MAU22C00 - TUTORIAL 1

1) Give an example of sentences P and Q such that the implication $P \to Q$ is true, but its converse $Q \to P$ is false. Give another example of sentences P and Q such that the implication $P \to Q$ is true and its converse $Q \to P$ is also true. Given an implication $P \to Q$, what can you deduce about the truth value of its converse?

2) Suppose we are told the following:
If turtles can sing then artichokes can fly. Artichokes can fly implies turtles can sing and dogs can't play chess. Dogs can play chess if and only if turtles can sing.
Deduce that turtles can't fly.

3) Prove that the order of quantifiers cannot be reversed without potentially modifying the truth value by providing a counterexample. The easiest counterexample can be given for two quantifiers. Find a sentence in predicate logic $P(x, y)$ such that $\forall x \, \exists y \, P(x, y)$ is true, but $\exists y \, \forall x \, P(x, y)$ is false. Do not forget to specify to which set x and y belong!

MAU22C00 - TUTORIAL 1 SOLUTIONS

1) Give an example of sentences P and Q such that the implication $P \to Q$ is true, but its converse $Q \to P$ is false. Give another example of sentences P and Q such that the implication $P \to Q$ is true and its converse $Q \to P$ is also true. Given an implication $P \to Q$, what can you deduce about the truth value of its converse?

Solution: Let P be: 'The set A is finite.' Let Q be: 'The set A has a finite subset B.' Clearly, $P \to Q$ is true as every finite set A has finite subsets. For example, we can set $B = A$ as every set is its own subset. $Q \to P$ is false, however. There are infinite sets that have finite subsets. An example is $A = \mathbb{N}$, the set of natural numbers, and $B = \{2, 4, 6\}$. The fact that a set has a finite subset does **not** imply the set itself is finite.

Now, let P be: "0=1." Let Q be: "Every real number is either even or odd." Both P and Q are false. As we know from the truth table of the implication, if both P and Q are false, both implications $P \to Q$ and $Q \to P$ are true.

Moral of the story: Given a true implication $P \to Q$, there is **NOTHING** that can be said about the truth value of the converse $Q \to P$.

2) Suppose we are told the following:
If turtles can sing then artichokes can fly. Artichokes can fly implies turtles can sing and dogs can't play chess. Dogs can play chess if and only if turtles can sing.
Deduce that turtles can't fly.

Proof.
We convert these statments into a logical format;
P = "turtles can sing".
Q = "artichokes can fly".
R = "dogs can't play chess".

We can assume the following hypotheses from the above paragraph;

(a) $P \to Q$

(b) $Q \to (P \wedge R)$

(c) $\neg R \leftrightarrow P$

We wish to prove $\neg P$. We do so as follows:

(1) $Q \rightarrow (\neg R \wedge R)$ - substitution of (c) into (b).

(2) $\neg(\neg R \wedge R) \rightarrow \neg Q$ - contrapositive of (1) (tautology #24 on the list of tautologies posted in Course Documents)

(3) $R \vee \neg R$ - law of the excluded middle (tautology #1 on the list of tautologies)

(4) $\neg(\neg R \wedge R)$ - De Morgan's law applied to (3) (tautology #18) and substitution of $\neg(\neg R)$ by R by the law of double negation (tautology #3)

(5) $\neg Q$ - modus ponens (2, 4) (tautology #10)

(6) $\neg Q \rightarrow \neg P$ - contrapositive of (a) (tautology #24)

(7) $\neg P$ - modus ponens (5,6) (tautology #10)

□

3) Prove that the order of quantifiers cannot be reversed without potentially modifying the truth value by providing a counterexample. The easiest counterexample can be given for two quantifiers. Find a sentence in predicate logic $P(x, y)$ such that $\forall x \, \exists y \, P(x, y)$ is true, but $\exists y \, \forall x \, P(x, y)$ is false. Do not forget to specify to which set x and y belong!

Solution: Let the domain of both x and y be $\mathbb{R}$, the set of real numbers. Let $P(x, y)$ be the statement $x + y = 0$. $\forall x \, \exists y \, P(x, y)$ is true because we can let $y = -x$. The statement $\exists y \, \forall x \, P(x, y)$ is false because there is no $y \in \mathbb{R}$ such that for every $x \in \mathbb{R}$, $x + y = 0$.

This phenomenon is true in general. Any existentially bound variable in a statement that is true can be expressed as a function of all universally bound variable to its left. In this case, in the statement $\forall x \, \exists y \, P(x, y)$, the variable x is universally bound (bound by the universal quantifier $\forall$), whereas the variable y is existentially bound (bound by the existential quantifier $\exists$). The statement is true because y can be expressed as a function of all universally bound variables to its left. Here we have only one universally bound variable to y's left, variable x, and the formula defining

y as a function of x is $y = -x$. For $\exists y \forall x \, P(x, y)$, variable y is existentially bound and has no universally bound quantifiers to its left, which means $\exists y \forall x \, P(x, y)$ would have to be true for y a constant, since y cannot be given as a formula involving any variables. Clearly, the statement $x + y = 0$ is not true for a constant over the real numbers $\mathbb{R}$, so $\exists y \forall x \, P(x, y)$ is false.

MAU22C00 - TUTORIAL 2

1) Prove $A \setminus (A \setminus B) \subseteq B$.

2) For each of the following statements, determine whether it is either true or false and give a brief justification for your answer:

(a) $3 \in \mathcal{P}(\mathbb{N})$

(b) $\{3\} \in \mathcal{P}(\mathbb{N})$

(c) $\{3\} \subseteq \mathcal{P}(\mathbb{N})$

(d)$\{\emptyset\} \in \mathcal{P}(\{\{\emptyset\}\})$

(e) $\mathcal{P}(\mathbb{Z} \cap (2,4)) = \{\emptyset, \{3\}\}$, where $(2,4)$ means the interval with endpoints 2 and 4 on the real line.

3) In the country of Tannu Tuva, a valid license plate consists of any digit except 0, followed by any two letters of the English alphabet, followed by any two digits.

(a) Let D be the set of all digits and L the set of all letters. With this notation, write the set of all possible license plates as a Cartesian product.

(b) How many possible license plates are there?

MAU22C00 - TUTORIAL 2 SOLUTIONS

1) Prove $A \setminus (A \setminus B) \subseteq B$.

Solution: This is done by examining where the elements lie in the set to the left of $\subseteq$ and proving they also lie in B. To this end, take $x \in A \setminus (A \setminus B)$. By the definition of $X \setminus Y = X \cap Y^c$, we have

$$x \in A \setminus (A \setminus B) \Rightarrow x \in A \cap (A \setminus B)^c \Rightarrow x \in A \text{ AND } x \in (A \setminus B)^c$$

Applying the definition of $\setminus$ again. we conclude $x \in A$ AND $x \in (A \cap B^c)^c$. Using De Morgan's laws for the later, we get $x \in A$ AND $x \in A^c \cup (B^c)^c$. Let's focus more on the later, with the knowledge that $x \in A$.

$$x \in A^c \cup (B^c)^c \Rightarrow x \in A^c \text{ OR } x \in (B^c)^c \Rightarrow x \in A^c \text{ OR } x \in B$$

Since x cannot be in both A and A^c at the same time, we conclude $x \in B$ (now ignoring A). What we have shown:

$$\forall x (x \in A \setminus (A \setminus B) \Rightarrow x \in B)$$

So $A \setminus (A \setminus B) \subseteq B$ as required. □

Remark. Veitch diagrams and/or Venn diagrams will **NOT** be accepted as a form of proof in set theory. Please bear in mind that only a solution of this kind is acceptable as a proof to an assertion in set theory.

2) For each of the following statements, determine whether it is either true or false and give a brief justification for your answer:

(a) $3 \in \mathcal{P}(\mathbb{N})$

(b) $\{3\} \in \mathcal{P}(\mathbb{N})$

(c) $\{3\} \subseteq \mathcal{P}(\mathbb{N})$

(d)$\{\emptyset\} \in \mathcal{P}(\{\{\emptyset\}\})$

(e) $\mathcal{P}(\mathbb{Z} \cap (2,4)) = \{\emptyset, \{3\}\}$, where $(2,4)$ means the interval with endpoints 2 and 4 on the real line.

Solution: (a) FALSE. The power set of $\mathbb{N}$ is a set whose elements are all the subsets of $\mathbb{N}$. We know $3 \in \mathbb{N}$, so 3 is an element of $\mathbb{N}$ but NOT a subset of $\mathbb{N}$, so $3 \in \mathcal{P}(\mathbb{N})$ is false.

(b) TRUE. As we showed in (a), $\mathcal{P}(\mathbb{N})$ consists of all subsets of $\mathbb{N}$. Since $3 \in \mathbb{N}$, the set consisting of the element 3 is a subset of $\mathbb{N}$, which written symbolically as $\{3\} \subseteq \mathbb{N}$, so $\{3\} \in \mathcal{P}(\mathbb{N})$ is true.

(c) FALSE. $\{3\}$ is an element of $\mathcal{P}(\mathbb{N})$ and NOT a subset of $\mathcal{P}(\mathbb{N})$, so $\{3\} \subseteq \mathcal{P}(\mathbb{N})$ is false. $\{\{3\}\} \subseteq \mathcal{P}(\mathbb{N})$ is true. In other words, the set consisting of $\{3\}$ is an element of $\mathcal{P}(\mathbb{N})$.

(d) FALSE. $\{\{\emptyset\}\}$ is the set consisting of one element $\{\emptyset\}$, which means $\mathcal{P}(\{\{\emptyset\}\}) = \{\emptyset, \{\{\emptyset\}\}\}$. $\{\emptyset\}$ is neither of the two elements of $\mathcal{P}(\{\{\emptyset\}\})$, so the statement is false.

(e) TRUE. $(2,4) = \{x \in \mathbb{R} \mid 2 < x < 4\}$, so $\mathbb{Z} \cap (2,4) = \{3\}$. $\mathcal{P}(\{3\}) = \{\emptyset, \{3\}\}$, so the statement is true.

Moral of the story: $\in$ means 'is an element of,' whereas $\subseteq$ means 'is a subset of.' You CANNOT use them interchangeably. You will be penalised on an exam or on the homework if you do. Please DO NOT make this mistake!

3) In the country of Tannu Tuva, a valid license plate consists of any digit except 0, followed by any two letters of the English alphabet, followed by any two digits.

(a) Let D be the set of all digits and L the set of all letters. With this notation, write the set of all possible license plates as a Cartesian product.

(b) How many possible license plates are there?

Solution: (a) The first character on the license plate belongs to the set $D \setminus \{0\}$ consisting of all digits but zero. The second character belongs to L, the third also to L, the fourth to D, and the fifth to D. The set of all possible license plates is the Cartesian product of all these sets in order, namely $(D \setminus \{0\}) \times L \times L \times D \times D$.

(b) The number of possible license plates is exactly the number of elements in the Cartesian product $(D \setminus \{0\}) \times L \times L \times D \times D$ from part (a). The number of elements of a **finite** Cartesian product is thus the product of the number of elements in each of the finite sets composing the product. We'll see in Hilary term what happens when we

look at Cartesian products of infinite sets. Since there are 10 digits, $\#(D) = 10$, which means $\#(D \setminus \{0\}) = 9$. There are 26 letters in the English alphabet, so $\#(L) = 26$. We conclude that

$$\#((D \setminus \{0\}) \times L \times L \times D \times D = 9 \times 26 \times 26 \times 10 \times 10 = 608,400.$$

MAU22C00 - TUTORIAL 3

1) (From the 2016-2017 Annual Exam) Let Q denote the relation on the set $\mathbb{Z}$ of integers, where integers x and y satisfy xQy if and only if

$$x - y = (x - y)(x + 2y).$$

Determine the following:

(i) Whether or not the relation Q is *reflexive*;
(ii) Whether or not the relation Q is *symmetric*;
(iii) Whether or not the relation Q is *transitive*;
(iv) Whether or not the relation Q is an *equivalence relation*;
(v) Whether or not the relation Q is *anti-symmetric*;
(vi) Whether or not the relation Q is a *partial order*.

Justify your answers.

2) In lecture we discussed an equivalence relation given by $f : A \to A$ for f any function on a non-empty set A with the relation R defined by $R = \{(x, y) \mid f(x) = f(y)\}$. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = \cos x$. What are the equivalence classes determined by the relation R on $\mathbb{R}$, namely for any $x \in \mathbb{R}$ what is $[x]_R$?

MAU22C00 - TUTORIAL 3 SOLUTIONS

1) (From the 2016-2017 Annual Exam) Let Q denote the relation on the set $\mathbb{Z}$ of integers, where integers x and y satisfy xQy if and only if

$$x - y = (x - y)(x + 2y).$$

Determine the following:

(i) Whether or not the relation Q is *reflexive*;
(ii) Whether or not the relation Q is *symmetric*;
(iii) Whether or not the relation Q is *transitive*;
(iv) Whether or not the relation Q is an *equivalence relation*;
(v) Whether or not the relation Q is *anti-symmetric*;
(vi) Whether or not the relation Q is a *partial order*.

Justify your answers.

Solution: $x, y \in \mathbb{Z}$ satisfy xQy iff $x - y = (x - y)(x + 2y)$, which is equivalent to $(x - y)(x + 2y - 1) = 0$, i.e., $x = y$ or $x + 2y - 1 = 0$.

(i) **Reflexivity:** The relation Q is reflexive because xQx holds for all $x \in \mathbb{Z}$ as $x - x = (x - x)(x + 2x) = 0$.

(ii) **Symmetry:** The relation Q is not symmetric because if $x \neq y$, then xQy holds if $x + 2y = 1$, thus for yQx we would need $y + 2x = 1$, which only holds at the same time with $x+2y = 1$ when $x = y = \dfrac{1}{3} \notin \mathbb{Z}$.

(iii) **Anti-symmetry:** The relation Q is anti-symmetric. Having xQy and yQx when $x \neq y$ would imply $x + 2y = 1$ and $y + 2x = 1$ hold simultaneously, which gives $x = y = \dfrac{1}{3} \notin \mathbb{Z}$. Therefore, xQy and yQx can both be true only if $x = y$.

(iv) **Transitivity:** The relation Q is not transitive. Assume xQy and yQz hold for $x, y, z \in \mathbb{Z}$. There are 4 cases to consider:

Case 1: $x = y$ and $y = z$, then $x = z$, so xQz as needed.

Case 2: $x = y$ and $y + 2z = 1$, then $x + 2z = 1$, so xQz as needed.

Case 3: $x + 2y = 1$ and $y = z$, then $x + 2z = 1$, so xQz as needed.

Case 4: $x + 2y = 1$ and $y + 2z = 1$, then $x + 2(1 - 2z) = 1$, so $x + 2 - 4z = 1$, i.e., $x - 4z = -1$. This last equation is satisfied for example for $x = 3$, $z = 1$. Take $y = -1$ in order to satisfy $x + 2y = 1$. We see that $x + 2z = 3 + 2 = 5 \neq 1$, so xQz fails. We have constructed a counterexample.

(v) **Equivalence relation:** The relation Q is not an equivalence relation because while reflexive, it fails to be symmetric and transitive.

(vi) **Partial order:** The relation Q is not a partial order because while reflexive and anti-symmetric, it fails to be transitive.

2) In lecture we discussed an equivalence relation given by $f : A \to A$ for f any function on a non-empty set A with the relation R defined by $R = \{(x, y) \mid f(x) = f(y)\}$. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = \cos x$. What are the equivalence classes determined by the relation R on $\mathbb{R}$, namely for any $x \in \mathbb{R}$ what is $[x]_R$?

Solution: By the definition of our relation R,

$$[x]_R = \{y \in \mathbb{R} \mid \cos x = \cos y\}.$$

We know two key facts about $f(x) = \cos x$. The cosine function is periodic with period 2π, so $f(x) = f(x + 2n\pi)$ for all $n \in \mathbb{Z}$. Also, the cosine function is even, which means $\cos(x) = \cos(-x)$ for all $x \in \mathbb{R}$. We put these two properties together in order to write down the equivalence class of x, $[x]_R$:

$$[x]_R = \{x + 2n\pi \mid n \in \mathbb{Z}\} \cup \{-x + 2p\pi \mid p \in \mathbb{Z}\}.$$

Note that if $x = 0$, then $x = -x$, so $[0]_R = \{2n\pi \mid n \in \mathbb{Z}\}$.

MAU22C00 - TUTORIAL 4 SOLUTIONS

1) Let A be a set, and let $\mathcal{A} = \{A_\alpha \mid \alpha \in I\}$, where I is an indexing set, be any partition of the set A. Define a relation R on A as follows: $x, y \in A$ satisfy xRy iff $x, y \in A_\alpha$ for some $\alpha \in I$. In other words, xRy iff x and y belong to the same set of the partition. Prove that R is an equivalence relation and that the partition R defines on A is precisely the given partition $\mathcal{A}$.

(Hint: Recall we discussed in lecture the one-to-one correspondence between partitions and equivalence relations, and this is the proof direction I sketched in lecture without providing the details.)

Solution: First, let us prove R is an equivalence relation:

Reflexivity: For any $x \in A$, since $\mathcal{A} = \{A_\alpha \mid \alpha \in I\}$ is a partition of A, there exists $\alpha \in I$ such that $x \in A_\alpha$. The element x is in the same set A_α as itself, so xRx.

Symmetry: If xRy, then by definition $x, y \in A_\alpha$ for some $\alpha \in I$, i.e. x and y belong to the same set of the partition. Therefore, yRx holds as well.

Transitivity: If xRy, then by definition $x, y \in A_\alpha$ for some $\alpha \in I$. If yRz, then z belongs to the same set of the partition as y, namely $z \in A_\alpha$ for the same α. Thus, $x, y, z \in A_\alpha$, which means xRz holds as well.

The partition determined by R is exactly $\mathcal{A}$: If $x \in A_\alpha$, then the equivalence class of x given by $[x]_R = A_\alpha$ by the very definition of R. Since $\mathcal{A}$ is a partition of A and it consists of the set of equivalence classes determined by the relation R, we conclude that R determines the partition $\mathcal{A}$ as needed.

2) (From the 2016-2017 Annual Exam) Let $f : [-2, 2] \to [-15, 1]$ be the function defined by $f(x) = x^2 + 3x - 10$ for all $x \in [-2, 2]$. Determine whether or not this function is injective and whether or not it is surjective. Justify your answers.

Injectivity: $f(x) = x^2 + 3x - 10 = (x - 2)(x - 5)$ This function is not injective on the interval $[-2, 2]$. Acceptable justifications: drawing the graph, providing two values $x_1, x_2 \in [-2, 2]$, $x_1 \neq x_2$ such that

$f(x_1) = f(x_2)$, applying Rolle's theorem (noticing that $f'(x) = 2x + 3$ so $f'\left(-\frac{3}{2}\right) = 0$, and $\frac{3}{2} \in [-2, 2]$), etc.

Surjectivity: $f(x) = x^2 + 3x - 10$ is not surjective on the interval $[-2, 2]$. Acceptable justifications: drawing the graph, providing a value in $[-15, 1]$ that $f(x)$ does not assume, showing the minimum value occurs at $\frac{3}{2}$, where $f\left(\frac{3}{2}\right) = -12.25 > -15$, etc.

MAU22C00 - TUTORIAL 5

1) Use mathematical induction to prove the geometric series formula, which states that for any $a, r \in \mathbb{R}$ with $r \neq 1$ and any $n \in \mathbb{N}^*$,

$$a + ar + ar^2 + \cdots + ar^{n-1} = a\frac{(1-r^n)}{(1-r)}.$$

2) Where is the fallacy in the following argument by induction?

Statement: If p is an even number and $p \geq 2$, then p is a power of 2.

"Proof:" We give a proof using strong induction on the even number p. Denote by $P(n)$ the statement "if n is an even number and $n \geq 2$, then $n = 2^j$, where $j \in \mathbb{N}$."

Base case: Show $P(2)$. $2 = 2^1$, so 2 is indeed a power of 2.

Inductive step: Assume $p > 2$ and that $P(n)$ is true for every n such that $2 \leq n < p$ (the strong induction hypothesis). We have to show that $P(p)$ also holds. We consider two cases:

Case 1: p is odd, then there is nothing to show.

