give a fraction in simpest form) [1]

4.6

Consider the sequence $S = \left\{\sin(n)\right\}_{n=1}^{\infty}$ The following plot of the function $y = \sin(x)$ is provided to help you.



1. Give a lower bound for this sequence that is also in this sequence. [1]
2. Is this sequence increasing, decreasing, monotonic, and/or bounded? (List all that apply) [1]

4.7

Simplify the following summations to the form $an^3 + bn^2 + cn + d$. For each, give values for a, b, c, d.

1. $\sum_{i=1}^{n} 7$ [1]
2. $\sum_{i=1}^{n}(2i+4)$ [1]
3. $\sum_{i=1}^{n}(6i^2+4i+1)$ [1]
4. $\sum_{i=1}^{n}\sum_{j=1}^{i}\sum_{k=1}^{j} 12$ [1]

5 Propositional Logic

5.1

When p is true and q is false, state whether the following statements are true or false

1. $\neg q \wedge \neg\neg q$ [1]
2. $(p \vee q) \wedge p$ [1]
3. $(p \implies \neg q) \implies q$ [1]
4. $p \iff (q \implies q)$ [1]
5. $\neg p \vee q \iff p \wedge q$ [1]

5.2

Let p be a true proposition and q be any proposition. Which of the following are true, and which of the following are false? (others might be true or false)

1. $p \iff q$ [1]
2. $\neg p \implies q$ [1]
3. $\neg q \implies p$ [1]
4. $p \implies \neg q$ [1]

5.3

For each, state whether the statement is always true, or if not give a case where it is false. You may wish to find this using a truth table.

1. $\neg(p \wedge q) \iff \neg p \vee \neg q \iff p \vee q$ [1]
2. $\neg(p \implies q) \implies p \wedge q$ [1]
3. $\neg\big(\neg(p \vee q) \wedge (p \vee \neg q)\big)$ [1]

5.4

For the following statements of propositional logic, state whether they are tautologies, contraditions, or contingiencies

1. p [1]
2. $\neg p \wedge p$ [1]
3. $(p \iff q) \implies p \vee \neg q$ [1]

5.5

Do the following properties hold of conjunction? You may wish to use either a truth table or Equational Reasoning to arrive at your answer.

1. Conjunction distributes over conjunction
$$(p \wedge (q \wedge r)) \iff (p \wedge q) \wedge (p \wedge r)$$
[1]
2. Conjunction distributes over disjunction
$$(p \wedge (q \vee r)) \iff (p \wedge q) \vee (p \wedge r)$$
[1]
3. Conjunction distributes over implication
$$(p \wedge (q \implies r)) \Leftrightarrow (p \wedge q) \implies (p \wedge r)$$
[1]

5.6

Prove the following by equational reasoning. Format your proof as in the lecture slides

1. $\neg\big(p \vee (p \wedge \neg p)\big) \vee p$ [2]
2. $p \wedge \neg(q \wedge \neg q) \iff p$ [2]

For this, use only the laws given in the lecture slides and the handout.

6 Set Theory

6.1

Define the following sets by extension

1. The set of natural numbers between 2 and 7 (inclusive) [1]
2. The set of subsets of the empty set [1]

6.2

State whether each of the following is a singleton, the empty set, or neither of these

1. The set of natural numbers, less the integers [1]
2. The set of real numbers, less the rational numbers [1]
3. The set of possible values of x in $\mathbb{R}$ when $x^2 = 2$ [1]
4. The proper subsets of the set $\{a\}$ [1]

6.3

Give the extension of the following sets

1. $\{a\} \cap \{b, c, d\}$ [1]
2. $\{a, b\} \cup \{a, c\}$ [1]
3. $\{b, c\} \setminus \{a, b, d\}$ [1]
4. $\{a\} \cap (\{a, b, d\} \setminus \{b, c\})$ [1]
5. $(\{c\} \cup \{b\} \cup \{a\}) \setminus (\{b, c, a\} \cup \emptyset)$ [1]

6.4

For the given sets, state whether the following propositions are true or false
$A = \{a, b\}$
$B = \{a, c, d\}$
$C = \{c, d\}$

