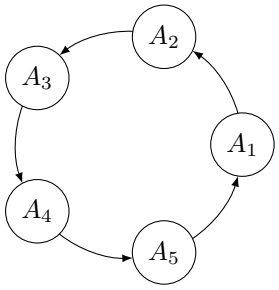
1 Formal Systems

1.1

A formal system has states $A_1, \ldots, A_5$ and rules R. Below is a graph showing all possible transitions between states.



1. Is the derivation $A_1 \Rightarrow_R^* A_5$ possible within this system?
2. If so, provide a derivation.

1.2

A formal system has states $X_1, \ldots, X_7$. The rules R are such that from a state X_i it is possible to derive the state X_{i+1}

1. List the steps in the derivation $X_1 \Rightarrow_R^* X_7$
2. What is the length of this derivation?
3. Is there a derivation $X_4 \Rightarrow_R^* X_3$?

1.3

A string rewriting system has the following rules R.

- $aba \curvearrowright b$
- $aaa \curvearrowright$

Let A be the string *aaaababbbbabababaaaababa*

1. List all the strings B that can be derived from A in one step: $A \Rightarrow_R B$
2. List the strings in one possible derivation of T, $A \Rightarrow_R^* T$, where T is a terminal state (where no further rule applications are possible)

1.4

A string rewriting system is defined with the following rules.

- $(fof) \curvearrowright f$
- $(tof) \curvearrowright t$
- $(fot) \curvearrowright t$
- $(tot) \curvearrowright t$

For each of the following, derive a terminal string (where no further rule applications are possible)

1. $((fot)ot)$
2. $((fof)o(tot))$
3. $(((tof)of)o(fo(fof)))$
4. Give a string from which the string f is derivable by a derivation of length 3

1.5

For the following binary relations, state whether they are: Reflexive, Symmetric, Transitive

1. $=$
2. $>$
3. $\leq$
4. $\neq$
5. older than
6. can be rotated (by some angle) to get

1.6

For the following table of binary operators, state whether they are: Commutative, Associative

1. $+$
2. $\times$
3. $\div$
4. $\times \pmod n$
5. $\div \pmod n$

2 Modular Arithmetic

2.1

Solve the following modular arithmetic questions

1. $(13 \mod 3) + (23 \mod 4)$
2. $(22 \mod 7) \times (13 \mod 7)$
3. $(14 \mod 55 + 42 \mod 55) \times (13 \mod 55)$
4. $11 \div 7 \pmod{13}$
5. $4 \div 11 \pmod{17}$

2.2

For each number below, give its modular inverse (if defined) under a modulus of 8

1. $0^{-1} \pmod 8$
2. $1^{-1} \pmod 8$
3. $2^{-1} \pmod 8$
4. $3^{-1} \pmod 8$
5. $4^{-1} \pmod 8$
6. $5^{-1} \pmod 8$
7. $6^{-1} \pmod 8$
8. $7^{-1} \pmod 8$

2.3

If multiplication distributes over subtraction under modulus then, which of the following statements are true

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

2.4

What is the additive inverse of:

1. 24
2. 5 (mod 17)
3. $a \mod b$ (give your answer as a formula)

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. 68
2. 123
3. 92
4. 44

2.6

Assume a string is encrypted using the encryption function $E(X) = (aX + b) \bmod n$, where X is the index 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=4
2. Decrypt the string "q4zajep" with the same keys

2.7

Assume $p = 23$, $g = 7$. Alice generates a public key $A = 11$ 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
2. You pick a private key $b = 11$. Calculate your public key, $B = g^b \mod p$
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.

2.8

The following strings have been encrypted using the function $E(X_i) = (X + k + i) \mod 26$, where i is the 1-based index of the character in the word to encrypt (ignoring spaces). For each, give a value for k.