Case 2: p is even. Since $p \geq 4$ and p is an even number, we can write $p = 2n$ with $2 \leq n < p$. By the inductive hypothesis, $P(n)$ holds, so we conclude that $n = 2^j$ for some $j \in \mathbb{N}$. Since $p = 2n = 2 \times 2^j = 2^{j+1}$, we conclude that $P(p)$ also holds.

3) In the 1730's, the "Grande Loge" of Freemasons in Paris was a highly secretive society following some rather bizarre rules. Each of the freemasons in the lodge had shaved one other member. No freemason in the lodge had ever shaved himself. Furthermore, no freemason was ever shaved by more than one member of the lodge. There was one freemason who had never been shaved by any other member of the lodge. The number and identity of the freemasons in the lodge was kept secret. One rumour circulating in Paris at that time was that there were fewer than a hundred freemasons in the "Grande Loge." Another rumour put the number at over a hundred. Which one of the two rumours is true? Justify your answer.

MAU22C00 - TUTORIAL 5 SOLUTIONS

1) Use mathematical induction to prove the geometric series formula, which states that for any $a, r \in \mathbb{R}$ with $r \neq 1$ and any $n \in \mathbb{N}^*$,

$$a + ar + ar^2 + \cdots + ar^{n-1} = a\frac{(1-r^n)}{(1-r)}.$$

Solution: Fix $a, r \in \mathbb{R}$, $r \neq 1$.
Base case: $n = 1$**.**
Then

$$a\frac{(1-r^1)}{(1-r)} = a(1) = a$$

as required.
Induction step: Assume true for $n = k$**.**
Prove true for $n = k + 1$**.**

$$a + ar + ar^2 + \cdots + ar^{k-1} + ar^k = a\frac{(1-r^k)}{(1-r)} + ar^k$$
$$= a\left(\frac{(1-r^k)}{(1-r)} + \frac{(1-r)r^k}{(1-r)}\right) = a\left(\frac{(1-r^k) + (r^k - r^{k+1})}{(1-r)}\right)$$
$$= a\frac{(1-r^{k+1})}{(1-r)}$$

as required.

2) Where is the fallacy in the following argument by induction?

Statement: If p is an even number and $p \geq 2$, then p is a power of 2.

"Proof:" We give a proof using strong induction on the even number p. Denote by $P(n)$ the statement "if n is an even number and $n \geq 2$, then $n = 2^j$, where $j \in \mathbb{N}$."

Base case: Show $P(2)$. $2 = 2^1$, so 2 is indeed a power of 2.

Inductive step: Assume $p > 2$ and that $P(n)$ is true for every n such that $2 \leq n < p$ (the strong induction hypothesis). We have to show that $P(p)$ also holds. We consider two cases:

Case 1: p is odd, then there is nothing to show.

Case 2: p is even. Since $p \geq 4$ and p is an even number, we can write $p = 2n$ with $2 \leq n < p$. By the inductive hypothesis, $P(n)$ holds, so

we conclude that $n = 2^j$ for some $j \in \mathbb{N}$. Since $p = 2n = 2 \times 2^j = 2^{j+1}$, we conclude that $P(p)$ also holds.

Solution: The argument fails at the inductive step as it is possible that $p = 2n$ and n is not even. For example, if $p = 6 = 2 \times 3$, the argument in the inductive step fails.

3) In the 1730's, the "Grande Loge" of Freemasons in Paris was a highly secretive society following some rather bizarre rules. Each of the freemasons in the lodge had shaved one other member. No freemason in the lodge had ever shaved himself. Furthermore, no freemason was ever shaved by more than one member of the lodge. There was one freemason who had never been shaved by any other member of the lodge. The number and identity of the freemasons in the lodge was kept secret. One rumour circulating in Paris at that time was that there were fewer than a hundred freemasons in the "Grande Loge." Another rumour put the number at over a hundred. Which one of the two rumours is true? Justify your answer.

Solution: This problem is an exercise in concept recognition. You're looking at Hilbert's hotel problem in disguise. Let x_0 be the freemason who has never been shaved by any member of the lodge. Let x_1 be the freemason x_0 shaves. Let x_2 be the freemason x_1 shaves and so on. We've constructed the map $x_{i-1} \to x_i$ for $i \geq 1$. If the number of freemasons were finite, we would have the scenario of musical chairs, which is ruled out by the problem. Therefore, the number of freemasons is infinite hence bigger than 100.

MAU22C00 - TUTORIAL 6

1) Let $A = \{3^p \mid p \in \mathbb{N}\}$ with the operation of multiplication.
   (a) Is $(A, \cdot)$ a semigroup? Justify your answer.
   (b) Is $(A, \cdot)$ a monoid? Justify your answer.
   (c) Does $(A, \cdot)$ have invertible elements? If so, which of its elements are invertible? Justify your answer.

2) (Slightly modified question from the annual exam 2017-2018) Let $A = \{(x, y) \in \mathbb{R}^2 \mid x + 2y = 0\}$ with the operation of addition given by

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

   (a) Is $(A, +)$ a semigroup? Justify your answer.
   (b) Is $(A, +)$ a monoid? Justify your answer.
   (c) Does $(A, +)$ have invertible elements? If so, which of its elements are invertible? Justify your answer.
   (d) What geometric object is the set A in $\mathbb{R}^2$?

MAU22C00 - TUTORIAL 6 SOLUTIONS

1) Let $A = \{3^p \mid p \in \mathbb{N}\}$ with the operation of multiplication.

(a) Is $(A, \cdot)$ a semigroup? Justify your answer.
(b) Is $(A, \cdot)$ a monoid? Justify your answer.
(c) Does $(A, \cdot)$ have invertible elements? If so, which of its elements are invertible? Justify your answer.

Solution: (a) Yes, $(A, \cdot)$ is a semi-group. $A \subset \mathbb{Q}^*$, and $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ is a monoid under the operation of multiplication. We proved in lecture that if $a \in M$ for M a monoid with operation $*$ and $m, n \in \mathbb{N}$, then $a^m * a^n = a^{m+n}$. Here $a = 3$ and since addition is a binary operation on $\mathbb{N}$ as we showed in class, multiplication is a binary operation on A. The associativity of multiplication on A follows from the associativity of addition on $\mathbb{N}$ and the theorem that if $a \in M$ for M a monoid with operation $*$ and $m, n \in \mathbb{N}$, then $a^m * a^n = a^{m+n}$.

(b) Yes, $(A, \cdot)$ is a monoid. $3^0 = 1$ is the identity element on A because any $b \in A$ is of the form 3^p, so $b \cdot 1 = a^p \cdot a^0 = a^{p+0} = a^{0+p} = 1 \cdot b = a^p = b$.

(c) By the theorem on powers proved in lecture that was quoted above, $3^m \cdot 3^n = 3^{m+n}$. The condition for invertibility $3^{m+n} = 3^0$ for $m \geq 0$ and $n \geq 0$ is only satisfied if $m = n = 0$. Therefore, $3^0 = 1$ is the only invertible element of A.

2) (Slightly modified question from the annual exam 2017-2018) Let $A = \{(x, y) \in \mathbb{R}^2 \mid x + 2y = 0\}$ with the operation of addition given by

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

(a) Is $(A, +)$ a semigroup? Justify your answer.
(b) Is $(A, +)$ a monoid? Justify your answer.
(c) Does $(A, +)$ have invertible elements? If so, which of its elements are invertible? Justify your answer.
(d) What geometric object is the set A in $\mathbb{R}^2$?

Solution: (a) Yes, $(A, +)$ is a semi-group. If $x_1 = -2y_1$ and $x_2 = -2y_2$, then $x_1 + x_2 = -2y_1 - 2y_2 = -2(y_1 + y_2)$, so $+$ is a binary operation on A. We proved in lecture that addition is an associative binary operation on $\mathbb{R}$, so $+$ is associative on A as associativity will function component by component in the vector (x, y).

(b) Yes, $(A, +)$ is a monoid. $(0, 0)$ is the identity element on A because for any $(x, y) \in A$,

$$(x, y) + (0, 0) = (x + 0, y + 0) = (0 + x, 0 + y) = (0, 0) + (x, y) = (x, y).$$

(c) For any $(x, y) \in A$, $(-x, -y)$ is its inverse because $(x, y)+(-x, -y) = (-x, -y) + (x, y) = (0, 0)$. Therefore, all elements of A are invertible.

(d) A is the line passing through the origin $(0, 0)$ and the point $(2, -1)$ as $2 + 2(-1) = 0$.

MAU22C00: TUTORIAL 7 PROBLEM SHEET
HOMOMORPHISMS AND ISOMORPHISMS

1) Let A be a finite set, and let A^* be the set of all words over the alphabet A. Consider $(A^*, \circ, \epsilon)$ with the operation of concatenation and empty word ϵ as the identity element. Let $(\mathbb{N}, +, 0)$ be the set of natural numbers with the operation of addition and 0 as the identity element. Let $f : A^* \to \mathbb{N}$ be the function that assigns to each word $w \in A^*$ its length, $f(w) = |w| \in \mathbb{N}$.

(a) What type of object is $(A^*, \circ, \epsilon)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(\mathbb{N}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

2) Let $(\mathbb{Z}, +, 0)$ be the set of integers with the operation of addition and 0 as the identity element. Let E be the set of even integers, $E = \{2p \mid p \in \mathbb{Z}\}$. Consider $(E, +, 0)$ the set of even integers with the operation of addition and 0 as the identity element. Let $f : \mathbb{Z} \to E$ be the function $f(n) = 2n$.

(a) What type of object is $(\mathbb{Z}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(E+, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

MAU22C00: TUTORIAL 7 SOLUTIONS

1) Let A be a finite set, and let A^* be the set of all words over the alphabet A. Consider $(A^*, \circ, \epsilon)$ with the operation of concatenation and empty word ϵ as the identity element. Let $(\mathbb{N}, +, 0)$ be the set of natural numbers with the operation of addition and 0 as the identity element. Let $f : A^* \to \mathbb{N}$ be the function that assigns to each word $w \in A^*$ its length, $f(w) = |w| \in \mathbb{N}$.

(a) What type of object is $(A^*, \circ, \epsilon)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(\mathbb{N}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) $\circ$ is an associative binary operation as we proved in lecture, so $(A^*, \circ, \epsilon)$ is definitely a semigroup. As we showed in lecture, ϵ is the identity element for $\circ$ on A^*, which means $(A^*, \circ, \epsilon)$ is a monoid. We discussed in lecture during the abstract algebra unit that ϵ is the only invertible element in A^*, so $(A^*, \circ, \epsilon)$ cannot be a group.

(b) Addition is an associative binary operation as we showed in lecture, so $(\mathbb{N}, +, 0)$ is clearly a semigroup. 0 is the identity element for addition on $\mathbb{N}$ which means $(\mathbb{N}, +, 0)$ is a monoid. Note that 0 is the only invertible element in $\mathbb{N}$ so $(\mathbb{N}, +, 0)$ cannot be a group.

(c) To show that f is a homomorphism, we need to show that for any two words $w_1, w_2 \in A^*$, $f(w_1 \circ w_2) = |w_1| + |w_2|$, but we have already showed in lecture that this property holds. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. Now we need to decide whether it is bijective. The function f is clearly surjective because for any length $n \in \mathbb{N}$, we can construct a word in $w \in A^*$, whose length $|w| = n$. Is f injective? Well, the answer depends whether A has one element or several. If $A = \{a\}$ has only one element, there is one and only one word $a \cdots a$ of any given length n, so f is injective. However, if A has more than one element, then there exist letters $a, b \in A$ such that $a \neq b$. Then the words ab and ba that are distinct have the same length 2, which means f cannot be injective, so it is not an isomorphism.

2) Let $(\mathbb{Z}, +, 0)$ be the set of integers with the operation of addition and 0 as the identity element. Let E be the set of even integers, $E = \{2p \mid p \in \mathbb{Z}\}$. Consider $(E, +, 0)$ the set of even integers with the operation of addition and 0 as the identity element. Let $f : \mathbb{Z} \to E$ be the function $f(n) = 2n$.

(a) What type of object is $(\mathbb{Z}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(E+, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) Addition on $\mathbb{R}$ hence on $\mathbb{Z}$ is an associative binary operation as we discussed in lecture. Therefore, $(\mathbb{Z}, +, 0)$ is a semigroup. 0 is the identity element for addition on $\mathbb{Z}$ as for any $n \in \mathbb{Z}$, $n + 0 = 0 + n = n$, so $(\mathbb{Z}, +, 0)$ is a monoid. Given any $n \in \mathbb{Z}$, $-n$ is its inverse as $n + (-n) = n - n = 0$, so every element of $(\mathbb{Z}, +, 0)$ is invertible. Therefore, $(\mathbb{Z}, +, 0)$ is a group.

(b) $E \subset \mathbb{Z}$. Since addition is associative on $\mathbb{Z}$, it is also associative on E. We do, however, have to prove it is a binary operation, i.e. closed. Consider $m, n \in E$. Thus, there exist $p, s \in \mathbb{Z}$ such that $m = 2p$ and $n = 2s$ by the definition of E. Then $m + n = 2p + 2s = 2(p + s)$. Since addition is a binary operation on $\mathbb{Z}$ hence closed, it follows

$$p, s \in \mathbb{Z} \implies p + s \in \mathbb{Z}.$$

Thus, $m + n \in E$, and addition is indeed closed on E. We conclude $(E+, 0)$ is a semigroup. Since $E \subset \mathbb{Z}$, the fact that 0 is the identity element for addition on $\mathbb{Z}$ carries over to E, so E has 0 as its identity element. Therefore, $(E+, 0)$ is a monoid. Now let $n \in E$. We know from part (a) that $-n \in \mathbb{Z}$ is the inverse of n under addition. We just have to prove $-n \in E$. Since $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p$. Therefore, $-n = -2p = 2(-p)$, so $-n \in E$ as needed, which means every element in E is invertible. Therefore, $(E+, 0)$ is a group.

(c) To show that f is a homomorphism, we need to show that for any two integers $p, s \in \mathbb{Z}$, $f(p + s) = f(p) + f(s)$. We apply the definition of f as follows: $f(p) + f(s) = 2p + 2s = 2(p + s) = f(p + s)$. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. We need to figure out whether it is bijective. The function f is clearly surjective by the definition of E because for every $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p = f(p)$. To show

injectivity, assume there exist $p, s \in \mathbb{Z}$ such that $f(p) = f(s)$. Then by the definition of f, $2p = 2s \iff p = s$. Therefore, f is indeed injective. We have shown f is bijective hence an isomorphism from $(\mathbb{Z}, +, 0)$ to $(E, +, 0)$.

MAU22C00: TUTORIAL 8 PROBLEMS
FORMAL LANGUAGES AND GRAMMARS

1) Let the formal language L over the alphabet $\{a, b, c\}$ be generated by the context-free grammar whose only non-terminal is $\langle S\rangle$, whose start symbol is $\langle S\rangle$, and whose production rules are the following:

(1) $\langle S\rangle \to b$
(2) $\langle S\rangle \to c$
(3) $\langle S\rangle \to a\langle S\rangle$

(a) Describe L. In other words, describe the structure of the strings generated by this grammar.
(b) Which words does $aa\langle S\rangle$ directly yield?
(c) Which words does $aa\langle S\rangle$ yield?

2) Consider the binary alphabet $\{0, 1\}$, start symbol $\langle S\rangle$, set of non-terminals consisting of $\{\langle S\rangle, \langle A\rangle, \langle B\rangle, \langle C\rangle, \langle D\rangle, \langle E\rangle\}$, and production rules given by

(1) $\langle S\rangle \to \langle A\rangle\langle B\rangle\langle C\rangle$
(2) $\langle A\rangle\langle B\rangle \to 0\langle A\rangle\langle D\rangle$
(3) $\langle A\rangle\langle B\rangle \to 1\langle A\rangle\langle E\rangle$
(4) $\langle D\rangle\langle C\rangle \to \langle B\rangle 0\langle C\rangle$
(5) $\langle E\rangle\langle C\rangle \to \langle B\rangle 1\langle C\rangle$
(6) $\langle D\rangle 0 \to 0\langle D\rangle$
(7) $\langle D\rangle 1 \to 1\langle D\rangle$
(8) $\langle E\rangle 0 \to 0\langle E\rangle$
(9) $\langle E\rangle 1 \to 1\langle E\rangle$
(10) $0\langle B\rangle \to \langle B\rangle 0$
(11) $1\langle B\rangle \to \langle B\rangle 1$
(12) $\langle A\rangle\langle B\rangle \to \epsilon$
(13) $\langle C\rangle \to \epsilon$

(a) What type of grammar is this (context-free or phrase structure)? Justify your answer.
(b) What language does this grammar generate? (Hint: Rules (12) and (13) show you that the word before the last non-terminals are swapped out can contain only non-terminals $\langle A\rangle$,$\langle B\rangle$,$\langle C\rangle$. Figure out how the other rules combine to give you words consisting of the terminals and $\langle A\rangle$,$\langle B\rangle$,$\langle C\rangle$.)

MAU22C00: TUTORIAL 8 SOLUTIONS
FORMAL LANGUAGES AND GRAMMARS

1) Let the formal language L over the alphabet $\{a, b, c\}$ be generated by the context-free grammar whose only non-terminal is $\langle S\rangle$, whose start symbol is $\langle S\rangle$, and whose production rules are the following:

(1) $\langle S\rangle \to b$
(2) $\langle S\rangle \to c$
(3) $\langle S\rangle \to a\langle S\rangle$

(a) Describe L. In other words, describe the structure of the strings generated by this grammar.
(b) Which words does $aa\langle S\rangle$ directly yield?
(c) Which words does $aa\langle S\rangle$ yield?

Solution: (a) This context-free grammar produces strings of the type $a^m b$ or $a^m c$ for $m \geq 0$, so

$$L = \{a^m b \mid m \in \mathbb{N}, m \geq 0\} \cup \{a^m c \mid m \in \mathbb{N}, m \geq 0\}.$$

(b) We are being asked which words we can obtain from $aa\langle S\rangle$ via the application of one production rule. The context-free grammar has three production rules, and the left-hand side of each one of these consists of the non-terminal $\langle S\rangle$, which appears exactly once in the word $aa\langle S\rangle$ that we are given. Therefore, we expect $aa\langle S\rangle$ to directly yield three different words. Indeed, via rule (1) we obtain aab, via rule (2) we obtain aac, and via rule (3) we obtain $aaa\langle S\rangle$.

(c) In this question part, we are being asked which words we can obtain from $aa\langle S\rangle$ via the application of finitely many production rules. We saw that the application of one production rule gave us a set of three words $\{aab, aac, aaa\langle S\rangle\}$. The first two consist of terminals, so only in the last one we can apply another production rule. In fact, in $aaa\langle S\rangle$ we can apply each of our three production rules to get $\{aaab, aaac, aaaa\langle S\rangle\}$. Thus, after two steps, we have obtained the set of words $\{aab, aac, aaab, aaac, aaaa\langle S\rangle\}$. By the same analysis, after three steps we will have obtained

$$\{aab, aac, aaab, aaac, aaaab, aaaac, aaaaa\langle S\rangle\},$$

and so on. After n steps, we will have the set

$$\{a^p b \mid 2 \leq p \leq n+1\} \cup \{a^p c \mid 2 \leq p \leq n+1\} \cup \{a^{n+2}\langle S\rangle\}.$$

Since we are allowed to have any finite number of steps, the set of words that $aa\langle S\rangle$ yields is given by

$$\bigcup_{n\geq 1}\{a^p b \mid 2\leq p\leq n+1\}\cup\{a^p c \mid 2\leq p\leq n+1\}\cup\{a^{n+2}\langle S\rangle\},$$

which equals

$$\{a^p b \mid p\geq 2\}\cup\{a^p c \mid p\geq 2\}\cup\{a^p\langle S\rangle \mid p\geq 3\}.$$

2) Consider the binary alphabet $\{0,1\}$, start symbol $\langle S\rangle$, set of non-terminals consisting of $\{\langle S\rangle,\langle A\rangle,\langle B\rangle,\langle C\rangle,\langle D\rangle,\langle E\rangle\}$, and production rules given by

(1) $\langle S\rangle\to\langle A\rangle\langle B\rangle\langle C\rangle$
(2) $\langle A\rangle\langle B\rangle\to 0\langle A\rangle\langle D\rangle$
(3) $\langle A\rangle\langle B\rangle\to 1\langle A\rangle\langle E\rangle$
(4) $\langle D\rangle\langle C\rangle\to\langle B\rangle 0\langle C\rangle$
(5) $\langle E\rangle\langle C\rangle\to\langle B\rangle 1\langle C\rangle$
(6) $\langle D\rangle 0\to 0\langle D\rangle$
(7) $\langle D\rangle 1\to 1\langle D\rangle$
(8) $\langle E\rangle 0\to 0\langle E\rangle$
(9) $\langle E\rangle 1\to 1\langle E\rangle$
(10) $0\langle B\rangle\to\langle B\rangle 0$
(11) $1\langle B\rangle\to\langle B\rangle 1$
(12) $\langle A\rangle\langle B\rangle\to\epsilon$
(13) $\langle C\rangle\to\epsilon$

(a) What type of grammar is this (context-free or phrase structure)? Justify your answer.
(b) What language does this grammar generate? (Hint: Rules (12) and (13) show you that the word before the last non-terminals are swapped out can contain only non-terminals $\langle A\rangle$,$\langle B\rangle$,$\langle C\rangle$. Figure out how the other rules combine to give you words consisting of the terminals and $\langle A\rangle$,$\langle B\rangle$,$\langle C\rangle$.)