1. $B \supset A$ [1]
2. $(B \setminus A) \subseteq C$ [1]
3. $b \in (A \cap B)$ [1]
4. $a \notin (B \setminus C)$ [1]
5. $(B \cap \{d, a\}) \supseteq B$ [1]

6.5

For the given sets, give the extension of the following sets
$A = \{a, b, c\}$
$B = \{a, d\}$
$C = \{c\}$

1. $(A \cup B) \setminus C$ [1]
2. $(B \cup C) \cap A$ [1]
3. $A \setminus (B \cup (A \setminus (B \cap A)))$ [1]

6.6

Use equational reasoning to prove the following. Reference the laws of set theory and propositional logic introduced in the lectures and on the handout.

1. $S \not\subset \big(S \cap (S \setminus \emptyset)\big)$ [2]
2. $\big((R \setminus S) \cap (R \setminus \emptyset)\big) \subseteq \big(R \setminus (S \cap R)\big)$ [2]

Marks on this page: 23

8 Set Theory 2

8.1

Give the cardinality of the following sets (state if infinite), where
$A = \{a, b, c\}$
$B = \{a, b, d\}$
$C = \{a, c, d, e\}$

1. $\{a, b, c, d\}$ [1]
2. $\bigcap\{A, B, C\}$ [1]
3. $\mathbb{P}(\{a, b\})$ [1]
4. $\mathbb{N} \setminus \mathbb{Z}$ [1]
5. $\mathbb{R} \setminus \mathbb{Q}$ [1]
6. $\bigcup\{A, B, C\}$ [1]

8.2

Given the following, which of the statements can be true?

- $\#A = 7$
- $\#B \setminus C = 6$
- $\mathbb{P}(A \cap B) = 4$
- $C \subseteq (A \cup B)$
- $\#\bigcap\{A, B, C\} = \emptyset$
- $\#A \setminus (B \cup C) = \#C$

1. $A \setminus C = B \setminus C$ [1]
2. $A \cap C = 3$ [1]
3. $\mathbb{P}(B) \in \{7, 9, 11\}$ [1]
4. $A \times B = 18$ [1]
5. $B \cap C = A \setminus B$ [1]
6. $A \setminus B = 6$ [1]

8.3

Give the extension of the following sets, given
$A = \{a, b\}$
$B = \{a, b, c, d\}$

1. $\mathbb{P}(A)$ [1]
2. $\bigcup \mathbb{P}(B)$ [1]
3. $\{a, b\} \times A$ [1]
4. $A \times \{1\}$ [1]

8.4

Give the extension of the following sets

1. $\{n : \mathbb{N} \mid 4 > n > 2\}$ [1]
2. $\{n : \mathbb{N}^0 \mid n < 10 \land n \mod 2 = 0\}$ [1]
3. $\{n : \mathbb{N} \bullet 2 + (n \mod 5)\}$ [1]
4. $\{a : \mathbb{N}; b : \mathbb{N} \mid a \mod 3 = b \bullet b\}$ [1]
5. $\{a : \mathbb{N}^+; b : \mathbb{N}^+ \mid a + b < 4\}$ [1]

8.5

Define by extension the set containing the smallest four elements of the following sets (give fractional values as fractions (e.g. 1/2)):

1. $\{n : \mathbb{N}^+ \bullet 2^n\}$ [1]
2. $\{n : \mathbb{N}^+ \bullet \frac{n+1}{n}\}$ [1]
3. $\{n : \mathbb{N}^+; i : \mathbb{N}^+ \mid n \times i \leq 9 \bullet n\}$ [1]

8.6

Given the table below, with types Name, Grade, and Day, give the extensions of the following sets

Name	Grade	Day
Alice	3	Monday
Bob	4	Monday
Eve	6	Tuesday
Mary	3	Wednesday

1. $\{x : Day \times Grade \mid \text{ true}\}$ [1]
2. $\{x : Name \times Grade \mid x.2 < 5 \bullet x.1\}$ [1]
3. $\{x : Name \times Grade \times Day \mid x.3 = Monday \bullet (x.2, x.1)\}$ [1]
4. $\{a : Name \times Grade \times Day; b : Name \times Grade \times Day \mid a.2 = b.2 \lor a.3 = b.3 \land a \neq b \bullet \{a.1, b.1\}\}$ [1]