1. "kxbcqph" (The first letter of plaintext is 'c')
2. "lacn ep gs" (The plaintext is a sentence)

2.9

VCKIVHH GSV UFMXGRLM FHVW GL VMXIBKG GSRH GVCG FHRMT Z ULINFOZ

3 Number Systems

3.1

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

1. $(01100011)_2$
2. $(0257)_8$
3. $(611)_{10}$
4. $(19F)_{16}$

3.2

Answer the following binary arithmetic questions. All numbers given are in binary. Representations use the number of bits shown. Give your answers in binary.

1. $0101011 + 1101011$
2. $1101 - 1011$
3. $00010100 - 10101000$
4. 1101×1010
5. 11101001×00101001
6. $01001011 \div 00010111$ (report both quotient and remainder)
7. $1011 \div 0101$ (report both quotient and remainder)

3.3

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

1. 10000000
2. 10100111
3. 01101011

3.4

Calculate the answers to the following, working with 8-bit signed binary numbers **stored as sign and magnitude**

1. What is the additive inverse of 01101111?
2. $00110001 + 11001101$
3. $10010101 - 00101010$

3.5

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

1. $(3, 7)$
2. $(14, 39)$
3. $(11, 23)$

3.6

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

1. $(52342)_{10}$
2. $(00231)_4$
3. $(01FA)_{16}$

3.7

Assume base 32 is written with the alphabet [0-9A-V] Convert $(321223123212)_4$ into base 32

3.8

A 23 digit number in base 536 can store how many different values?

3.9

A web application needs to encode session ids in as few characters as possible. It can safely use numbers and upper and lowercase letters. What is the smallest number of characters that can encode the id 2348923947234?

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. 1, 7, 13
2. 0.9, 0.6, 0.4
3. 2k, 6k, 18k

4.2

Give the first 5 elements of the following sequences:

1. $\{\frac{n^2}{n-1}\}_{n=1}^{\infty}$
2. $\{i^3\}_{i=3}^{\infty}$
3. $a_n = a_{n-1} + 3$ where $a_1 = 22$
4. $a_n = 14 \times 3^{n-1}$

4.3

A geometric sequence has 10 terms and a common ratio of $\frac{1}{10}$ and it's final term is 10^{-8}.

1. Is this sequence increasing, decreasing, monotonic, and/or bounded? (List all that apply)
2. Is -10 a lower bound for this sequence?
3. Is 1 an upper bound for this sequence?

4.4

Solve the following summations

1. $\sum_{i=1}^{5} 2$
2. $\sum_{i=4}^{7} i$
3. $\sum_{i=1}^{3} 2^i$
4. $\sum A$ where $A = \{n^2\}_{n=1}^{7}$

4.5

Solve the following products

1. $\prod_{k=1}^{3}(2k+1)$
2. $\prod_{k=7}^{17} 2$
3. $\prod A$ where $A = \{\frac{1}{k}\}_{k=1}^{4}$

4.6

Consider the sequence $S = \{\frac{n}{n+1}\}_{n=1}^{\infty}$

1. Give a lower bound for this sequence that is also in this sequence.
2. What is a number that this sequence will approach, but never quite reach?
3. Is this sequence increasing, decreasing, monotonic, and/or bounded? (List all that apply)

4.7

Simplify the following summations

1. $\sum_{i=1}^{n} c$
2. $\sum_{i=1}^{n}(i+2)$
3. $\sum_{i=1}^{n}(i^2+3i)$
4. $\sum_{i=1}^{n}\sum_{j=1}^{i} j$
5. $\sum_{i=1}^{n} A_i$ where $A_n = A_{n-1} + \frac{1}{2}$ and $A_1 = \frac{1}{2}$

5 Propositional Logic

5.1

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

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

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. $p \implies q$
2. $q \implies p$
3. $\neg q \implies p$
4. $\neg p \implies q$

5.3

Construct a truth table for each of the following. For each, state whether the statement is always true, or if not give a case where it is false.