Solution: (a) Production rule (2) has two non-terminals on the left-hand side, so this grammar is clearly a phrase structure grammar as context-free grammars have production rules that allow only one non-terminal to be swapped for something else.

(b) Rules (1), (2), and (4) yield $0\langle A\rangle\langle B\rangle 0\langle C\rangle$, whereas rules (1), (3), and (5) yield $1\langle A\rangle\langle B\rangle 1\langle C\rangle$. We can get to $01\langle A\rangle\langle B\rangle 01\langle C\rangle$ from $0\langle A\rangle\langle B\rangle 0\langle C\rangle$ by applying rules (3), (8), (5), and (10). Similarly, we can get $w\langle A\rangle\langle B\rangle w\langle C\rangle$

for any word $w \in \{0,1\}^*$. Rules (6) to (11) are there to rearrange non-terminals so that rules (2) to (5) can be applied. Altogether, we generate the language $L = \left\{ww \;\middle|\; w \in \{0,1\}^*\right\}$. Note that the language L CANNOT be generated by a context-free grammar as a context-free grammar could NOT keep track of the duplicate w by replacing only one non-terminal at a time. We have thus constructed an example of a language that is generated by a phrase structure grammar and cannot be generated by a context-free grammar thus showing that the former category is more general than the latter.

MAU22C00: TUTORIAL 9 PROBLEMS
FORMAL LANGUAGES AND GRAMMARS

1) Let L be the language over the alphabet $A = \{0, 1\}$ consisting of all words where the string 00 occurs as a substring.

(a) Prove from the definition of a regular language that the language L is regular.

(b) Draw a finite state acceptor that accepts the language L. Carefully label all the states including the starting state and the finishing states as well as all the transitions. Make sure you justify it accepts all strings in the language L and no others.

(c) Write down the transition mapping of the finite state acceptor you drew in the previous part of the problem.

(d) Let $\equiv_L$ be the equivalence relation defined in Lecture 23 before the statement and proof of the Myhill-Nerode theorem. Determine the equivalence classes into which this equivalence relation partitions L.

MAU22C00: TUTORIAL 9 SOLUTIONS
FORMAL LANGUAGES AND GRAMMARS

1) Let L be the language over the alphabet $A = \{0, 1\}$ consisting of all words where the string 00 occurs as a substring.

(a) Prove from the definition of a regular language that the language L is regular.

(b) Draw a finite state acceptor that accepts the language L. Carefully label all the states including the starting state and the finishing states as well as all the transitions. Make sure you justify it accepts all strings in the language L and no others.

(c) Write down the transition mapping of the finite state acceptor you drew in the previous part of the problem.

(d) Let $\equiv_L$ be the equivalence relation defined in Lecture 23 before the statement and proof of the Myhill-Nerode theorem. Determine the equivalence classes into which this equivalence relation partitions L.

Solution: (a) Let the alphabet $A = \{0, 1\}$. Recall that the definition of a regular language allows for finite subsets of A^*, the Kleene star, concatenations, and unions. Note that

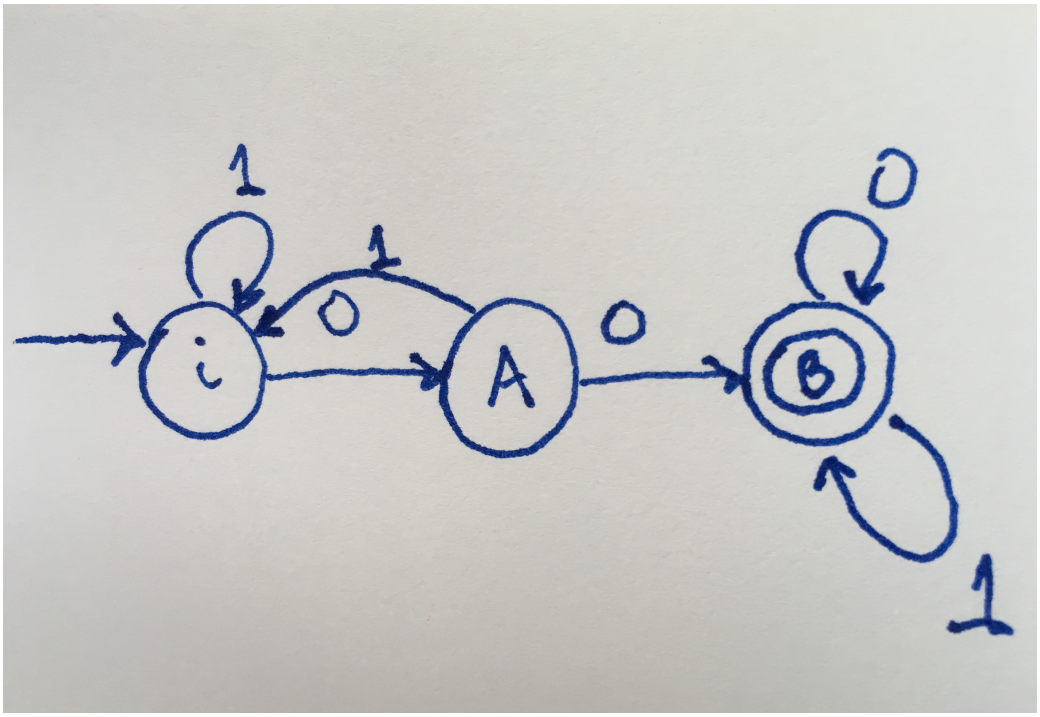
$$L = \{w \in A^* \mid w = u \circ 00 \circ v \quad u, v \in A^*\}.$$

Therefore, we can let $L_1 = \{00\}$ be the language consisting of just the string 00 of interest. L_1 is a finite set, so it is allowed in the definition of a regular language. Let $L_2 = \{0, 1\}$. L_2 is finite, hence likewise allowed. Let $L_3 = L_2^*$, the Kleene star applied to L_2. The language $L_3 = A^*$, i.e. it is the set of all words that can be formed over the alphabet $A = \{0, 1\}$. Set $L_4 = L_3 \circ L_1$, and then $L_5 = L_4 \circ L_3$. Note that the words in L_5 have exactly the structure of the words in L, and in fact, $L = L_5$. Note also that the solution here is by no means unique. No two of you will necessarily have arrived at the same exact expression, order or labelling of the intermediate languages L_i that come into the definition of a regular language as applied to L.

(b) See diagram of finite state acceptor on the next page.

We can use three states $\{i, A, B\}$, where i is the initial state. Since we must ensure the word contains the string 00, when 1 is the input, we stay in the initial state i. For input 0, we move to a new state A. A is not an accepting state as we have so far only half of the string 00, the

first zero. If we get input 1, we have to restart the process of capturing the string 00, so we get back to the initial state i. If we get input 0, then we will have received the second zero we want, so we'll move to a new state B, which is an accepting state. Once we have the substring 00, we don't care what follows, so the transitions for both 0 and 1 out of state B are back into B itself.



(c)

$$\begin{aligned} t(i,0) &= A & t(i,1) &= i \\ t(A,0) &= B & t(A,1) &= i \\ t(B,0) &= B & t(B,1) &= B \end{aligned}$$

(d) Recall from Lecture 23 that the equivalence relation $\equiv_L$ is defined as $x \equiv_L y$ if $\forall w \in A^*, xw \in L \Leftrightarrow yw \in L$, where $x, y \in L$. As we saw in lecture, if $x \equiv_L y$, then x and y place our finite state acceptor into the same state s. We also know that a word is in the language L if it places the finite state acceptor into an accepting state. We have only one accepting state, which is B. Therefore, we have only one equivalence class, which is all of L since every word $x \in L$ will place the finite state acceptor into state B.

If we were to extend the definition of our equivalence relation to $x \equiv_L y$ if $\forall w \in A^*, xw \in L \Leftrightarrow yw \in L$, where $x, y \in A^*$, namely if we were to look at the equivalence classes that $\equiv_L$ determines on all of A^*, then the question would be a lot more interesting as then we would determine which words in A^* place our finite state acceptor into each of the states i, A, and B. For B we already have the answer. The equivalence class is exactly our language L. The words in A^* that place the finite state acceptor into state A are all words that do not contain the string 00 and end in 0. Finally, the words in A^* that place the finite state acceptor into state i are all words that do not contain the string 00 and end in 1.

MAU22C00: TUTORIAL 10 PROBLEMS
FORMAL LANGUAGES AND GRAMMARS

1) Let L be the language over the alphabet $A = \{0, 1\}$ consisting of all words where the string 00 occurs as a substring.

(a) Devise a regular grammar in normal form that generates the language L. Be sure to specify the start symbol, the non-terminals, and all the production rules.

(b) Write down a regular expression that gives the language L and justify your answer.

2) Let M be the language

$$\{0101,\ 001001,\ 00010001,\ 0000100001,\ \dots\}$$

whose words consist of some positive number n of occurrences of the digit 0, followed by the digit 1, followed by n further occurrences of the digit 0, and followed by the digit 1. (In particular, the number of occurrences of 0 preceding the first 1 is equal to the number of occurrences of 0 preceding the second 1.)

(a) Use the Pumping Lemma to show this language is not regular.

(b) Write down the production rules of a context-free grammar that generates exactly M. Justify your answer.

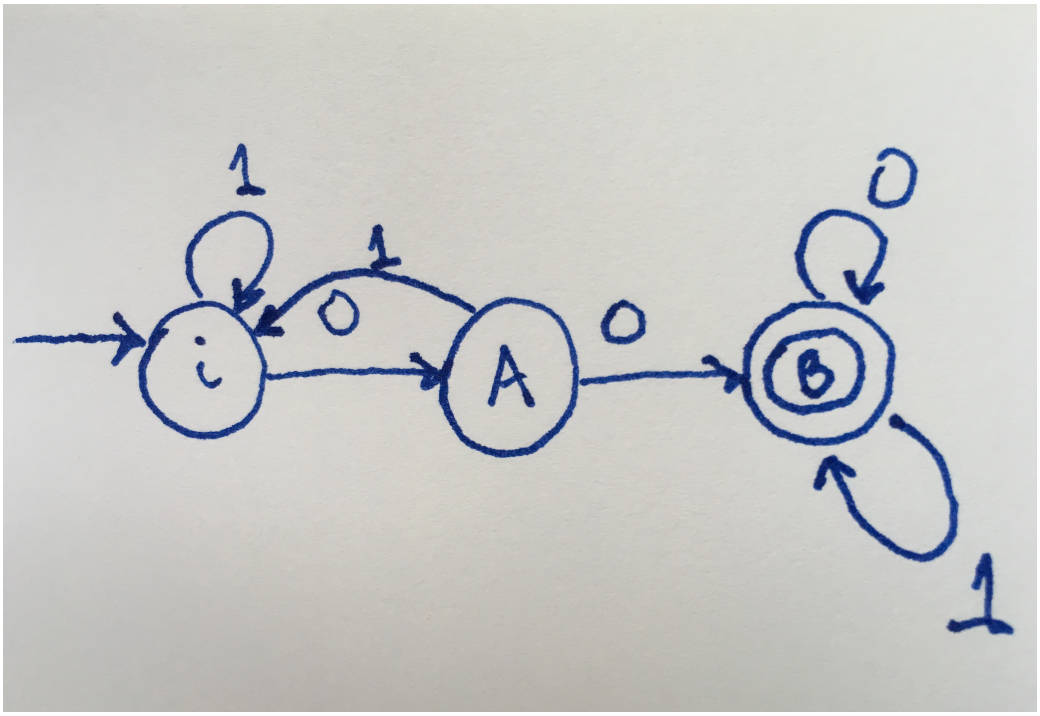
MAU22C00: TUTORIAL 10 SOLUTIONS
FORMAL LANGUAGES AND GRAMMARS

1) Let L be the language over the alphabet $A = \{0, 1\}$ consisting of all words where the string 00 occurs as a substring.

(a) Devise a regular grammar in normal form that generates the language L. Be sure to specify the start symbol, the non-terminals, and all the production rules.

(b) Write down a regular expression that gives the language L and justify your answer.

Solution: (a) We shall use the algorithm discussed in lecture in order to generate the regular grammar in normal form corresponding to the finite state acceptor constructed in last week's tutorial. Here is the finite state acceptor again:



The finite state acceptor has three states $\{i, A, B\}$, where i is the initial state. Correspondingly, we use three non-terminals in our regular grammar: the start symbol $\langle S \rangle$ corresponding to the initial state i, $\langle A \rangle$

corresponding to state A, and $\langle B\rangle$ corresponding to state B. We first write the production rules corresponding to the transitions out of the initial state i :

(1) $\langle S\rangle \to 1\langle S\rangle$.
(2) $\langle S\rangle \to 0\langle A\rangle$.

Next, we write the production rules corresponding to the transitions out of state A :

(3) $\langle A\rangle \to 1\langle S\rangle$.
(4) $\langle A\rangle \to 0\langle B\rangle$.

Finally, we write the production rules corresponding to the transitions out of state B :

(5) $\langle B\rangle \to 1\langle B\rangle$.
(6) $\langle B\rangle \to 0\langle B\rangle$.

Rules (1)-(6) are of type (i). For each accepting state, we will write down a rule of type (iii). Since there is only one accepting state, B, we have only one such rule:

(7) $\langle B\rangle \to \epsilon$.

(b) Recall from last week's tutorial that

$$L = \{w \in A^* \mid w = u \circ 00 \circ v \quad u, v \in A^*\}.$$

Therefore, $L = A^* \circ 00 \circ A^*$, and we have obtained the regular expression giving us the language L. Compare this solution to last week's tutorial when we proved this language was regular by applying the definition of a regular language.

2) Let M be the language

$$\{0101,\ 001001,\ 00010001,\ 0000100001,\ \dots\}$$

whose words consist of some positive number n of occurrences of the digit 0, followed by the digit 1, followed by n further occurrences of the digit 0, and followed by the digit 1. (In particular, the number of occurrences of 0 preceding the first 1 is equal to the number of occurrences of 0 preceding the second 1.)

(a) Use the Pumping Lemma to show this language is not regular.
(b) Write down the production rules of a context-free grammar that generates exactly M. Justify your answer.

Solution: (a) If M is regular, then it has a pumping length p. Consider $w = 0^p10^p1 \in M$ and the decomposition $w = xuy$ with $|u| \geq 1$ and $|xu| \leq p$. Since $|xu| \leq p$, u can only consist of zeroes. Let $u = 0^{n_1}$, for some $n_1 \geq 1$. Clearly, $xu^2y \notin M$ as $xu^2y = 0^{p+n_1}10^p1$, so the length of

the first sequence of zeroes is greater than that of the second sequence of zeroes violating the pattern of the language.

(b) Consider the following production rules:

(1) $\langle S \rangle \to 0 \langle A \rangle 01$,
(2) $\langle A \rangle \to 0 \langle A \rangle 0$,
(3) $\langle A \rangle \to 1$.

We can show by induction that a string w generated by these production rules is of one of the following forms:

- $w = \langle S \rangle$,
- $w = 0^n \langle A \rangle 0^n 1$,
- $w = 0^n 1 0^n 1$.

Here $n \geq 1$. These rules will then generate exactly M. Note how these rules differ from the production rules of a regular grammar as non-terminals occur on both sides of the non-terminal in the first two production rules.

MAU22C00: TUTORIAL 11 PROBLEMS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae.

(a) Draw this graph. Write down its incidence table and its incidence matrix.
(b) Write down this graph's adjacency table and its adjacency matrix.
(c) Is this graph complete? Justify your answer.
(d) Is this graph bipartite? Justify your answer.
(e) Is this graph regular? Justify your answer.
(f) Does this graph have any regular subgraph? Justify your answer.
(g) Give an example of an isomorphism from the graph (V, E) specified at the beginning of this problem to the graph (V', E') with vertices p, q, r, s, and t, and edges pq, ps, rt, st, rs, and rq.

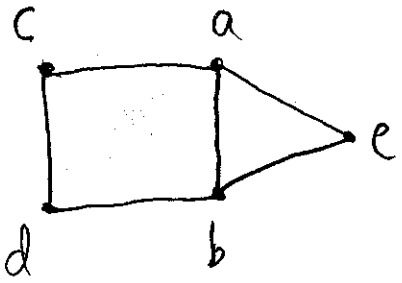
MAU22C00: TUTORIAL 11 SOLUTIONS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae.

(a) Draw this graph. Write down its incidence table and its incidence matrix.
(b) Write down this graph's adjacency table and its adjacency matrix.
(c) Is this graph complete? Justify your answer.
(d) Is this graph bipartite? Justify your answer.
(e) Is this graph regular? Justify your answer.
(f) Does this graph have any regular subgraph? Justify your answer.
(g) Give an example of an isomorphism from the graph (V, E) specified at the beginning of this problem to the graph (V', E') with vertices p, q, r, s, and t, and edges pq, ps, rt, st, rs, and rq.

Solution: Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae.

(a) Here is the graph:



If we keep the same order of the vertices and edges given in the statement of the problem, the incidence table is:

	ab	bd	be	ac	cd	ae
a	1	0	0	1	0	1
b	1	1	1	0	0	0
c	0	0	0	1	1	0
d	0	1	0	0	1	0
e	0	0	1	0	0	1

The corresponding incidence matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b) If we keep the same order of the vertices given in the statement of the problem, the adjacency table is:

	a	b	c	d	e
a	0	1	1	0	1
b	1	0	0	1	1
c	1	0	0	1	0
d	0	1	1	0	0
e	1	1	0	0	0

The corresponding adjacency matrix is

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

(c) No, as for example edge bc does not belong to the graph, so not every vertex is connected to every other vertex.

(d) No, as the graph contains the complete subgraph $V' = \{a, b, e\}$ and $E' = \{ab, ae, be\}$, which cannot be partitioned.

(e) No, as vertices a and b have degree 3, whereas the other vertices have degree 2.

(f) Any two vertices that have an edge between them taken with that edge form a regular subgraph (1-regular) as do $\{a, b, e\}$ and the edges between them (2-regular) and $\{a, b, c, d\}$ and the edges between them (2-regular).

(g) It does NOT suffice to show the two graphs have the same structure. An isomorphism is a MAP, so you must provide the map on vertices. Two possible isomorphisms are $\varphi(a) = s$, $\varphi(b) = r$, $\varphi(c) = p$, $\varphi(d) = q$, and $\varphi(e) = t$ or the following: $\varphi(a) = r$, $\varphi(b) = s$, $\varphi(c) = q$, $\varphi(d) = p$, and $\varphi(e) = t$.

MAU22C00: TUTORIAL 12 PROBLEMS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Draw this graph.
(b) Is this graph connected? Justify your answer.
(c) What is the minimum number of edges you would have to remove for the resulting subgraph to have two connected components? Justify your answer.
(d) What about three connected components? Justify your answer.
(e) What about four connected components? Justify your answer.
(f) What about five connected components? Justify your answer.
(g) Give an example of a shortest possible circuit in the graph. Justify your answer.
(h) Give an example of a longest possible circuit in the graph. Justify your answer.