8.7

The following is a list of set comprehensions for the table given above. For each description given below, identify which is the matching set comprehension by giving the letter

(a) $\{x : Name \times Day; y : Name \times Day \mid x.2 = y.2 = Monday \wedge x.1 \neq y.1 \bullet (x.1, y.1)\}$

(b) $\{x : Name \times Day \times Grade \mid 5 \leq x.3 \leq 8\}$

(c) $\{x : Name \times Day; y : Name \times Day \mid y.2 = Monday \bullet x.1\}$

(d) $\{x : Name \times Grade \times Day \mid x.3 = Monday \vee 5 \leq x.2 \leq 8\}$

(e) $\{x : Name \times Day \times Grade \mid x.2 = Monday \vee 5 \leq x.2 \leq 8\} \bullet x$

(f) $\{x : Grade \times Day; y : Name \times Day \mid 5 \leq x.1 \leq 8 \wedge y.2 = Monday \bullet x.2\}$

(g) $\{x : Name; y : Name \mid \text{true}\}$

(h) $\{x : Name \times Day \times Grade \mid 5 \leq x.3 \leq 8 \bullet (x.1, x.2)\}$

(i) $\{x : Name \times Grade \times Day; y : Name \mid \text{true}\}$

(j) none of the above

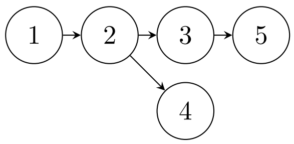
1. The set of all names [1]
2. The set of days containing someone in grade 5–8 [1]
3. The set of Name, Day tuples for everyone in grades 5–8 [1]
4. The set of Name, Grade, Day tuples for everyone who either has a class on Monday or is in grades 5–8 [1]
5. The set of pairs of (different) names that both have a class on Monday [1]

Marks on this page: 5

9 Graph Theory

9.1

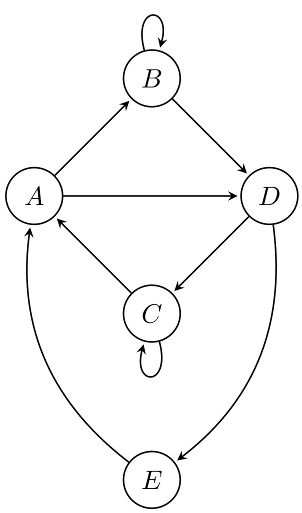
Consider the following graph.



1. Is it directed, strongly connected, and/or cyclic? [1]
2. Give the min. and max. degree of the graph [1]
3. Give the degree of node 3 [1]
4. Write the longest directed path in this graph as a list of nodes [1]

9.2

Consider the following graph.



1. Is it directed, strongly connected, and/or cyclic? [1]
2. Give the min. and max. degree of the graph [1]
3. What is the in- and out-degree of node D? [1]
4. List the nodes with loops in this graph as a set [1]
5. Write a shortest simple cycle (excluding loops) in this graph as a list [1]

9.3

A graph G is defined as $G = \{V, E, \Phi\}$, where $V = \{a, b, c\}$, and $E = \{e_1, e_2\}$, and $\Phi = \{(e_1, (a, b)), (e_2, (b, a))\} \times V$

1. Is it directed, connected, and/or cyclic? [1]
2. How many strongly connected components does it contain? [1]

10 Probability

In this section, give any non-whole-numbered answers as fractions in simplest form.