1. $p \implies (q \implies (r \implies p))$
2. $p \vee \neg r \implies (\neg(r \wedge p)$

5.4

Identify the atomic propositions in the following sentences and assign them each a letter (e.g. b = "the bus is late") Then express this as a statement of propositional logic using the notation taught in class

1. If my bike is not working or the bus is late, then I am late for class
2. I am happy if and only if I am riding my bike

5.5

For the following, state whether they are tautologies, contraditions, or contingiencies

1. $p \implies (\neg p \vee p)$
2. $p \vee q \implies p \wedge q$
3. $\neg p \vee \neg\neg p$
4. $p \vee \neg(p \vee \neg p)$

5.6

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

1. Implication distributes over conjunction

   $$(p \implies (q \wedge r)) \iff (p \implies q) \wedge (p \implies r)$$

2. Implication distributes over disjunction

   $$(p \implies (q \vee r)) \iff (p \implies q) \vee (p \implies r)$$

3. Implication distributes over implication

   $$(p \implies (q \implies r)) \Leftrightarrow (p \implies q) \implies (p \implies r)$$

5.7

Prove the following by Equational Reasoning. Format your proof as in the lecture slides

1. $p \implies (p \vee \neg p)$
2. $\neg p \wedge \text{true} \iff \neg p$

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 6 and 11 (not inclusive)
2. The set of letters in the phrase "formal systems, logic, and semantics"
3. The set of sets with exactly one subset

6.2

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

1. The set of Real numbers, less the Natural numbers
2. The set of even primes
3. The set of digits used in binary
4. The set black hearts in a standard deck of cards
5. A set that has no proper subsets
6. A set with exactly two subsets

6.3

Give the extension of the following sets

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

6.4

For the given sets, state whether the following propositions are true or false

$A = \{a, b, c\}$
$B = \{a, d\}$
$C = \{c\}$

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

6.5

For the given sets, give the extension of the following sets

$A = \{a, b, c\}$
$B = \{a, d\}$
$C = \{c\}$

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

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. $S \subseteq (T \cup (S \cap S))$
2. $(S = T) \wedge (T \not\subseteq S) \iff \text{false}$
3. $\emptyset \not\subset ((S \cap S) \setminus (S \setminus \emptyset))$

8 Set Theory 2

8.1

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

1. $\{7, 8, 8\}$
2. $\bigcap\{A, B, C\}$
3. $\mathbb{P}(\{a, b, c\})$
4. $\mathbb{N}^0 \setminus \mathbb{N}^+$
5. $\mathbb{Q} \setminus \mathbb{R}$
6. $\bigcup\{A, B, C\}$

8.2

Give the cardinality of the following sets, given:

- $\#A = 4$
- $\#B = 6$
- $\mathbb{P}(C) = 8$
- $\#(A \cap B) = 1$
- $C \subseteq A$
- $\#(C \cap B) = \emptyset$

1. $A \cup B$
2. $\mathbb{P}(A \setminus B)$
3. $C \cap A$
4. $B \cup C$
5. $A \times B$
6. $B \setminus C$

8.3

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

1. $\mathbb{P}(A)$
2. $\bigcup\mathbb{P}(B)$
3. $\{a, b\} \times A$
4. $\mathbb{P}(\emptyset)$
5. $(\{1\} \times \{a, b\}) \cap (\{1, 2\} \times \{b, a\})$

8.4

Give the extension of the following sets

1. $\{n : \mathbb{N} \mid n \mod 3 = 1 \land n < 13\}$
2. $\{n : \mathbb{N} \mid 4 < n < 7\}$
3. $\{n : \mathbb{N} \bullet n \mod 7\}$
4. $\{a : \mathbb{R}; b : \mathbb{R} \mid a^2 = b \land b^2 = a \bullet a\}$
5. $\{a : \mathbb{N}^+; b : \mathbb{N}^+ \mid a + b < 3 \bullet (a, b)\}$

8.5

Define by extension the set containing the smallest four elements of the following sets:

1. $\{n : \mathbb{N}^+ \bullet n^n\}$
2. $\{n : \mathbb{N}^+ \bullet \frac{n}{n+1}\}$
3. $\{n : \mathbb{Z} \mid n^2 \leq 16\}$

8.6

Given the table below, with types Name, Age, and Group, give the extensions of the following sets

Name	Age	Group
Alice	18	A
Bob	17	B
Eve	19	A
Mary	22	B

1. $\{x : Group \times Name \mid \text{ true}\}$
2. $\{x : Name \times Age \mid x.2 \geq 18 \bullet x.1\}$
3. $\{x : Name \times Age \times Group \mid x.3 = A\}$
4. $\{a : Name \times Group; b : Name \times Group \mid a.2 = b.2 \bullet \{a.1, b.1\}\}$

8.7

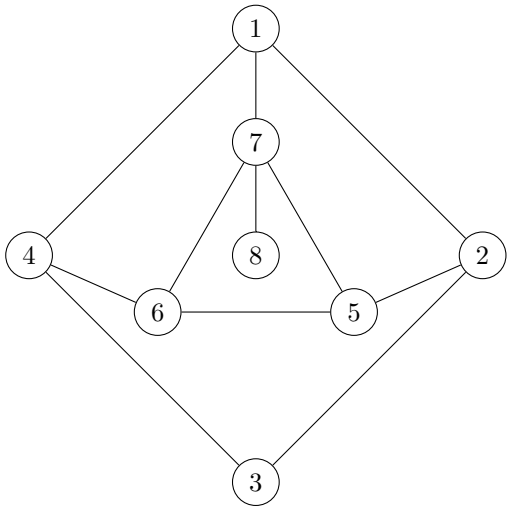
For the table given above, define the following sets by set comprehension:

1. The set of all names
2. The set of groups containing someone under the age of 18
3. The set of Name, Age tuples for someone whose age is a multiple of 3
4. The set of Name, Age, Group tuples for everyone who isn't called Alice

9 Graph Theory

9.1

Consider the following graph.



1. Is it directed, connected, and/or cyclic?
2. Give the min. and max. degree of the graph
3. What is the degree of node 4?
4. List the loops in this graph as a set
5. Write a simple cycle in this graph as a list
6. Write a simple path that connects every node in this graph as a list
7. Write a shortest path connecting every even-numbered node as a list

9.2

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

1. Is it directed, connected, and/or cyclic?
2. How many nodes and edges does it contain?
3. Give the min. and max. degree of the graph

9.3

A formal string-rewriting system is defined with the rules below. The starting string is a

- $a \rightsquigarrow aba$
- $bab \rightsquigarrow b$

1. Draw a graph of the first 5 unique strings that can be constructed in this system, where edges represent applications of one of the grammatical rules

9.4

Below is a database for a Twitter-like social network

Username	Following	Posts
Alice	{Bob, Eve}	24
Bob	{Alice, Eve}	3
Eve	{Alice, Mary}	124
Mary	{Eve}	10

We can produce a graph of this social network $G = (V, E)$ where $V = \{x : \text{Username} \mid \text{true}\}$, and E is a set of directed edges (a, b) where A 'follows' B.

1. Give an extensional definition of E
2. Give an intensional definition of E using set comprehension
3. List of followers: Give a set comprehension that returns a tuple (a, b), where a is a username and b is a person following that user
4. Follow recommendation: Give a set comprehension that returns a tuple (a, b), where a is a username and b is a username of someone a might like to follow (a might 'like to follow' b if and only if b is followed by someone a follows, a does not already follow them, and a and b are not the same person).