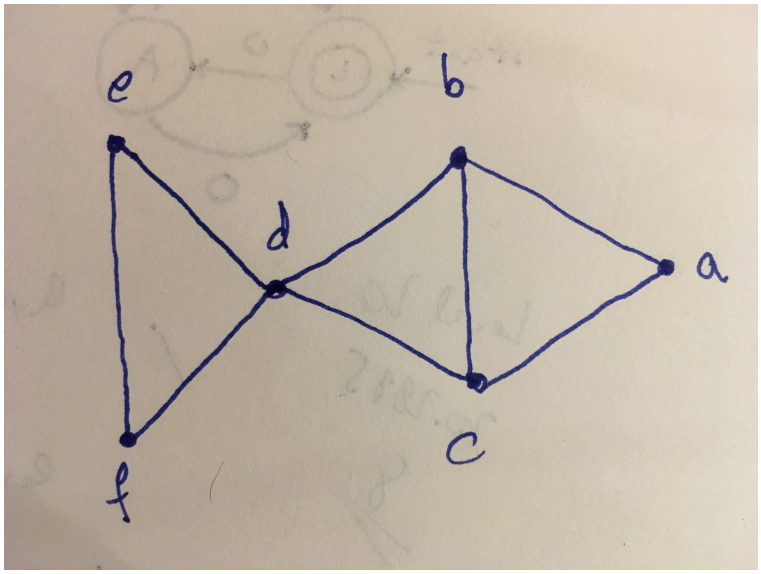
MAU22C00: TUTORIAL 12 SOLUTIONS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Draw this graph.
(b) Is this graph connected? Justify your answer.
(c) What is the minimum number of edges you would have to remove for the resulting subgraph to have two connected components? Justify your answer.
(d) What about three connected components? Justify your answer.
(e) What about four connected components? Justify your answer.
(f) What about five connected components? Justify your answer.
(g) Give an example of a shortest possible circuit in the graph. Justify your answer.
(h) Give an example of a longest possible circuit in the graph. Justify your answer.

Solution: Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Here is the graph:



(b) The graph is connected as there is a walk from every vertex to every other vertex.
(c) Two edges: removing de and ef gives the component consisting of the vertex e alone and the component consisting of abcdf.
(d) Three edges: removing de, ef, and df from the original graph gives the component consisting of vertex e alone, the component consisting of vertex f alone, and the component consisting of abcd.
(e) Five edges: the three we removed before (de, ef, and df) as well as the two edges bd and cd to disconnect vertex d from abc.
(f) Seven edges: besides the five edges we removed (de, ef, df, bd, and cd), we also need to disconnect one vertex from the triangle abc by removing for example ab and ac.
(g) A circuit has a minimum of three vertices as it cannot be trivial, it cannot repeat edges, and it must close up. Any three-vertex circuit in this graph is thus an example of a shortest possible circuit: defd, bcdb, or abca.
(h) abdefdca is an example of a longest possible circuit in this graph. We cannot use edge bc without repeating one other edge, which would not give us a circuit as a circuit is a trail (and cannot repeat edges).

MAU22C00: TUTORIAL 13 PROBLEMS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Does this graph have an Eulerian trail? Justify your answer.

(b) Does this graph have an Eulerian circuit? Justify your answer.

2) For what type of n does the complete graph K_n have an Eulerian circuit? Justify your answer.

3) For what type of n does the complete graph K_n have an Eulerian trail that is not a circuit? Justify your answer.

4) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian circuit? Justify your answer.

5) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian trail that is not a circuit? Justify your answer.

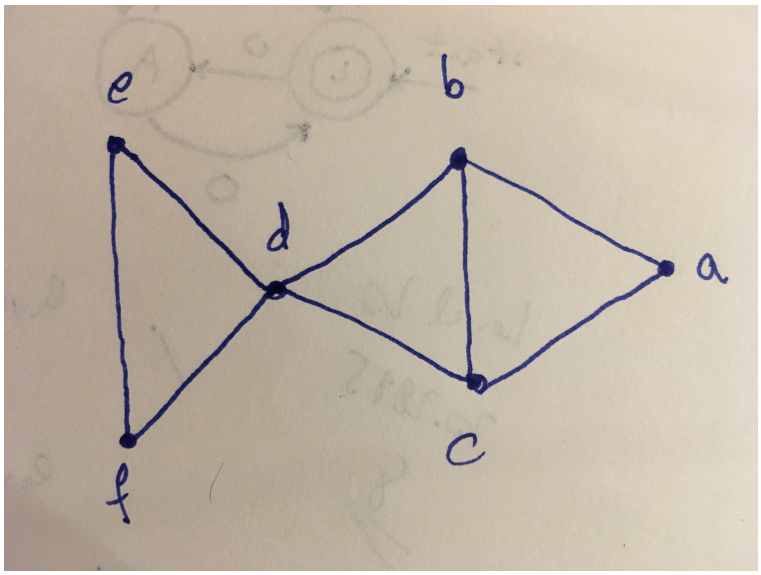
6) Illustrate Lemma B in lecture 36 by finding the longest circuit starting and ending at vertex G, which has no edges in common with circuit $EFGE$ in the graph with vertices A, B, C, D, E, F, G, H, and I, and edges AI, BI, CI, HI, AB, AG, AF, BC, BG, CD, CG, DG, DE, DH, EF, EG, EH, FG, and FH.

MAU22C00: TUTORIAL 13 SOLUTIONS
GRAPH THEORY

1) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Does this graph have an Eulerian trail? Justify your answer.
(b) Does this graph have an Eulerian circuit? Justify your answer.

Solution: Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef. Here is the graph:



(a) $\deg b = \deg c = 3$, so we have two vertices of odd degree, whereas the rest of the vertices have even degrees $\deg a = \deg e = \deg f = 2$ and $\deg d = 4$. By the corollary in lecture 37, this graph must have an Eulerian trail.
(b) Since not all vertices have even degrees, which is a necessary condition for the existence of an Eulerian circuit (Corollary 2 in lecture 35), this graph does not have an Eulerian circuit.

2) For what type of n does the complete graph K_n have an Eulerian circuit? Justify your answer.

Solution: In a complete graph K_n every vertex is connected to every other vertex, so the degree of every vertex is $n-1$. By Euler's theorem

we proved in lecture 37, we need $n-1$ to be even, so n must be odd. Note that we need $n \geq 3$ to have a circuit in the first place, so for $n \geq 3$, n odd K_n has an Eulerian circuit.

3) For what type of n does the complete graph K_n have an Eulerian trail that is not a circuit? Justify your answer.

Solution: Since all vertices have the same degree in the complete graph K_n, we cannot be in the case where all but two of the vertices have odd degree and the rest have even degree unless $n = 2$. Therefore, K_n has an Eulerian trail only for $n = 2$.

4) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian circuit? Justify your answer.

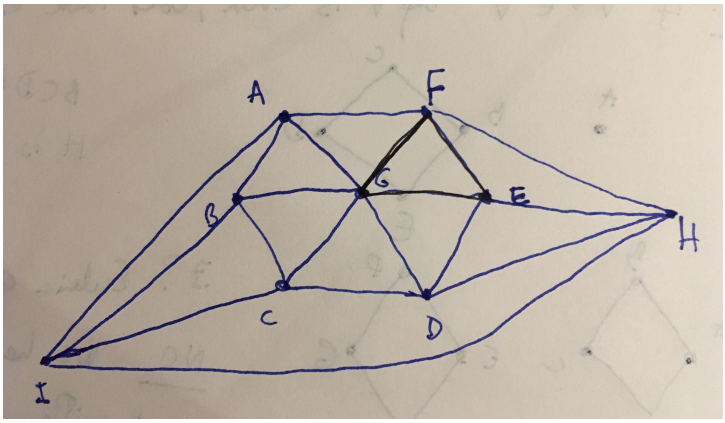
Solution: Recall that a bipartite graph satisfies that its vertices are partitioned into two sets V_1 and V_2 such that $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$, the set of all vertices. In the case of the complete bipartite graph $K_{p,q}$, the number of elements in V_1 is p, and the number of elements in V_2 is q. Therefore, $\forall v \in V_1$, deg v $= q$, and $\forall v \in V_2$, deg v $= p$ as the graph is a complete bipartite graph. For the degrees of all vertices to be even, we must have that both p and q are even to guarantee the existence of an Eulerian circuit. Furthermore, the total number of vertices should be at least 3 for a circuit to exist, so $p \geq 2$, $q \geq 2$ and both are even.

5) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian trail that is not a circuit? Justify your answer.

Solution: Either $p \geq 1$ is odd and $q = 2$ or vice versa $p = 2$ and $q \geq 1$ is odd as we need two vertices to have odd degree and the rest to have even degrees and the degrees of vertices in the same set of the partition, V_1 and V_2, is the same.

6) Illustrate Lemma B in lecture 36 by finding the longest circuit starting and ending at vertex G, which has no edges in common with circuit $EFGE$ in the graph with vertices A, B, C, D, E, F, G, H, and I, and edges AI, BI, CI, HI, AB, AG, AF, BC, BG, CD, CG, DG, DE, DH, EF, EG, EH, FG, and FH.

Solution: Here is the graph:



An example of the longest circuit we could find starting and ending at G, which has no edges in common with circuit $EFGE$ is $GAFHEDHICDGCBIABG$.

MAU22C00: TUTORIAL 14 PROBLEMS
GRAPH THEORY

1) For what type of p and q does the complete bipartite graph $K_{p,q}$ have a Hamiltonian circuit? Justify your answer.

2) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Does this graph have a Hamiltonian circuit? Justify your answer.
(b) Is this graph a tree? Justify your answer.
(c) If it is not a tree, how many distinct spanning trees does it have?

3) Consider the statement "A graph (V, E) is a tree $\iff$ $\#(E) = \#(V) - 1$. " What hypothesis is needed for this equivalence to be true? Give an example to show why this hypothesis is necessary.

Recall that

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

read as " n choose k" gives the number of distinct combinations of k objects taken out of a possible n objects for $n \geq k \geq 0$ with the convention $0! = 1$.

4) Consider the complete graph K_n for $n = 2, 3, 4$. In each of the three cases

(a) Is this graph a tree? Justify your answer.
(b) If it is not a tree, how many distinct spanning trees does it have?

(Hint: How many edges does K_n have?)

MAU22C00: TUTORIAL 14 SOLUTIONS
GRAPH THEORY

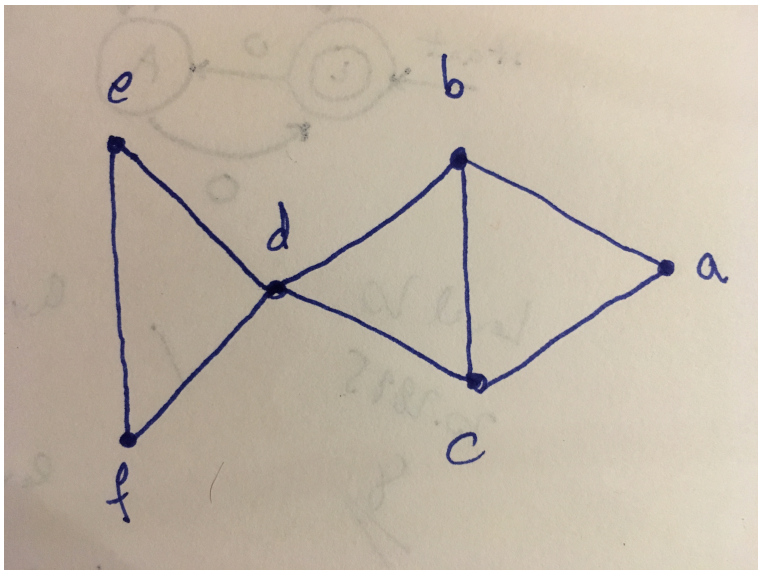
1) For what type of p and q does the complete bipartite graph $K_{p,q}$ have a Hamiltonian circuit? Justify your answer.

Solution: Recall that a bipartite graph satisfies that its vertices are partitioned into two sets V_1 and V_2 such that $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$, the set of all vertices. In the case of the complete bipartite graph $K_{p,q}$, the number of elements in V_1 is p, and the number of elements in V_2 is q. We must have $p = q \geq 2$ for a Hamiltonian circuit to exist as we hop from a vertex in V_1 to a vertex in V_2 and back.

2) Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef.

(a) Does this graph have a Hamiltonian circuit? Justify your answer.
(b) Is this graph a tree? Justify your answer.
(c) If it is not a tree, how many distinct spanning trees does it have?

Solution: Let (V, E) be the graph with vertices a, b, c, d, e, and f and edges ab, ac, bc, bd, cd, de, df, and ef. Here is the graph:



(a) No, as we would have to pass through vertex d twice.
(b) It is not a tree as it contains circuits defd, abca, and bcdb.

(c) We have to break up each of the three circuits by deleting one edge per circuit. The complication is that circuits abca, and bcdb share edge bc. To break up circuit defd, we delete one of de, df, or ef (3 possibilities). To break up circuits abca and bcdb, we could
- either delete one of db and dc (2 possibilities) and one of bc, ba, and ac (3 possibilities) for a total of $2 \cdot 3 = 6$ possibilities
- or keep both db and dc, in which case we must delete bc to break up circuit dcdb and delete either ab or ac for a total of $1 \cdot 2 = 2$ additional possibilities.

Altogether, we have 8 possibilities to break up circuits abca and bcdb and 3 independent possibilities to break up circuit defd for a total of $8 \cdot 3 = 24$ distinct spanning trees.

3) Consider the statement "A graph (V, E) is a tree $\iff$ $\#(E) = \#(V) - 1$. " What hypothesis is needed for this equivalence to be true? Give an example to show why this hypothesis is necessary.

Solution: The missing hypothesis is "connected." If the graph (V, E) is not connected we could have something like the graph with vertices a, b, c, d, and e and edges ab, bc, cd, and da, where the vertex e is isolated. This graph has 5 vertices and 4 edges, but it contains the circuit abcda, so it is not acyclical, and it has two connected components, so it is not connected. Therefore, it cannot be a tree.

Recall that

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

read as " n choose k" gives the number of distinct combinations of k objects taken out of a possible n objects for $n \geq k \geq 0$ with the convention $0! = 1$.

4) Consider the complete graph K_n for $n = 2, 3, 4$. In each of the three cases

(a) Is this graph a tree? Justify your answer.
(b) If it is not a tree, how many distinct spanning trees does it have?

(Hint: How many edges does K_n have?)

Solution: In a complete graph K_n every vertex is connected to every other vertex, so the degree of every vertex is $n - 1$. We have n vertices, so the number of edges in K_n is $\dfrac{n(n-1)}{2}$ as each edge is counted twice. Out of $\dfrac{n(n-1)}{2}$ edges, we are supposed to choose $n - 1$ to construct a spanning tree as we have n vertices, so a tree connecting them has

$n-1$ edges. Therefore, we first check whether our K_n has any circuits. If it does not, it is a tree. If it does, then the count

$$\binom{\frac{n(n-1)}{2}}{n-1}$$

gives the number of ways $n-1$ edges can be chosen, but in certain configurations depending on n, we can get graphs (V, E) satisfying $\#(E) = \#(V) - 1$ that are not connected (as we saw in the previous problem). We have to count those and subtract them from

$$\binom{\frac{n(n-1)}{2}}{n-1}$$

in order to get the number of distinct spanning trees.

$n = 2$ We have 2 vertices and 1 edge, so K_2 is a tree and hence its own spanning tree (1 choice of spanning tree).

$n = 3$ We have 3 vertices and 3 edges, K_3 contains a circuit, so it is not a tree. The number of distinct spanning trees is

$$\binom{3}{2} = \frac{3!}{1!\,2!} = 3$$

as it is not possible in this case to construct subgraphs of K_3 with 3 vertices and 2 edges that are disconnected.

$n = 4$ We have 4 vertices and $\dfrac{4 \cdot 3}{2} = 6$ edges, K_4 contains a number of circuits, so it is not a tree. The number of ways we can choose 3 edges out of 6 is

$$\binom{6}{3} = \frac{6!}{3!\,3!} = 20,$$

but there are

$$4 = \binom{4}{1}$$

different disconnected subgraphs of K_4 consisting of a triangle plus an isolated point. Those are not spanning trees of K_4, so the number of distinct spanning trees is

$$\binom{6}{3} - \binom{4}{1} = \frac{6!}{3!\,3!} - 4 = 20 - 4 = 16.$$

MAU22C00: TUTORIAL 15 PROBLEMS
MINIMAL SPANNING TREES

1) (Annual Exam Trinity Term 2018) Consider the connected undirected graph with vertices A, B, C, D, E, F, G, H, I, J, K, and L, and with edges listed with associated costs in the following table:

CF	JK	IJ	AD	CH	EI	BL	CE	HG	BH
2	2	3	3	3	4	5	6	6	7
EF	FJ	GK	CD	DE	HL	AC	FH	EJ	AB
8	8	9	9	10	10	10	11	12	14

(a) Draw the graph and label each edge with its cost.
(b) Determine the minimum spanning tree generated by Kruskal's Algorithm, where that algorithm is applied with the queue specified in the table above. For each step of the algorithm, write down the edge that is added.

2) In the previous problem, how many distinct ways can the edges of the graph be ordered in non-decreasing order of cost, i.e. how many different non-decreasing queues are there for the edges of the graph? Justify your answer.

3) Would every non-decreasing queue from problem 2 give a different minimal spanning tree when Kruskal's Algorithm is applied? Justify your answer by either a proof or a counterexample.

4) Prove that every nontrivial tree is a bipartite graph.

MAU22C00: TUTORIAL 15 PROBLEMS
MINIMAL SPANNING TREES

1) (Annual Exam Trinity Term 2018) Consider the connected undirected graph with vertices A, B, C, D, E, F, G, H, I, J, K, and L, and with edges listed with associated costs in the following table:

CF	JK	IJ	AD	CH	EI	BL	CE	HG	BH
2	2	3	3	3	4	5	6	6	7
EF	FJ	GK	CD	DE	HL	AC	FH	EJ	AB
8	8	9	9	10	10	10	11	12	14

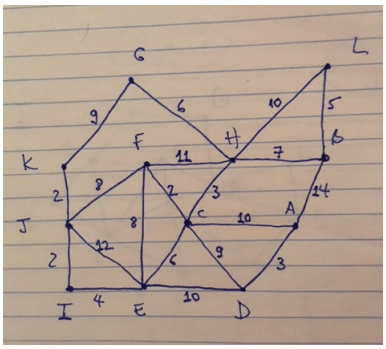
(a) Draw the graph and label each edge with its cost.
(b) Determine the minimum spanning tree generated by Kruskal's Algorithm, where that algorithm is applied with the queue specified in the table above. For each step of the algorithm, write down the edge that is added.

2) In the previous problem, how many distinct ways can the edges of the graph be ordered in non-decreasing order of cost, i.e. how many different non-decreasing queues are there for the edges of the graph? Justify your answer.

3) Would every non-decreasing queue from problem 2 give a different minimal spanning tree when Kruskal's Algorithm is applied? Justify your answer by either a proof or a counterexample.

4) Prove that every nontrivial tree is a bipartite graph.

Solution: 1)(a) Here is the graph:



(b) The edges are added in the following order: CF, JK, IJ, AD, CH, EI, BL, CE, HG, BH, and CD.

2) Two edges have cost 2, so they can be reshuffled (for a total of 2! possibilities), three edges have cost 3, two edges have cost 6, two edges have cost 8, two edges have cost 9, and three edges have cost 10. We thus have

$$2! \times 3! \times 2! \times 2! \times 2! \times 3! = 36 \times 16 = 576$$

ways of obtaining a non-decreasing queue of edges.

3) Not necessarily! Here is a counterexample: Queue CF, JK, IJ, AD, CH, EI, BL, CE, HG, BH, EF, FJ, GH, CD, DE, HL, AC, FH, EJ, AB and queue CF, JK, IJ, AD, CH, EI, BL, CE, HG, BH, FJ, EF, GH, CD, DE, HL, AC, FH, EJ, AB with edges EF and FJ exchanged give the same minimal spanning tree.

4) We need to prove that the vertices V of a tree (V, E) can be partitioned into two sets V_1 and V_2 with $V_1 \cap V_2 = \emptyset$, $V_1 \cup V_2 = V$, and every edge in E has a vertex in V_1 and a vertex in V_2. We do so by induction:

Base Case: The smallest nontrivial tree has 2 vertices. We call them v and w. Since it is a tree, there is an edge between v and w; otherwise, the graph would not be connected. We place vertex v in set V_1 and vertex w in set V_2. Since the only edge vw goes from a vertex in V_1 to a vertex in V_2, this tree with 2 vertices is indeed a bipartite graph as needed.