10.1

You have 3 fair 20-sided dice. What is the probability of rolling:

1. The sequence [20, 19, 18] [1]
2. At least two 20s [1]
3. An sequence of three ascending primes in order (e.g. 2,3,5 or 3,5,7, but not 2,7,13) [1]

10.2

Let $P(A) = \frac{1}{8}$, $P(B) = \frac{1}{4}$, and $P(C) = \frac{1}{6}$. You know that events B and C are independent, and that $P(A \mid B) = \frac{1}{8}$. Calculate the following:

1. $P(A \cap B)$ [1]
2. $P(B \cup A)$ [1]
3. $P(B \cup C)$ [1]
4. $P(A')$ [1]
5. $P(C \mid B)$ [1]
6. $P(B \mid A)$ [1]

10.3

Calculate the following

1. ${}^7P_4$ [1]
2. ${}^6C_3$ [1]

10.4

1. How many ways are there to order the set {a, b, c, d, e} ? [1]
2. A retro games console can produce 256 unique colours, but only 8 can be displayed at a time, thus a game must pick a palate of 8 colours out of these 256 colours. How many possible palates are there? [1]

10.5

Events $A_1, \dots A_n$, partition a sample space.

1. What is $\sum_{i=1}^{n} P(A_i)$? [1]

10.6

You have 3 bags of balls, their colours are described in the table below.

Bag	Red Balls	Black Balls
Bag 1	3	5
Bag 2	1	3
Bag 3	6	8

You pick a bag at random but are twice as likely to pick bag 3 than any other individual bag. You draw a random ball from the bag you pick. What is the probability that you draw a red ball? [1]

10.7

What is the probability that a student who passed their exam attended lectures, given: $\frac{3}{4}$ of students attend lectures; $\frac{3}{5}$ of students pass their exam; and of those who attend lectures, $\frac{7}{10}$ pass their exam. [1]

10.8

You have 3 hypotheses that are disjoint and collectively exhaustive, H_1, H_2, H_3. The prior probability of each being true, and conditional probabilities that each is true given the event E are given in the table below.

H_n	$P(H_n)$	$P(E \mid H_n)$
H_1	1/6	3/4
H_2	2/6	2/4
H_3	3/6	1/4

Calculate posterior probabilities $P(H_n \mid E)$ for all three hypotheses. [3]

Marks on this page: 19

12 Descriptive Statistics

12.1

A utility company collects the type of data described below in a survey. In each case say whether the data is nominal, ordinal, or numeric, and give the most appropriate measure of central tendancy to use to describe such data

1. Water pressure [1]
2. Town [1]
3. Customer satisfaction on a 5-point Likert scale (scale from 1-5) [1]

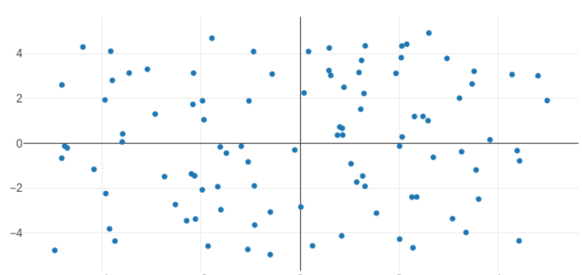
12.2

The following data represents a sample of water pressure data collected by the utility company (expressed in bars). Give answers to 2 decimal places.
3.10, 2.75, 3.45, 3.05, 3.33, 2.98, 2.85, 3.21, 2.22

1. Median [1]
2. Arithmetic mean [1]
3. Arithmetic mean excluding outliers using Tukey's Fences with a value of $k = 1.5$ [1]
4. An appropriate form of standard deviation [1]

12.3

What is the approximate correlation of the data shown? Pick the closest out of $\{-1, -0.5, 0, 0.5, 1\}$ [1]



12.4

A variable X follows a normal distribution. Estimate parameters μ and σ of this distribution from the following sample. Give your answers to 1 decimal place.

1. -9, 10, -3, 17, 25, 18, 20, 10, -5, 9 [1]
2. Is X discrete or continuous? [1]
3. What is $P(X = 10)$? [1]

12.5

Let Y be a variable following a binomial distribution defined by the variables $n = 4$ and $p = 0.5$. Give your answers as fractions in simplest form.

1. Is Y discrete or continuous? [1]
2. What is $P(Y = 2)$? [1]
3. What is $P(Y > 2)$? [1]

Marks on this page: 14