10 Probability

10.1

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

1. 3 sixes
2. At least 2 sixes
3. An ascending sequence $\{n, n+1, n+2\}$ in order (e.g. 1,2,3 or 3,4,5)

10.2

Let $P(A) = 0.25$, $P(B) = 0.5$, and $P(C) = 0.75$. You know that events B and C are independent, and that $P(A \mid B) = 0.1$. Calculate the following

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

10.3

Calculate the following

1. 4!
2. 0!
3. ${}^4P_3$
4. ${}^8C_7$

10.4

1. How many combinations of four unique 8-bit binary numbers are possible?
2. I define an ordering over the set {a, b, c, d}. How many possible orderings can I define?
3. A industrial robot is designed to carry 4 objects simultaneously. Each object is carried by one of 4 differently positioned and proporitioned arms. Each object can be in one of 6 weight categories. To exhaustively test that the robot will never overbalance on any set of weights, how many tests must be run?

10.5

A_1, and A_2 partition a probability space. B_1, B_2, and B_3 partition the event A_1. There is an event C, such that $P(C) = \frac{1}{2}$, and $P(C \mid A_2) = 0$

1. What is $\sum_{i=1}^{3} P(C \mid B_i)$?

10.6

You have 3 bags of balls that each contain 80 balls, their colours are described in the table below.

Bag	Red Balls	Black Balls
Bag 1	65	15
Bag 2	23	57
Bag 3	23	57

You pick a bag at random and pick a random ball from that bag. What is the probability that you pick a red ball?

10.7

What is the probability that a student who passed their exam attended lectures, given: 80% of students attend lectures; 80% of students pass their exam; and of those who attend lectures, 95% pass their exam

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	3/8	2/6
H_2	1/8	2/6
H_3	4/8	1/6

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

12 Descriptive Statistics

12.1

For the following types of data, say whether they are nominal, ordinal, or numeric, and give the most appropriate measure of central tendancy to use to describe such data

1. Duration of daily commute
2. Frequency in Hz
3. DEFCON level[1]
4. Brands of espresso maker

12.2

For the following data calculate the median and mode(s). Use Tukey's Fences with a value of $k = 1.5$ to exclude outliers before calculating the mean.

1. 4, 2, 5, 2, 34, 2, 4
2. 1, 4, 6, 2, 4, 3, 1

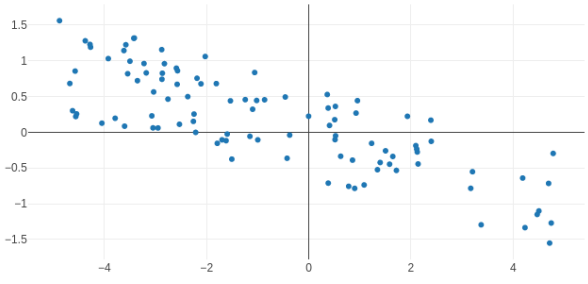
12.3

The following data represents a sample of scores collected from two levels of a mobile game. For each, calculate the range, inter-quartile range, and an appropriate form of standard deviation.

1. 1, 9, 3, 9, 23, 5, 3, 6
2. 5, 2, 14, 25, 14, 11, 5

12.4

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



[1]See `https://en.wikipedia.org/wiki/DEFCON`

12.5

8 bytes of data are transmitted over a noisy channel. For every bit transmitted, the probability of the bit being flipped (a transmission error) is 10^{-2}. What is the chance that at least one error occours?

12.6

The time taken to sort an array using Insertion Sort is $n(n+1)/2$, where n is the size of the array. You use Insertion Sort on 100 arrays which are uniformly distributed in length between 1 and 100 elements.

1. What is the total time taken?
2. What is the mean time per array?

12.7

You flip an unfair coin 6 times. The probability of heads is 0.2. The number of heads is given by the variable X.

1. What is $P(X = 2)$?
2. What is the most likely value of X (mode)?
3. What is $\sum_{i=0}^{6} P(X = i)$?

12.8

Let Y be a continuous variable uniformly distributed between 0 and 1.

1. What is $P(Y = 0.1)$?
2. What is $P(Y > 0.6)$?

12.9

A variable Z is defined by a normal distribution where $\mu = 0$ and $\sigma = 1$.

1. What is the median value of Z?
2. What is $P(-2 < Z < 2)$, approximately?
3. What is the (approximate) probability of generating a value of Z that is greater than 2?