Inductive Step: Assume that every tree with n vertices is a bipartite graph. We seek to prove the same for every tree with $n + 1$ vertices. Let (V, E) be a tree with $n+1$ vertices. By a theorem proven in lecture 38, (V, E) has at least one pendant vertex. Let v be such a pendant vertex. Since v has degree 1, there is only one edge incident to v. Let us call that edge vw, where w is the other endpoint of this edge. Consider the subgraph (V', E') of (V, E) obtained by deleting vertex v and edge vw. In other words, $V' = V \setminus \{v\}$ and $E' = E \setminus \{vw\}$. (V', E') is clearly still connected and acyclical hence a tree because v was a pendant vertex of the original graph and vw the only edge incident to it. The inductive hypothesis thus applies to (V', E'), which is therefore bipartite. Without loss of generality, assume $w \in V_1$. Place v in V_2. Since vw goes from a vertex in V_1 to a vertex in V_2 and (V', E') is itself bipartite, we conclude (V, E) must be bipartite as well.

MAU22C00: TUTORIAL 16 PROBLEMS
MINIMAL SPANNING TREES AND DIRECTED GRAPHS

1) Prove that any subgraph (V', E') of a connected graph (V, E) is contained in some spanning tree of $(V, E) \iff (V', E')$ contains no circuits.

2) (Annual Exam Trinity Term 2018) Consider the connected undirected graph with vertices A, B, C, D, E, F, G, H, I, J, K, and L, and with edges listed with associated costs in the following table:

CF	JK	IJ	AD	CH	EI	BL	CE	HG	BH
2	2	3	3	3	4	5	6	6	7
EF	FJ	GK	CD	DE	HL	AC	FH	EJ	AB
8	8	9	9	10	10	10	11	12	14

Determine the minimum spanning tree generated by Prim's Algorithm, starting from the vertex F, where that algorithm is applied with the queue specified in the table above. For each step of the algorithm, write down the edge that is added.

3) (Annual Exam Trinity Term 2018)

(a) How many distinct directed graphs with three vertices $V = \{a, b, c\}$ are there? Justify your answer.

(b) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is reflexive **but neither** symmetric **nor** transitive. Justify your answer.

(c) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is symmetric **but neither** reflexive **nor** transitive. Justify your answer.

(d) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is transitive **but not** reflexive **nor** symmetric. Justify your answer.

MAU22C00: TUTORIAL 16 PROBLEMS
MINIMAL SPANNING TREES AND DIRECTED GRAPHS

1) Prove that any subgraph (V', E') of a connected graph (V, E) is contained in some spanning tree of $(V, E) \iff (V', E')$ contains no circuits.

2) (Annual Exam Trinity Term 2018) Consider the connected undirected graph with vertices A, B, C, D, E, F, G, H, I, J, K, and L, and with edges listed with associated costs in the following table:

CF	JK	IJ	AD	CH	EI	BL	CE	HG	BH
2	2	3	3	3	4	5	6	6	7
EF	FJ	GK	CD	DE	HL	AC	FH	EJ	AB
8	8	9	9	10	10	10	11	12	14

Determine the minimum spanning tree generated by Prim's Algorithm, starting from the vertex F, where that algorithm is applied with the queue specified in the table above. For each step of the algorithm, write down the edge that is added.

3) (Annual Exam Trinity Term 2018)

(a) How many distinct directed graphs with three vertices $V = \{a, b, c\}$ are there? Justify your answer.

(b) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is reflexive **but neither** symmetric **nor** transitive. Justify your answer.

(c) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is symmetric **but neither** reflexive **nor** transitive. Justify your answer.

(d) Using the one-to-one correspondence between directed graphs and relations, draw a directed graph that corresponds to a relation on $V = \{a, b, c\}$ that is transitive **but not** reflexive **nor** symmetric. Justify your answer.

Solution: 1) We have to prove an equivalence, which we will do by proving each implication in turn:

" $\Longrightarrow$ " (V', E') is contained in a spanning tree (V, E'') of (V, E). Therefore, $V' \subseteq V$, $E' \subseteq E$, and (V', E') is a subgraph of (V, E'').

Since (V, E'') is a spanning tree of (V, E), it is a tree, so by definition it contains no circuits. Therefore, its subgraph (V', E') cannot contain any circuits either.

" $\Longleftarrow$ " (V', E') contains no circuits. If (V', E') is itself a spanning tree of (V, E), it is clearly contained in a spanning tree, and there is nothing to prove; otherwise, if $V' \subsetneq V$ or (V', E') is not connected, then let $\tilde{E} = E \setminus E'$. Since (V, E) is connected, if $V' \subsetneq V$ or (V', E') is not connected, $\tilde{E} \neq \emptyset$. We seek to add edges from $\tilde{E}$ and their endpoints not already in V' to (V', E') in order to construct a spanning tree. Since $\tilde{E}$ is a finite set, we can write it as $\tilde{E} = \{e_1, e_2, \ldots, e_m\}$. We now examine each edge in $\tilde{E}$ in turn. Consider e_1. If adding e_1 to (V', E') produces a circuit, then discard e_1; otherwise, add e_1 to (V', E') along with any of its endpoints not already in (V', E') and denote by (V_1, E_1) the resulting graph. If e_1 is discarded, then let $(V_1, E_1) = (V', E')$. We continue this process. Consider e_2. If adding e_2 to (V_1, E_1) produces a circuit, then discard e_2; otherwise, add e_2 to (V_1, E_1) along with any of its endpoints not already in (V_1, E_1) and denote by (V_2, E_2) the resulting graph. If e_2 is discarded, then let $(V_2, E_2) = (V_1, E_1)$. At step j of this process, consider e_j. If adding e_j to (V_{j-1}, E_{j-1}) produces a circuit, then discard e_j; otherwise, add e_j to (V_{j-1}, E_{j-1}) along with any of its endpoints not already in (V_{j-1}, E_{j-1}) and denote by (V_j, E_j) the resulting graph. If e_j is discarded, then let $(V_j, E_j) = (V_{j-1}, E_{j-1})$. The process stops after e_m is considered, hence after m steps. Since the starting subgraph (V', E') had no circuits and since all edges not already in E' were considered and only added if no circuit was created, the resulting graph (V_m, E_m) cannot contain any circuits. Note that we added all vertices not already in V' that were endpoints of edges added. Assume $\exists\, v \in V \setminus V_m$. Since all edges in E are either in E' or were considered by the algorithm, v cannot be an endpoint of either an edge in E' or in $\tilde{E}$, but $E = E' \cup \tilde{E}$. Therefore, v is not incident to any edge in E. We conclude that $\deg v = 0$ in (V, E), which means (V, E) contains an isolated vertex. $v \notin V'$, $\deg v = 0$, and $V' \neq \emptyset$ together imply that (V, E) has at least two components $\Rightarrow\!\!\!\!\!\!\Leftarrow$ as (V, E) is connected. Therefore, $V \setminus V_m = \emptyset$, so $V_m = V$. We have obtained a subgraph (V_m, E_m) of (V, E) that has no circuits and satisfies $V_m = V$. To show, (V_m, E_m) is a spanning tree of (V, E), we must show that it is connected. Assume not, then (V_m, E_m) contains at least two components. Assume vertices v and w belong to different components of (V_m, E_m). (V, E) is connected, so there exists a path from v to w via edges in (V, E). Some of those edges in this path then do not belong to E_m $\Rightarrow\!\!\!\!\!\!\Leftarrow$ as these edges were in $\tilde{E}$ and should have

been added at some step i of the algorithm since their addition could not have created a circuit. Therefore, (V_m, E_m) is connected, so it is a spanning tree of (V, E) containing (V', E'). □

2) The edges are added in the following order: CF, CH, CE, EI, IJ, JK, HG, BH, BL, CD, and AD.

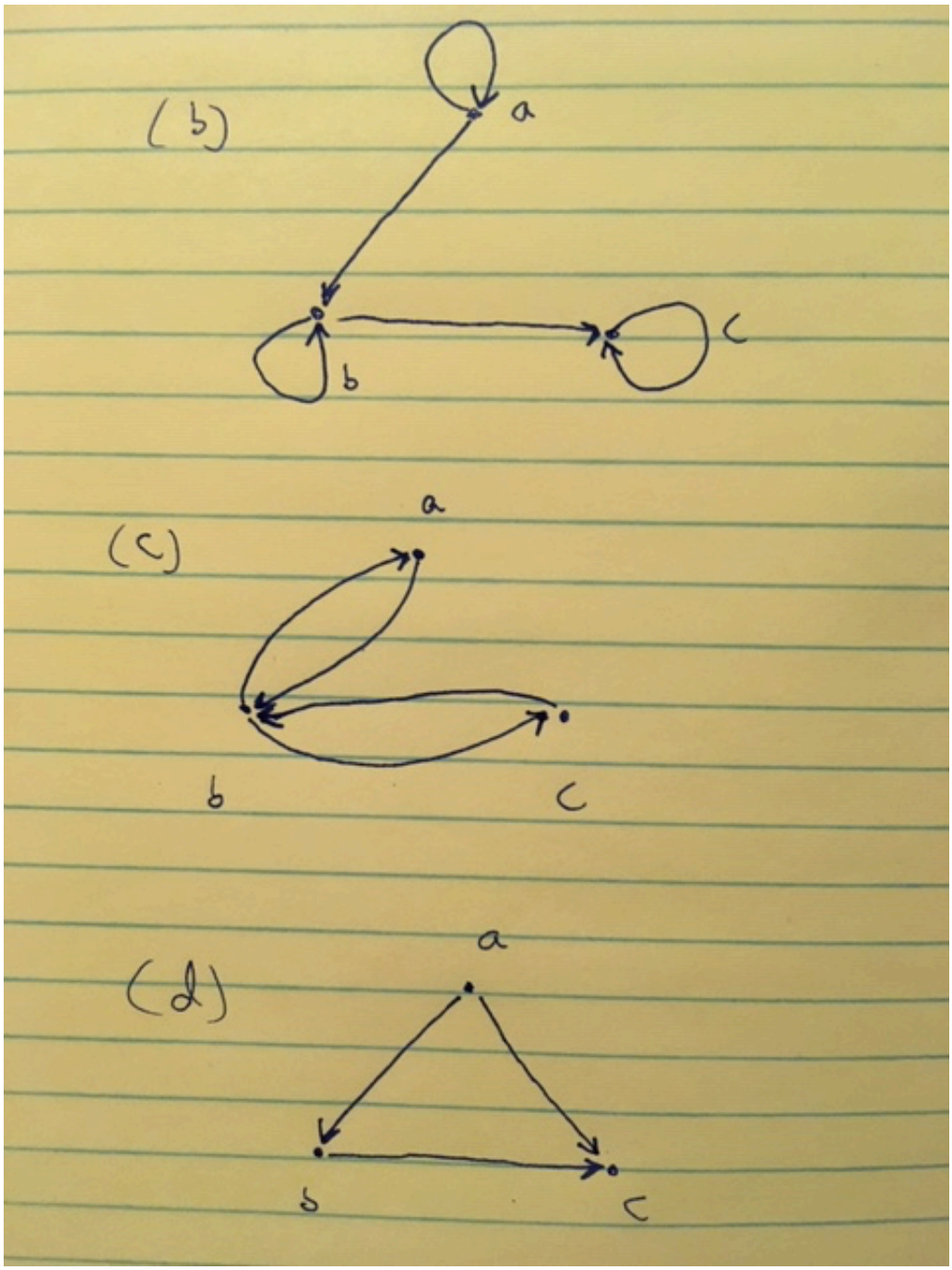
3) (a) An edge of a directed graph is any pair in $V \times V$. Since V has 3 elements, there are $3 \times 3 = 9$ different such pairs hence possible edges. A directed graph on three vertices $V = \{a, b, c\}$ will have as its set of edge a subset of this 9-element set. As the power set of a set of nine elements has $2^9 = 512$ elements, there are 512 distinct directed graphs on 3 vertices $\{a, b, c\}$.

For (b), (c), (d), note that reflexivity is universally quantified, whereas symmetry and transitivity are given by implications, which are vacuously true if the antecedents (the 'if" part of the statements) fail to be true. The graphs are drawn at the end of the solutions.

(b) $E = \{(a, a), (b, b), (c, c), (a, b), (b, c)\}$. Since (b, a) and (c, b) are missing, the relation isn't symmetric. Since (a, c) is missing but (a, b) and (b, c) are present, the relation isn't transitive. The presence of (a, a), (b, b), and (c, c) makes the relation reflexive.

(c) $E = \{(a, b), (b, a), (b, c), (c, b)\}$. No (a, a) in E means the relation isn't reflexive. No (a, c) and (c, a) in E makes the relation non-transitive. The pairs (a, b) with (b, a) and (b, c) with (c, a) make the relation symmetric.

(d) $E = \{(a, b), (b, c), (a, c)\}$. Those three pairs make the relation transitive. Since (b, a) is not present, the relation isn't symmetric. Since (a, a) isn't present, the relation isn't reflexive.


(b)
a
b
c
(c)
a
b
c
(d)
a
b
c

MAU22C00: TUTORIAL 17 PROBLEMS
COUNTABILITY OF SETS

For each of the following sets, determine whether it is finite, countably infinite, or uncountably infinite. Justify your answer.

1) The set of integers divisible by 7.

2) $\{11^p \mid p \in \mathbb{Z}\}$

3) $\left\{\left(\frac{m}{3}, \frac{n}{5}\right) \in \mathbb{R}^2 \;\middle|\; m, n \in \mathbb{Z}\right\}$

4) $\{x \in \mathbb{C} \mid x^4 - 2x - 1 = 0\}$

5) $\{(x, y) \in \mathbb{R}^2 \mid y = x^6\} \cap \mathbb{Z}^2$

6) $\{x \in \mathbb{R} \mid \sin x = 1\}$

7) $\bigcup_{q \in \mathbb{Q}} L_q$ where $L_q = \{(x, y) \in \mathbb{R}^2 \mid x = q\} \cap (\mathbb{Q} \times \mathbb{N})$.

MAU22C00: TUTORIAL 17 PROBLEMS
COUNTABILITY OF SETS

For each of the following sets, determine whether it is finite, countably infinite, or uncountably infinite. Justify your answer.

1) The set of integers divisible by 7.

2) $\{11^p \mid p \in \mathbb{Z}\}$

3) $\left\{\left(\frac{m}{3}, \frac{n}{5}\right) \in \mathbb{R}^2 \mid m, n \in \mathbb{Z}\right\}$

4) $\{x \in \mathbb{C} \mid x^4 - 2x - 1 = 0\}$

5) $\{(x, y) \in \mathbb{R}^2 \mid y = x^6\} \cap \mathbb{Z}^2$

6) $\{x \in \mathbb{R} \mid \sin x = 1\}$

7) $\bigcup_{q \in \mathbb{Q}} L_q$ where $L_q = \{(x, y) \in \mathbb{R}^2 \mid x = q\} \cap (\mathbb{Q} \times \mathbb{N})$.

Solution: 1) An integer $m \in \mathbb{Z}$ is divisible by 7 if there exists some integer $p \in \mathbb{Z}$ such that $m = 7p$. Therefore, the set A of integers divisible by 7 is given by $A = \{7p \mid p \in \mathbb{Z}\}$. The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(p) = 7p$ is a bijection (check!). Therefore, $A \sim \mathbb{Z}$, and we know from lecture that $\mathbb{Z}$ is countably infinite. Therefore, the set A of integers divisible by 7 is countably infinite.

2) $\{11^p \mid p \in \mathbb{Z}\} \sim \mathbb{Z}$ via the bijection $f(p) = 11^p$ (check it is a bijection). Therefore, the set is countably infinite.

3) $\mathbb{Z} \times \mathbb{Z} \subset \left\{\left(\frac{m}{3}, \frac{n}{5}\right) \in \mathbb{R}^2 \mid m, n \in \mathbb{Z}\right\} \subset \mathbb{Q} \times \mathbb{Q}$. Since both $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$ and $\mathbb{Q} \times \mathbb{Q} = \mathbb{Q}^2$ are countably infinite as proven in class, the set itself is sandwiched between two countably infinite sets, so it must be countably infinite.

4) $\{x \in \mathbb{C} \mid x^4 - 2x - 1 = 0\}$ consists of all roots of the polynomial $x^4 - 2x - 1 = 0$, which has degree 4. Therefore, there are at most 4 roots over $\mathbb{R}$ and exactly 4 roots over $\mathbb{C}$ by the Fundamental Theorem of Algebra. It means our set must be finite.

5) $\{(x, y) \in \mathbb{R}^2 \mid y = x^6\} \cap \mathbb{Z}^2$ is a subset of $\mathbb{Z}^2$ by definition, and $\mathbb{Z}^2$ is countably infinite as proven in class. A subset of a countably infinite set could be either finite or countably infinite. It remains to figure out which one of the two is true for our set. We note that the set of all pairs (x, x^6) for $x \in \mathbb{Z}$ is a subset of our set. The set of all such pairs is countably infinite because $\{(x, x^6) \mid x \in \mathbb{Z}\} \sim \mathbb{Z}$ (it is in one-to-one

correspondence with $\mathbb{Z}$.) Therefore, $\{(x,y) \in \mathbb{R}^2 \mid y = x^6\} \cap \mathbb{Z}^2$ is countably infinite.

6)

$$\{x \in \mathbb{R} \mid \sin x = 1\} = \left\{\frac{\pi}{2} + 2\pi n \mid n \in \mathbb{Z}\right\} \sim \mathbb{Z}$$

because the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = 2\pi n$ is a bijection, so the set must be countably infinite.

7) $L_q = \{(x,y) \in \mathbb{R}^2 \mid x = q\} \cap (\mathbb{Q} \times \mathbb{N}) = \{q\} \times \mathbb{N} \sim \mathbb{N}$. Therefore, $\bigcup_{q \in \mathbb{Q}} L_q$ is a union of disjoint countably infinite sets and thus countably infinite by the theorem proven in class.

MAU22C00: TUTORIAL 18 PROBLEMS
COUNTABILITY OF SETS

For each of the following sets, determine whether it is finite, countably infinite, or uncountably infinite. Justify your answer.

1) $\bigcup_{q\in\mathbb{Q}} L_q$ where $L_q = \{(x,y) \in \mathbb{R}^2 \mid x = q\}$.

2) $\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{Q}\}$

3) $\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{R} \setminus \mathbb{Q}\}$

4) $\{(x,y,z) \in \mathbb{N}^3 \mid x^2 + y^2 = z^2 \text{ and } x,y,z \in \mathbb{N}^*\}$, the Pythagorean triplets that give the lengths of the legs and the hypothenuse of a right triangle.

5) $\{(x,y) \in \mathbb{R}^2 \mid y = x^2 + 1\}$

6) $\mathcal{P}(J_n) \times \mathcal{P}(\mathbb{N})$, where $J_n = \{1,\ldots,n\}$ and $\mathcal{P}(A)$ is the power set of a set A.

7) $\mathbb{R}^n$ for $n \geq 1$.

MAU22C00: TUTORIAL 18 PROBLEMS
COUNTABILITY OF SETS

For each of the following sets, determine whether it is finite, countably infinite, or uncountably infinite. Justify your answer.

1) $\bigcup_{q\in\mathbb{Q}} L_q$ where $L_q = \{(x,y) \in \mathbb{R}^2 \mid x = q\}$.

2) $\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{Q}\}$

3) $\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{R} \setminus \mathbb{Q}\}$

4) $\{(x,y,z) \in \mathbb{N}^3 \mid x^2 + y^2 = z^2 \text{ and } x,y,z \in \mathbb{N}^*\}$, the Pythagorean triplets that give the lengths of the legs and the hypothenuse of a right triangle.

5) $\{(x,y) \in \mathbb{R}^2 \mid y = x^2 + 1\}$

6) $\mathcal{P}(J_n) \times \mathcal{P}(\mathbb{N})$, where $J_n = \{1,\dots,n\}$ and $\mathcal{P}(A)$ is the power set of a set A.

7) $\mathbb{R}^n$ for $n \geq 1$.

Solution: 1) $L_q = \{(x,y) \in \mathbb{R}^2 \mid x = q\} = \{q\} \times \mathbb{R} \sim \mathbb{R}$. Therefore, $\bigcup_{q\in\mathbb{Q}} L_q$ is a countably infinite union of disjoint uncountably infinite sets, so it must itself be uncountably infinite as it contains $\{0\} \times \mathbb{R} \sim \mathbb{R}$, which is uncountably infinite.

2) $\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{Q}\}$ is a finite set. Let $q = \dfrac{r}{s}$ for $r,s \in \mathbb{Z}$, $s \neq 0$, $(r,s) = 1$. Therefore, $a^p = e^{\frac{pr\pi i}{s}}$, which assumes one of s values $e^{\frac{\pi i}{s}}, e^{\frac{2\pi i}{s}}, \dots, e^{\frac{(s-1)\pi i}{s}}, e^{\frac{s\pi i}{s}}$ depending upon the value of p. We conclude that our set is finite

$$\{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{Q}\} = \left\{e^{\frac{\pi i}{s}}, e^{\frac{2\pi i}{s}}, \dots, e^{\frac{(s-1)\pi i}{s}}, e^{\frac{s\pi i}{s}}\right\}.$$

3) $A = \{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{R} \setminus \mathbb{Q}\}$ is countably infinite. Since $q \in \mathbb{R} \setminus \mathbb{Q}$, $a^{p_1} \neq a^{p_2}$ if $p_1 \neq p_2$, so the map $f : \mathbb{N} \to A$ given by $f(p) = a^p$ is a bijection. Therefore,

$$A = \{a^p \mid p \in \mathbb{N} \text{ and } a = e^{q\pi i} \text{ for } q \in \mathbb{R} \setminus \mathbb{Q}\} \sim \mathbb{N}.$$

4) $\{(x,y,z) \in \mathbb{N}^3 \mid x^2 + y^2 = z^2 \text{ and } x,y,z \in \mathbb{N}^*\} \subset \mathbb{N}^3$, and we know from class that $\mathbb{N}^3$ is countably infinite. Therefore, our set can be

finite or countably infinite. We will prove that it is countably infinite by showing that it has a countably infinite subset. We remark that

$$(3,4,5) \in \{(x,y,z) \in \mathbb{N}^3 \mid x^2+y^2=z^2 \text{ and } x,y,z \in \mathbb{N}^*\}$$

as $3^2+4^2 = 9+16 = 25 = 5^2$. Furthermore,

$$(3p,4p,5p) \in \{(x,y,z) \in \mathbb{N}^3 \mid x^2+y^2=z^2 \text{ and } x,y,z \in \mathbb{N}^*\}$$

for every $p \in \mathbb{N}^*$ as $3^2p^2+4^2p^2 = 9p^2+16p^2 = 5^2p^2$. Since $\mathbb{N}^* \sim \mathbb{N}$ is countably infinite, the subset $\{(3p,4p,5p) \mid p \in \mathbb{N}^*\}$ is countably infinite, hence our set must likewise be countably infinite.

5) Consider the subset A of $\{(x,y) \in \mathbb{R}^2 \mid y = x^2+1\}$ given by

$$A = \{(x,y) \in \mathbb{R}^2 \mid y = x^2+1\} \cap [(0,1) \times \mathbb{R}].$$

The function $f(x) = x^2+1 = y$ is a bijection on $(0,1)$ (easy to check). Therefore, $\{(x,y) \in \mathbb{R}^2 \mid y = x^2+1\} \cap [(0,1) \times \mathbb{R}] \sim (0,1)$, so the set A is uncountably infinite as we proved in class that $(0,1)$ was uncountably infinite. Since $A \subset \{(x,y) \in \mathbb{R}^2 \mid y = x^2+1\}$, the set $\{(x,y) \in \mathbb{R}^2 \mid y = x^2+1\}$ must itself be uncountably infinite. Note that we have employed here a very standard technique for showing a set is uncountably infinite. It suffices to show it has an uncountably infinite subset.

6) As you saw during Michaelmas term, the number of elements of a set with n elements is 2^n, so $\mathcal{P}(J_n)$ is a finite set with 2^n elements, where $n \geq 1$ by the definition of J_n. By contrast, we proved in class that $\mathcal{P}(\mathbb{N})$ is uncountably infinite. Thus, our set is a Cartesian product of a finite set with an uncountably infinite set. Since $J_n = \{1,\ldots,n\}$ for $n \geq 1$, the subset containing just the element 1 is always in $\mathcal{P}(J_n)$ for every $n \geq 1$, $\{1\} \in \mathcal{P}(J_n)$. Therefore, $\{1\} \times \mathcal{P}(\mathbb{N}) \subset \mathcal{P}(J_n) \times \mathcal{P}(\mathbb{N})$, but $\{1\} \times \mathcal{P}(\mathbb{N}) \sim \mathcal{P}(\mathbb{N})$. We conclude that $\mathcal{P}(J_n) \times \mathcal{P}(\mathbb{N})$ has an uncountably infinite subset, so it itself must be uncountably infinite.

7) For $n = 1$, we have already shown in class that $\mathbb{R}^1 = \mathbb{R}$ was uncountably infinite. Now for $n \geq 2$ consider

$$\mathbb{R}^n = \{(x_1,\ldots,x_n) \mid x_i \in \mathbb{R}\ \forall i\}.$$

The set

$$\mathbb{R} \times \{0\} \cdots \{0\} = \{(x_1, 0 \ldots, 0) \mid x_1 \in \mathbb{R}\} \subset \mathbb{R}^n,$$

but $\mathbb{R} \times \{0\} \cdots \{0\} \sim \mathbb{R}$, which is uncountably infinite. Therefore, $\mathbb{R}^n$ has an uncountably infinite subset, which means it must itself be uncountably infinite.

MAU22C00: TUTORIAL 19 PROBLEMS

1) Is $\{x \in \mathbb{R}^+ \mid \log x \in \mathbb{R} \setminus \mathbb{Q}\}$ finite, countably infinite, or uncountably infinite? Justify your answer. The set $\mathbb{R}^+$ is the set of all positive real numbers.

2) Is $\bigcup_{n=1}^{10} \left\{ \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = n^2\} \cap \{(x,y) \in \mathbb{R}^2 \mid y^2 - x^4 = 0\} \right\}$ finite, countably infinite, or uncountably infinite? Justify your answer.

3) Let $A = \{0,1\}$. Is $(0^* \circ 1^*) \cap \{A^* \circ 11 \circ A^*\}$ finite, countably infinite, or uncountably infinite? Justify your answer.

4) Prove that the language generated by a regular expression is countable. Give an example of a regular expression that generates a finite language and another example of a regular expression that generates a countably infinite language. Justify your answers.

5) Consider the language over the binary alphabet $A = \{0,1\}$ given by $L = \{0^m 1^{2m} \mid m \in \mathbb{N}\}$.

(a) Use the Pumping Lemma to show L is not a regular language.

(b) Is the language L finite, countably infinite, or uncountably infinite? Justify your answer.

(c) A language L' over the same alphabet $A = \{0,1\}$ is called a *sublanguage* of L if $L' \subset L$. Let $\mathcal{C}$ be the set of sublanguages of L. Is $\mathcal{C}$ finite, countably infinite, or uncountably infinite? Justify your answer.

MAU22C00: TUTORIAL 19 SOLUTIONS

1) Is $\{x \in \mathbb{R}^+ \mid \log x \in \mathbb{R} \setminus \mathbb{Q}\}$ finite, countably infinite, or uncountably infinite? Justify your answer. The set $\mathbb{R}^+$ is the set of all positive real numbers.

2) Is $\bigcup_{n=1}^{10} \left\{ \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = n^2\} \cap \{(x,y) \in \mathbb{R}^2 \mid y^2 - x^4 = 0\} \right\}$ finite, countably infinite, or uncountably infinite? Justify your answer.

3) Let $A = \{0,1\}$. Is $(0^* \circ 1^*) \cap \{A^* \circ 11 \circ A^*\}$ finite, countably infinite, or uncountably infinite? Justify your answer.

4) Prove that the language generated by a regular expression is countable. Give an example of a regular expression that generates a finite language and another example of a regular expression that generates a countably infinite language. Justify your answers.

5) Consider the language over the binary alphabet $A = \{0,1\}$ given by $L = \{0^m 1^{2m} \mid m \in \mathbb{N}\}$.

(a) Use the Pumping Lemma to show L is not a regular language.

(b) Is the language L finite, countably infinite, or uncountably infinite? Justify your answer.

(c) A language L' over the same alphabet $A = \{0,1\}$ is called a *sublanguage* of L if $L' \subset L$. Let $\mathcal{C}$ be the set of sublanguages of L. Is $\mathcal{C}$ finite, countably infinite, or uncountably infinite? Justify your answer.

Solution: 1) The log function $log : \mathbb{R}^+ \to \mathbb{R}$ is bijective as you learned before coming to university, which means $\{x \in \mathbb{R}^+ \mid \log x \in \mathbb{R} \setminus \mathbb{Q}\}$ is in bijective correspondence with $\mathbb{R} \setminus \mathbb{Q}$. We showed in lecture that $\mathbb{R}$ is uncountably infinite, while $\mathbb{Q}$ is countably infinite. We also showed in lecture that taking out a countably infinite set from an uncountably infinite one leaves an uncountably infinite set. Therefore, $\{x \in \mathbb{R}^+ \mid \log x \in \mathbb{R} \setminus \mathbb{Q}\}$ is uncountably infinite.

2) $y^2 - x^4 = (y - x^2)(y + x^2) = 0$ so for each n, we are intersecting the circle centered at the origin of radius n with the two parabolae $y = x^2$ and $y = -x^2$. This gives us four intersection points, and we have ten values for n. For different values of n, we get different intersection points, so we

have a total of 40 points in the set $\bigcup_{n=1}^{10} \left\{ \left\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=n^2\right\} \cap \left\{(x,y) \in \mathbb{R}^2 \mid y^2-x^4=0\right\} \right\}$, which is thus finite.

3) $(0^* \circ 1^*) \cap \{A^* \circ 11 \circ A^*\} = 0^* \circ 11 \circ 1^*$. Each of 0^* and 1^* is countably infinite, so the given set is countably infinite.

4) By definition, a set is countable, if it is finite or countably infinite. A regular expression is built up from $\emptyset$, ϵ, and the letters of the alphabet A via the Kleene star $*$, concatenation, and union. The Kleene star makes a countably infinite set out of a finite one. Concatenation gives a set whose size matches the size of the biggest set in the concatenation. In other words, the concatenation of strings from two finite sets will yield a finite set. The concatenation of strings from a finite set with a countably infinite set will yield a countably infinite set, whereas the concatenation of strings from two countably infinite sets yields a countably infinite set. Union behaves just like concatenation. Therefore, from a finite set via the Kleene star, union, and concatenation, we can only obtain a finite set or a countably infinite set. This concludes our proof. To give the required examples, let us consider the binary alphabet $A = \{0, 1\}$. The regular expression $\{01\} \cup \{11\}$ yields a regular language with two elements, whereas the regular expression $0^* \cup 1^*$ gives the regular language consisting of all strings of just 0's and all strings of just 1's, which is countably infinite as the sequence of strings ϵ, 0, 00, 000, etc. is inside this language.

5) (a) If L is a regular language, then it has a pumping length p. In order to consider just one case, we work with $w = 0^p 1^{2p} \in L$. According to the Pumping Lemma, w is to be decomposed as xuy, where $|u| \geq 1$ and $|xu| \leq p$. Since $|xu| \leq p$, u can only consist of zeroes. Let $u = 0^{n_1}$, for some $n_1 \geq 1$. Clearly, $xu^2y \notin L$ as $xu^2y = 0^{p+n_1}1^{2p}$, so the length of the first sequence of zeroes is not one half that of the second sequence of zeroes violating the pattern of the language.

(b) The language L is countably infinite. Consider the function $f : \mathbb{N} \to L$ given by $f(m) = 0^m 1^{2m}$. It is easy to see that f is both injective and surjective hence bijective. Therefore, L is in one-to-one correspondence with $\mathbb{N}$, hence L is countably infinite.

(c) Since a language L' is a sublanguage of L if $L' \subset L$, the set of sublanguages of L, $\mathcal{C}$, is exactly the power set of L, which is denoted by $\mathcal{P}(L)$. We proved in part (c) that L is countably infinite, so $L \sim \mathbb{N}$. Therefore, $\mathcal{P}(L) \sim \mathcal{P}(\mathbb{N})$. As we proved in lecture, $\mathcal{P}(\mathbb{N})$ is uncountably infinite, so $\mathcal{C} = \mathcal{P}(L)$ must likewise be uncountably infinite.

MAU22C00: TUTORIAL 20 PROBLEMS
TURING MACHINES

1) Consider the language over the binary alphabet $A = \{0, 1\}$ given by $L = \{0^m 1^{2m} \mid m \in \mathbb{N}\}$.

(a) Write down the algorithm of a Turing machine that recognizes L. Process the following strings according to your algorithm: ϵ, 01, 011, and 010.

(b) Draw the transition diagram of the Turing machine from part (a) carefully labelling the initial state, the accept state, the reject state, and all the transitions specified in your algorithm.

MAU22C00: TUTORIAL 20 SOLUTIONS
TURING MACHINES

1) Consider the language over the binary alphabet $A = \{0, 1\}$ given by $L = \{0^m 1^{2m} \mid m \in \mathbb{N}\}$.

(a) Write down the algorithm of a Turing machine that recognizes L. Process the following strings according to your algorithm: ϵ, 01, 011, and 010.

(b) Draw the transition diagram of the Turing machine from part (a) carefully labelling the initial state, the accept state, the reject state, and all the transitions specified in your algorithm.

Solution: 1) (a) Here is the algorithm for recognising $L = \{0^m 1^{2m} : m \in \mathbb{N}\}$.

(1) If there is a blank in the first cell, ACCEPT. If there is anything else, apart from 0, then REJECT.
(2) If 0 is in the current cell, delete it, then move right to the first 1.
(3) If there is no first 1, REJECT. Otherwise change 1 to x.
(4) Move to the leftmost non blank symbol. If 0, go to step 2. If 1, REJECT. If x, go to step 5. If y, go to step 6.
(5) Delete x, move right to the nearest 1. If none, REJECT. Otherwise change it to y and go to step 4.
(6) Move right to the rightmost non blank character. If anything but y is found, REJECT. Otherwise, ACCEPT.

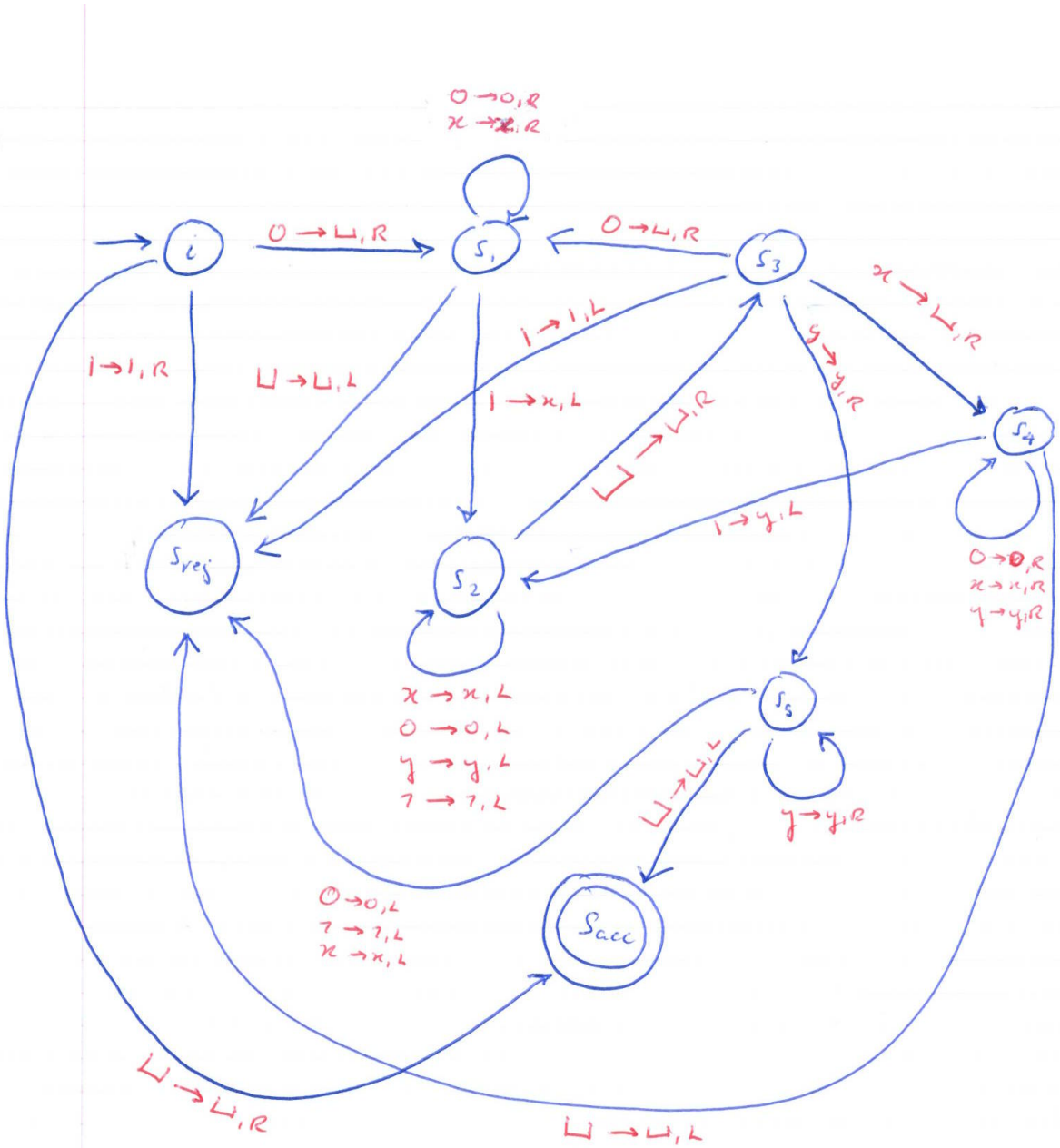
Here is how the following strings are treated:

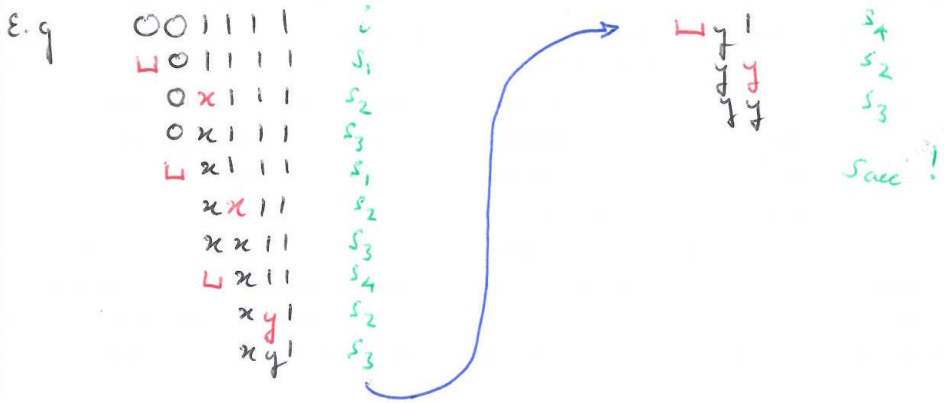
- ϵ is accepted immediately.
- $01 \to \sqcup 1 \to \sqcup x \to \sqcup\sqcup \to$ REJECT.
- $011 \to \sqcup 11 \to \sqcup x1 \to \sqcup\sqcup 1 \to \sqcup\sqcup y \to$ ACCEPT.
- $010 \to \sqcup 10 \to \sqcup x0 \to \sqcup\sqcup 0 \to$ REJECT.

(b) Here is transition diagram for

$$T = (\{i, s_1, s_2, s_3, s_4, s_5, s_{\text{acc}}, s_{\text{rej}}\}, \{0, 1\}, \{0, 1, x, y, \sqcup\}, t, i, s_{\text{acc}}, s_{\text{rej}})$$

along with an example of an accepted string:


0 → 0, R
x → x, R
i
s1
s2
s3
s4
s5
s_rej
s_acc
0 → ␣, R
␣ → ␣, L
1 → 1, R
1 → 1, L
1 → x, L
x → x, R
␣ → ␣, R
y → y, R
1 → y, L
0 → 0, L
1 → 1, L
x → x, L
y → y, L
␣ → ␣, L


e.g.
i
s1
s2
s3
s1
s2
s3
s4
s2
s3
s4
s2
s3
s_acc !

MAU22C00: TUTORIAL 21 PROBLEMS
TURING MACHINES

1) Consider the language over the binary alphabet $A = \{0, 1\}$ given by

$$L = \{(01)^m \mid m \in \mathbb{N}\} = \{\epsilon, 01, 0101, 010101, \dots\}.$$

(a) Draw a finite state acceptor that accepts L. Be sure to carefully label the initial state, the accept states, and all the transitions.

(b) Write down the algorithm of a Turing machine M that recognizes L.

(c) Draw the transition diagram of the Turing machine M from part (b). How is it different from the finite state acceptor you drew in part (a)?

2) Consider the language over the decimal digits

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

given by $L = \{3m \mid m \in \mathbb{N}\}$. Write down the algorithm of a Turing machine that **decides** L. Process the following strings according to your algorithm: 0, 1, 5, and 9.

MAU22C00: TUTORIAL 21 PROBLEMS
TURING MACHINES

1) Consider the language over the binary alphabet $A = \{0, 1\}$ given by

$$L = \{(01)^m \mid m \in \mathbb{N}\} = \{\epsilon, 01, 0101, 010101, \dots\}.$$

(a) Draw a finite state acceptor that accepts L. Be sure to carefully label the initial state, the accept states, and all the transitions.

(b) Write down the algorithm of a Turing machine M that recognizes L.

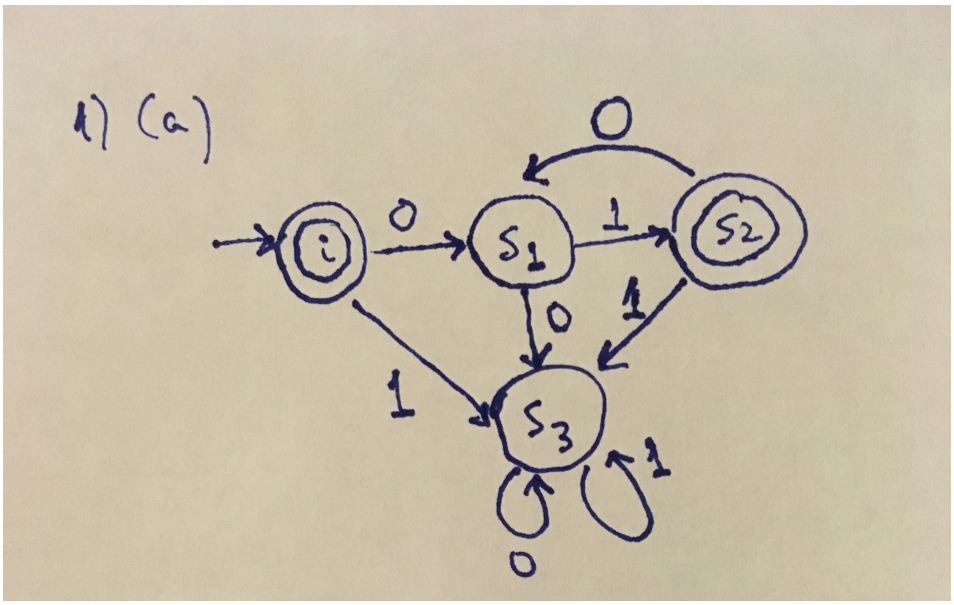
(c) Draw the transition diagram of the Turing machine M from part (b). How is it different from the finite state acceptor you drew in part (a)?

2) Consider the language over the decimal digits

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

given by $L = \{3m \mid m \in \mathbb{N}\}$. Write down the algorithm of a Turing machine that **decides** L. Process the following strings according to your algorithm: 0, 1, 5, and 9.

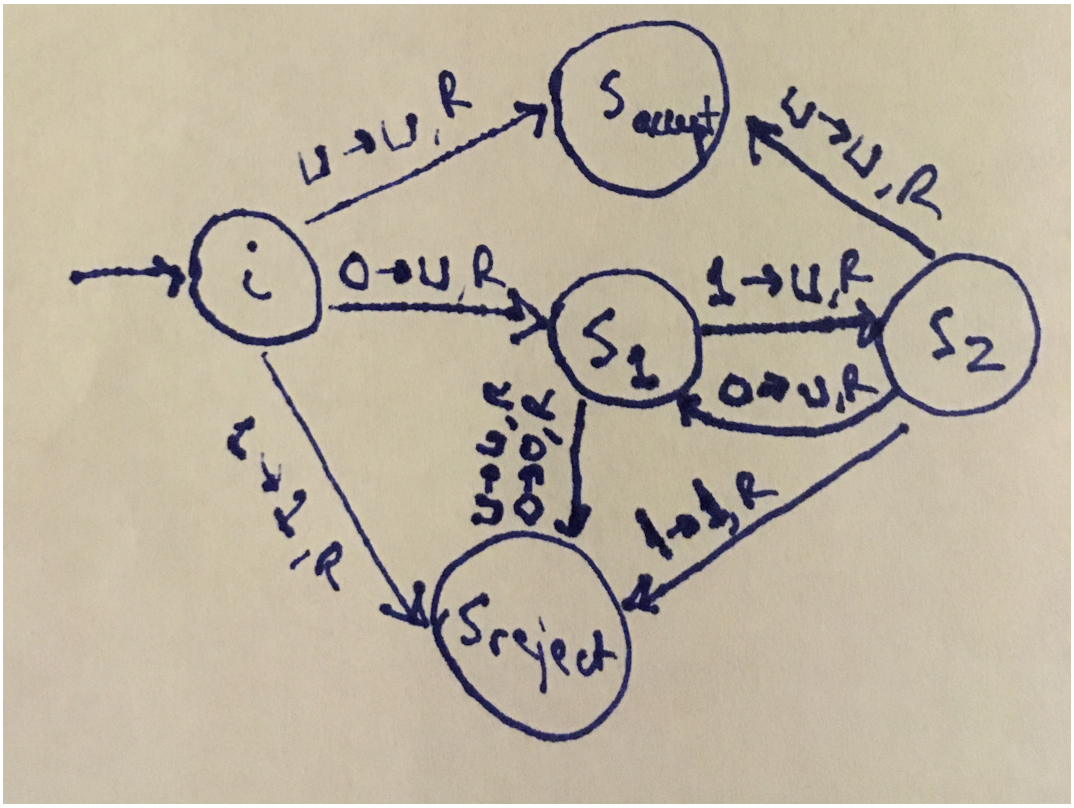
Solution: 1 (a) The finite state acceptor is drawn below:



(b)

(1) If ␣ is in the current cell, then ACCEPT. If 1 is in the current cell, then REJECT. If 0 is in the current cell, then erase 0 and move right.
(2) If ␣ or 0 is in the current cell, then REJECT. If 1 is in the current cell, then erase 1 and move right.
(3) Go to step 1.

(c) See the diagram below. The Turing machine is an elaboration of the finite state acceptor with more complicated transitions ('character $\rightarrow$ character, direction' instead of just 'character'), separate transitions for ␣, and separate accept and reject states as opposed to having all states of the finite state acceptor be either accepting or rejecting states.



2) Note that $L = \{3m : m \in \mathbb{N}\} = \{m \equiv 0 \mod 3 : m \in \mathbb{N}\}$.

We can tell if a number is divisible by three by just examining its digits. We will use modular arithmetic heavily - recall the Michaelmas lectures and tutorials!

Note that for all $n \in \mathbb{N}, n \geq 1$, $10^n \equiv 1 \mod 3$ (also written $10^n \equiv_3 1$).

Consider 279. Is this divisible by 3?

$$279 = 200 + 70 + 9 = 2 \cdot 100 + 7 \cdot 10 + 9 \equiv_3 2 \cdot 1 + 7 \cdot 1 + 9.$$

To determine if 279 is divisible by 3, we just need to determine the conjugacy classes of its digits:

$$2 \equiv_3 2, 7 \equiv_3 1, 9 \equiv_3 0 \quad \rightarrow \quad 2 + 7 + 9 \equiv_3 2 + 1 + 0 \equiv_3 3 \equiv_3 0.$$

Therefore 279 is indeed divisible by 3. We see to determine this, we need only know the conjugacy classes of the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Our Turing machine will reflect that.

Let $T = (\{s_0, s_1, s_2, s_{\text{rej}}, s_{\text{acc}}\}, A, A, t, s_0, s_{\text{rej}}, s_{\text{acc}}\}$. The states s_0, s_1, s_2 correspond to "congruent to 0, 1, 2 mod 3". Note that we begin in state s_0.

Here is the algorithm:

(1) If there is a blank in the first cell, REJECT. Otherwise move to step 2.
(2) If in state s_0, remain in s_0 if the digit is $0, 3, 6, 9$, then move right and go to step 3. If the digit is $1, 4$ or 7, move to state s_1, move right, and go to step 3. If the digit is $2, 5$ or 8, move to state s_2, move right, and go to step 3.

    If in state s_1, remain in s_1 if the digit is $0, 3, 6, 9$, then move right and go to step 3. If the digit is $1, 4$ or 7, move to state s_2, move right, and go to step 3. If the digit is $2, 5$ or 8, move to state s_0, move right, and go to step 3.

    If in state s_2, remain in s_2 if the digit is $0, 3, 6, 9$, then move right and go to step 3. If the digit is $1, 4$ or 7, move to state s_0, move right, and go to step 3. If the digit is $2, 5$ or 8, move to state s_1, move right, and go to step 3.
(3) Suppose there is a blank cell here. If in s_0, ACCEPT, otherwise, REJECT.

    If the cell is not blank, move right and go to step 4.
(4) Move left and go to step 2. Do not change the contents of the current cell.[1]

Note that this is indeed a **decider** as there are no loops.

Here is how the following strings are treated:

[1]If we allow our Turing machine the option to 'stay in place' after reading the contents of a cell, this step is not needed.

- Begin in s_0. Read 0, remain in s_0. ACCEPT.
- Begin in s_0. Read 1, move to s_1. REJECT.
- Begin in s_0. Read 5, move to s_2. REJECT.
- Begin in s_0. Read 9, remain in s_0. ACCEPT.
- For the purposes of our example, suppose the input is 279. The configurations are as follows:

$$\epsilon s_0 279 \to 2 s_2 79 \to 27 s_0 9 \to 279 s_0 \to \text{ACCEPT}.$$

This answer is technically correct, but maybe difficult to think up of in an exam. Another solution is an algorithm for a two-tape Turing machine as follows:

(1) The input is on the first tape (T1), and 0 is on the second tape (T2) initially.
(2) If the number on T2 is equal to the number on T1, ACCEPT. If the number on T2 is bigger than the number on T1, REJECT. If the number on T2 is smaller than the number on T1, add 3 to the number on T2 and write the result on T2.
(3) Go to step 2.

Here we might need to write as a subroutine the process via which a Turing machine 'understands' what the number on a tape is - how a sequence of cells like $\|5\|0\|1\|$ becomes the number 501 in the machine.

MAU22C00: TUTORIAL 22 PROBLEMS
TURING MACHINES

1) Recall the Turing machine constructed in lecture that decides the language $L = \{0^m 1^m \mid m \in \mathbb{N}, m \geq 1\}$. For input string 0011, write down each configuration in turn starting with the initial configuration of the Turing machine and ending with the accepting configuration.

2) (Annual Exam 2020) Let L_1 and L_2 be two Turing-recognisable languages over the same finite alphabet A. Construct an enumerator that outputs $L_1 \cap L_2$.

3) Recall Hilbert's 10th Problem from lecture. What is the size of D_1? Finite, countably infinite or uncountably infinite? Remember that each polynomial in D_1 has integer coefficients.

4) (Annual Exam 2020) In lecture, we defined the language

$$E_{DFA} = \{\langle B \rangle \mid B \text{ is a DFA and } L(B) = \emptyset\}$$

when we examined whether the emptiness testing problem for deterministic finite state acceptors was a Turing-decidable language. Is E_{DFA} finite, countably infinite, or uncountably infinite? Justify your answer.

MAU22C00: TUTORIAL 22 SOLUTIONS
TURING MACHINES

1) Recall the Turing machine constructed in lecture that decides the language $L = \{0^m 1^m \mid m \in \mathbb{N}, m \geq 1\}$. For input string 0011, write down each configuration in turn starting with the initial configuration of the Turing machine and ending with the accepting configuration.

2) (Annual Exam 2020) Let L_1 and L_2 be two Turing-recognisable languages over the same finite alphabet A. Construct an enumerator that outputs $L_1 \cap L_2$.

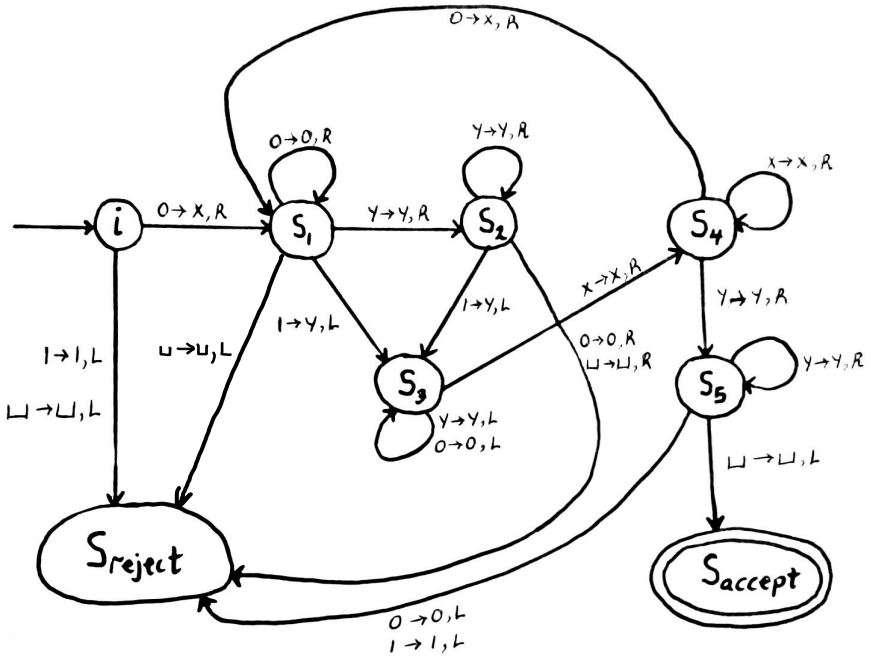
3) Recall Hilbert's 10th Problem from lecture. What is the size of D_1? Finite, countably infinite or uncountably infinite? Remember that each polynomial in D_1 has integer coefficients.

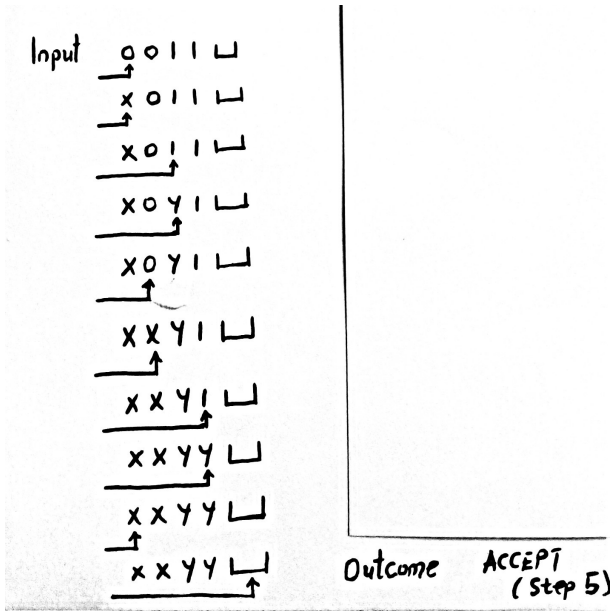
4) (Annual Exam 2020) In lecture, we defined the language

$$E_{DFA} = \{\langle B \rangle \mid B \text{ is a DFA and } L(B) = \emptyset\}$$

when we examined whether the emptiness testing problem for deterministic finite state acceptors was a Turing-decidable language. Is E_{DFA} finite, countably infinite, or uncountably infinite? Justify your answer.

Solution: 1) Recall from lecture the transition diagram of the Turing machine that decides the language $L = \{0^m 1^m \mid m \in \mathbb{N}, m \geq 1\}$:





Here is how input string 0011 is processed: Correspondingly, we have the following configurations: $\epsilon i0011$, xS_1011, $x0S_111$, xS_30y1, ϵS_3x0y1, xS_40y1, xxS_1y1, $xxyS_21$, xxS_3yy, xS_3xyy, xxS_4yy, $xxyS_5y$, $xxyyS_5\epsilon$, and finally $xxyS_{accept}y$. Note that the diagram showing how 0011 is processed skips some steps showing how we

move to get to the next character we wish to process, whereas the list of configurations exactly traces what the Turing machine does including which states it enters. Each configuration in the list yields the next one, and going from one to the other is given by a transition that is marked on the transition diagram of the Turing machine.

2) Let M be a Turing machine that recognises L_1, and let N be a Turing machine that recognises L_2. A^* has an enumeration as a sequence

$$A^* = \{w_1, w_2, \dots\}.$$

We construct our enumerator that outputs $L_1 \cap L_2$ as follows:

$E =$ Ignore the input

1. Repeat the following for $i = 1, 2, 3, \dots$
2. Run M for i steps on each input $w_1, w_2, \dots, w_i$.
3. If any computations accept, run N for i steps on the corresponding w_j.
3. Print out every w_j that N accepts.

Note that we need to run M and N for only i steps because either of these Turing machines could loop if we do not specify a number of steps. Each w_j that is printed out has been accepted by both M and N, which means it belongs to $L_1 \cap L_2$.

3) Recall that D_1 is given by

$$D_1 = \{p(x) \mid \exists x \in \mathbb{Z} \text{ such that } p(x) = 0\},$$

where each $p(x)$ has integer coefficients. Note that $p(x)$ could have any degree as long as that degree is at least 1 (polynomials of degree zero are by definition constant polynomials, so they cannot have a root, hence we exclude them). Before we worry about how many of these polynomials have roots in $\mathbb{Z}$, let us first figure out what is the size of the set of polynomials $p(x)$ of degree at least 1 with integer coefficients. Let us call this set B. Let B_d be the set of polynomials $p(x)$ of degree d with integer coefficients. Since the degree of the polynomials in the set B is at least 1, we can represent B as the union

$$B = \bigcup_{d=1}^{\infty} B_d.$$

Note that $B_d \cap B_{d'} = \emptyset$ if $d \neq d'$ because if a polynomial has degree d, it cannot have degree d' if $d \neq d'$. Therefore, B is the union of the disjoint sets B_d. Let us now figure out the size of each B_d. Let $p(x) \in B_d$. Since $p(x)$ has degree d, it can be written as $p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$, where $a_d \neq 0$. Note that we can put each element $p(x)$ of B_d in

bijective correspondence with the $(d+1)$-tuple $(a_d, a_{d-1}, \ldots, a_1, a_0)$ of its coefficients. Therefore, $B_d \sim \{(a_d, a_{d-1}, \ldots, a_1, a_0) \in \mathbb{Z}^{n+1} \mid a_d \neq 0\}$ since all coefficients of $p(x)$ must be integers, hence in $\mathbb{Z}$.

$$\{(a_d, a_{d-1}, \ldots, a_1, a_0) \in \mathbb{Z}^{n+1} \mid a_d \neq 0\} = (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^n$$

because $a_d \neq 0$, so $a_d \in \mathbb{Z} \setminus \{0\}$. Therefore, $B_d \sim (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^n$. We proved in lecture that $\mathbb{Z}$ is countably infinite. When we take away one element, namely 0, it stays countably infinite, so $\mathbb{Z} \setminus \{0\}$ is countably infinite. Thus, $(\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^n$ is a Cartesian product of finitely many countably infinite sets. We conclude that $(\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^n$ must be countably infinite, hence B_d must be countably infinite as it is in bijective correspondence with it. We conclude that B as the countably infinite disjoint union

$$B = \bigcup_{d=1}^{\infty} B_d$$

of countably infinite sets, B_d must itself be countably infinite by a theorem proven in the unit on countability of sets. Note that $D_1 \subset B$, so the set we are interested in, D_1, is a subset of a countably infinite set. Therefore, D_1 could be finite or countably infinite. We will prove that D_1 is countably infinite by showing it contains a sequence, namely a countably infinite subset. D_1 consists of all polynomials $p(x)$ of degree at least 1 with integer coefficients that have at least one integer root. Define $p_i(x) = x - i$. Therefore $p_1(x) = x - 1$, $p_2(x) = x - 2$, etc. Clearly, each p_i has root $i \in \mathbb{N} \subset \mathbb{Z}$, so $p_i(x) \in D_1$. The polynomials $p_i(x)$ for $i \geq 1$ form a sequence $\{p_1(x), p_2(x), p_3(x), \ldots\}$, and $\{p_1(x), p_2(x), p_3(x), \ldots\} \subset D_1$.Therefore, D_1 is countably infinite. Note this argument was a sandwich argument as we showed

$$\{p_1(x), p_2(x), p_3(x), \ldots\} \subset D_1 \subset B,$$

with $\{p_1(x), p_2(x), p_3(x), \ldots\}$ and B both countably infinite. Note also that D_n is likewise countably infinite. The argument is fundamentally the same as the one given for D_1, but we have to account for the fact that $p(x_1, \ldots, x_n)$ has monomials in terms of the n variables $x_1, \ldots, x_n$, so writing out its coefficients requires the use of the multi-index notation.

4) The language

$$E_{DFA} = \{\langle B \rangle \mid B \text{ is a DFA and } L(B) = \emptyset\}$$

consists of two conditions:

- B is a DFA.
- $L(B) = \emptyset$.

Let C be the set of all DFA's that accept languages over a given finite alphabet A. We first need to figure out the size of C. Recall from the unit on formal languages and grammars that a language L is regular $\Leftrightarrow$ L is accepted by a DFA. As proven in lecture, the set of regular languages is countably infinite, so C must also be countably infinite. Clearly, $E_{DFA} \subsetneq C$ as the condition $L(B) = \emptyset$ shrinks the size of the set. E_{DFA} is thus a subset of a countably infinite set, so it could be finite or countably infinite. Note that for any $m \in \mathbb{N}^*$, we can construct a DFA B with m non-accepting states ensuring that $L(B) = \emptyset$. Since $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ is a countably infinite set with an element taken out hence still countably infinite, we have shown E_{DFA} has a countably infinite subset. We conclude that E_{DFA} must be countably infinite. Once again, this was a sandwich argument.

MA2C03: PROBLEM SHEET

1) (From the 2016-2017 Annual Exam) Let Q denote the relation on the set $\mathbb{Z}$ of integers, where integers x and y satisfy xQy if and only if

$$x - y = (x - y)(x + 2y).$$

Determine the following:

(i) Whether or not the relation R is *reflexive*;
(ii) Whether or not the relation R is *symmetric*;
(iii) Whether or not the relation R is *transitive*;
(iv) Whether or not the relation R is an *equivalence relation*;
(v) Whether or not the relation R is *anti-symmetric*;
(vi) Whether or not the relation R is a *partial order*.

Justify your answers.

Solution: $x, y \in \mathbb{Z}$ satisfy xRy iff $x - y = (x - y)(x + 2y)$, which is equivalent to $(x - y)(x + 2y - 1) = 0$, i.e., $x = y$ or $x + 2y - 1 = 0$.

(i) **Reflexivity:** The relation R is reflexive because xRx holds for all $x \in \mathbb{Z}$ as $x - x = (x - x)(x + 2x) = 0$.

(ii) **Symmetry:** The relation R is not symmetric because if $x \neq y$, then xRy holds if $x + 2y = 1$, thus for yRx we would need $y + 2x = 1$, which only holds at the same time with $x+2y = 1$ when $x = y = \dfrac{1}{3} \notin \mathbb{Z}$.

(iii) **Anti-symmetry:** The relation R is anti-symmetric. Having xRy and yRx when $x \neq y$ would imply $x + 2y = 1$ and $y + 2x = 1$ hold simultaneously, which gives $x = y = \dfrac{1}{3} \notin \mathbb{Z}$. Therefore, xRy and yRx can both be true only if $x = y$.

(iv) **Transitivity:** The relation R is not transitive. Assume xRy and yRz hold for $x, y, z \in \mathbb{Z}$. There are 4 cases to consider:

Case 1: $x = y$ and $y = z$, then $x = z$, so xRz as needed.

Case 2: $x = y$ and $y + 2z = 1$, then $x + 2z = 1$, so xRz as needed.

Case 3: $x + 2y = 1$ and $y = z$, then $x + 2z = 1$, so xRz as needed.

Case 4: $x + 2y = 1$ and $y + 2z = 1$, then $x + 2(1 - 2z) = 1$, so $x + 2 - 4z = 1$, i.e., $x - 4z = -1$. This last equation is satisfied for example for $x = 3$, $z = 1$. Take $y = -1$ in order to satisfy $x + 2y = 1$. We see that $x + 2z = 3 + 2 = 5 \neq 1$, so xRz fails. We have constructed a counterexample.

(v) **Equivalence relation:** The relation R is not an equivalence relation because while reflexive, it fails to be symmetric and transitive.

(vi) **Partial order:** The relation R is not a partial order because while reflexive and anti-symmetric, it fails to be transitive.

2) (From the 2016-2017 Annual Exam) Let $f : [-2, 2] \to [-15, 1]$ be the function defined by $f(x) = x^2 + 3x - 10$ for all $x \in [-2, 2]$. Determine whether or not this function is injective and whether or not it is surjective. Justify your answers.

Injectivity: $f(x) = x^2 + 3x - 10 = (x - 2)(x - 5)$ This function is not injective on the interval $[-2, 2]$. Acceptable justifications: drawing the graph, providing two values $x_1, x_2 \in [-2, 2]$, $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$, applying Rolle's theorem (noticing that $f'(x) = 2x + 3$ so $f'\left(-\frac{3}{2}\right) = 0$, and $\frac{3}{2} \in [-2, 2]$), etc.

Surjectivity: $f(x) = x^2 + 3x - 10$ is not surjective on the interval $[-2, 2]$. Acceptable justifications: drawing the graph, providing a value in $[-15, 1]$ that $f(x)$ does not assume, showing the minimum value occurs at $\frac{3}{2}$, where $f\left(\frac{3}{2}\right) = -12.25 > -15$, etc.

3) Let $A = \{3^p \mid p \in \mathbb{N}\}$ with the operation of multiplication.

(a) Is $(A, \cdot)$ a semigroup? Justify your answer.
(b) Is $(A, \cdot)$ a monoid? Justify your answer.
(c) Is $(A, \cdot)$ a group? Justify your answer.

Solution: (a) Yes, $(A, \cdot)$ is a semi-group. $A \subset \mathbb{Q}^*$, and $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ is a monoid under the operation of multiplication. We proved in lecture that if $a \in M$ for M a monoid with operation $*$ and $m, n \in \mathbb{N}$, then $a^m * a^n = a^{m+n}$. Here $a = 3$ and since addition is a binary operation on $\mathbb{N}$ as we showed in class, multiplication is a binary operation on A. The associativity of multiplication on A follows from the associativity of addition on $\mathbb{N}$ and the theorem that if $a \in M$ for M a monoid with operation $*$ and $m, n \in \mathbb{N}$, then $a^m * a^n = a^{m+n}$.

(b) Yes, $(A, \cdot)$ is a monoid. $3^0 = 1$ is the identity element on A because any $b \in A$ is of the form 3^p, so $b \cdot 1 = a^p \cdot a^0 = a^{p+0} = a^{0+p} = 1 \cdot b = a^p = b$.

(c) No, $(A, \cdot)$ is not a group. By the theorem on powers we proved in lecture, 3^{-p} would have to be the inverse of 3^p for $p \in \mathbb{N}$ because $3^{-p} \cdot 3^p = 3^p \cdot 3^{-p} = 3^{p-p} = 3^0 = 1$, but if $p \in \mathbb{N}$, then $p \geq 0$, so $-p \notin \mathbb{N}$

when p is negative. So if $p < 0$, $3^{-p} \notin A$. Therefore, the only invertible element in A is the identity element $3^0 = 1$.

4) (Slightly modified question from the annual exam 2017-2018) Let $A = \{(x, y) \in \mathbb{R}^2 \mid x + 2y = 0\}$ with the operation of addition given by

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

(a) Is $(A, +)$ a semigroup? Justify your answer.
(b) Is $(A, +)$ a monoid? Justify your answer.
(c) Is $(A, +)$ a group? Justify your answer.
(d) What geometric object is the set A in $\mathbb{R}^2$?

Solution: (a) Yes, $(A, +)$ is a semi-group. If $x_1 = -2y_1$ and $x_2 = -2y_2$, then $x_1 + x_2 = -2y_1 - 2y_2 = -2(y_1 + y_2)$, so $+$ is a binary operation on A. We proved in lecture that addition is an associative binary operation on $\mathbb{R}$, so $+$ is associative on A as associativity will function component by component in the vector (x, y).

(b) Yes, $(A, +)$ is a monoid. $(0, 0)$ is the identity element on A because for any $(x, y) \in A$,

$$(x, y) + (0, 0) = (x + 0, y + 0) = (0 + x, 0 + y) = (0, 0) + (x, y) = (x, y).$$

(c) Yes, $(A, +)$ is a group. For any $(x, y) \in A$, $(-x, -y)$ is its inverse because $(x, y) + (-x, -y) = (-x, -y) + (x, y) = (0, 0)$. Therefore, all elements of A are invertible.

(d) A is the line passing through the origin $(0, 0)$ and the point $(2, -1)$ as $2 + 2(-1) = 0$.

5) Let A be a finite set, and let A^* be the set of all words over the alphabet A. Consider $(A^*, \circ, \epsilon)$ with the operation of concatenation and empty word ϵ as the identity element. Let $(\mathbb{N}, +, 0)$ be the set of natural numbers with the operation of addition and 0 as the identity element. Let $f : A^* \to \mathbb{N}$ be the function that assigns to each word $w \in A^*$ its length, $f(w) = |w| \in \mathbb{N}$.

(a) What type of object is $(A^*, \circ, \epsilon)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(\mathbb{N}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) $\circ$ is an associative binary operation as we proved in lecture, so $(A^*, \circ, \epsilon)$ is definitely a semigroup. As we showed in lecture,

ϵ is the identity element for $\circ$ on A^*, which means $(A^*, \circ, \epsilon)$ is a monoid. We discussed in lecture during the abstract algebra unit that ϵ is the only invertible element in A^*, so $(A^*, \circ, \epsilon)$ cannot be a group.

(b) Addition is an associative binary operation as we showed in lecture, so $(\mathbb{N}, +, 0)$ is clearly a semigroup. 0 is the identity element for addition on $\mathbb{N}$ which means $(\mathbb{N}, +, 0)$ is a monoid. Note that 0 is the only invertible element in $\mathbb{N}$ so $(\mathbb{N}, +, 0)$ cannot be a group.

(c) To show that f is a homomorphism, we need to show that for any two words $w_1, w_2 \in A^*$, $f(w_1 \circ w_2) = |w_1| + |w_2|$, but we have already showed in lecture that this property holds. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. Now we need to decide whether it is bijective. The function f is clearly surjective because for any length $n \in \mathbb{N}$, we can construct a word in $w \in A^*$, whose length $|w| = n$. Is f injective? Well, the answer depends whether A has one element or several. If $A = \{a\}$ has only one element, there is one and only one word $a \cdots a$ of any given length n, so f is injective. However, if A has more than one element, then there exist letters $a, b \in A$ such that $a \neq b$. Then the words ab and ba that are distinct have the same length 2, which means f cannot be injective, so it is not an isomorphism.

6) Let $(\mathbb{Z}, +, 0)$ be the set of integers with the operation of addition and 0 as the identity element. Let E be the set of even integers, $E = \{2p \mid p \in \mathbb{Z}\}$. Consider $(E, +, 0)$ the set of even integers with the operation of addition and 0 as the identity element. Let $f : \mathbb{Z} \to E$ be the function $f(n) = 2n$.

(a) What type of object is $(\mathbb{Z}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(E+, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) Addition on $\mathbb{R}$ hence on $\mathbb{Z}$ is an associative binary operation as we discussed in lecture. Therefore, $(\mathbb{Z}, +, 0)$ is a semigroup. 0 is the identity element for addition on $\mathbb{Z}$ as for any $n \in \mathbb{Z}$, $n + 0 = 0 + n = n$, so $(\mathbb{Z}, +, 0)$ is a monoid. Given any $n \in \mathbb{Z}$, $-n$ is its inverse as $n + (-n) = n - n = 0$, so every element of $(\mathbb{Z}, +, 0)$ is invertible. Therefore, $(\mathbb{Z}, +, 0)$ is a group.

(b) $E \subset \mathbb{Z}$. Since addition is associative on $\mathbb{Z}$, it is also associative on E. We do, however, have to prove it is a binary operation, i.e. closed. Consider $m, n \in E$. Thus, there exist $p, s \in \mathbb{Z}$ such that $m = 2p$ and $n = 2s$ by the definition of E. Then $m + n = 2p + 2s = 2(p + s)$. Since addition is a binary operation on $\mathbb{Z}$ hence closed, it follows

$$p, s \in \mathbb{Z} \implies p + s \in \mathbb{Z}.$$

Thus, $m + n \in E$, and addition is indeed closed on E. We conclude $(E+, 0)$ is a semigroup. Since $E \subset \mathbb{Z}$, the fact that 0 is the identity element for addition on $\mathbb{Z}$ carries over to E, so E has 0 as its identity element. Therefore, $(E+, 0)$ is a monoid. Now let $n \in E$. We know from part (a) that $-n \in \mathbb{Z}$ is the inverse of n under addition. We just have to prove $-n \in E$. Since $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p$. Therefore, $-n = -2p = 2(-p)$, so $-n \in E$ as needed, which means every element in E is invertible. Therefore, $(E+, 0)$ is a group.

(c) To show that f is a homomorphism, we need to show that for any two integers $p, s \in \mathbb{Z}$, $f(p + s) = f(p) + f(s)$. We apply the definition of f as follows: $f(p) + f(s) = 2p + 2s = 2(p + s) = f(p + s)$. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. We need to figure out whether it is bijective. The function f is clearly surjective by the definition of E because for every $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p = f(p)$. To show injectivity, assume there exist $p, s \in \mathbb{Z}$ such that $f(p) = f(s)$. Then by the definition of f, $2p = 2s \iff p = s$. Therefore, f is indeed injective. We have shown f is bijective hence an isomorphism from $(\mathbb{Z}, +, 0)$ to $(E, +, 0)$.

7) Describe the formal language over the alphabet $\{a, b, c\}$ generated by the context-free grammar whose only non-terminal is $\langle S \rangle$, whose start symbol is $\langle S \rangle$, and whose production rules are the following:

(1) $\langle S \rangle \to b$
(2) $\langle S \rangle \to c$
(3) $\langle S \rangle \to a\langle S \rangle$

In other words, describe the structure of the strings generated by this grammar.

Solution: This context-free grammar produces strings of the type $a^m b$ or $a^m c$ for $m \geq 0$.

8) Let L be the language over the alphabet $\{0, 1\}$ consisting of all words where the string 00 occurs as a substring. Prove from the definition of a regular language that the language L is regular.

Solution: Let the alphabet $A = \{0, 1\}$. Recall that the definition of a regular language allows for finite subsets of A^*, the Kleene star, concatenations, and unions. Note that

$$L = \{w \in A^* \mid w = u \circ 00 \circ v \quad u, v \in A^*\}.$$

Therefore, we can let $L_1 = \{00\}$ be the language consisting of just the string 00 of interest. L_1 is a finite set, so it is allowed in the definition of a regular language. Let $L_2 = \{0, 1\}$. L_2 is finite, hence likewise allowed. Let $L_3 = L_2^*$, the Kleene star applied to L_2. The language $L_3 = A^*$, i.e. it is the set of all words that can be formed over the alphabet $A = \{0, 1\}$. Set $L_4 = L_3 \circ L_1$, and then $L_5 = L_4 \circ L_3$. Note that the words in L_5 have exactly the structure of the words in L, and in fact, $L = L_5$. Note also that the solution here is by no means unique. No two of you will necessarily have arrived at the same exact expression, order or labelling of the intermediate languages L_i that come into the definition of a regular language as applied to L.

9) Let L be the language over the alphabet $\{0, 1\}$ consisting of all words where the string 00 occurs as a substring.

(a) Draw a finite state acceptor that accepts the language L. Carefully label all the states including the starting state and the finishing states as well as all the transitions. Make sure you justify it accepts all strings in the language L and no others.
(b) Write down the transition mapping of the finite state acceptor you drew in the previous part of the problem.
(c) Devise a regular grammar in normal form that generates the language L. Be sure to specify the start symbol, the non-terminals, and all the production rules.
(d) Write down a regular expression that gives the language L and justify your answer.

Solution: (a) See diagram of finite state acceptor on the next page.

We can use three states $\{i, A, B\}$, where i is the initial state. Since we must ensure the word contains the string 00, when 1 is the input, we stay in the initial state i. For input 0, we move to a new state A. A is not an accepting state as we have so far only half of the string 00, the first zero. If we get input 1, we have to restart the process of capturing the string 00, so we get back to the initial state i. If we get input 0, then we will have received the second zero we want, so we'll move to a

new state B, which is an accepting state. Once we have the substring 00, we don't care what follows, so the transitions for both 0 and 1 out of state B are back into B itself.

(b)

$$\begin{aligned} t(i,0) &= A \qquad & t(i,1) &= i \\ t(A,0) &= B \qquad & t(A,1) &= i \\ t(B,0) &= B \qquad & t(B,1) &= B \end{aligned}$$

(c) We shall use the algorithm discussed in lecture in order to generate the regular grammar in normal form corresponding to the finite state acceptor constructed above. The finite state acceptor had three states $\{i, A, B\}$, where i was the initial state. Correspondingly, we use three non-terminals in our regular grammar: the start symbol $\langle S\rangle$ corresponding to the initial state i, $\langle A\rangle$ corresponding to state A, and $\langle B\rangle$ corresponding to state B. We first write the production rules corresponding to the transitions out of the initial state i :

(1) $\langle S\rangle \to 1\langle S\rangle$.
(2) $\langle S\rangle \to 0\langle A\rangle$.

Next, we write the production rules corresponding to the transitions out of state A :

(3) $\langle A\rangle \to 1\langle S\rangle$.
(4) $\langle A\rangle \to 0\langle B\rangle$.

Finally, we write the production rules corresponding to the transitions out of state B :

(5) $\langle B\rangle \to 1\langle B\rangle$.
(6) $\langle B\rangle \to 0\langle B\rangle$.

Rules (1)-(6) are of type (i). For each accepting state, we will write down a rule of type (iii). Since there is only one accepting state, B, we have only one such rule:

(7) $\langle B\rangle \to \epsilon$.

(d) Recall that

$$L = \{w \in A^* \;\big|\; w = u \circ 00 \circ v \quad u, v \in A^*\}.$$

Therefore, $L = A^* \circ 00 \circ A^*$, and we have obtained the regular expression giving us the language L.

10) (Annual Exam 2017) Consider the language L over the alphabet $A = \{a, l, p\}$ consisting of all words of the form $a^m l^{2m} p^m$ for $m \in \mathbb{N}^*$. Use the Pumping Lemma to show the language L is not regular.

Solution: Assume L is regular. Then it must have a pumping length T. We will now choose a string in terms of T that is particularly easy to analyse in the setting of the Pumping Lemma. Let this string be $w = a^T l^{2T} p^T$. By the Pumping Lemma, we can break w into three components: x, u, and y, with $u \neq \epsilon$ and $|xu| \leq T$.

Note that if $|xu| \leq T$, then xu must consist of a's as the first T characters in w are a's. Also if $u \neq \epsilon$, we must conclude $u = a^k$ for some $k \geq 1$.

Therefore, by the Pumping Lemma, for all n, $xu^n y \in L$. By choosing $n = 2$, however, we obtain a string $xu^2y = a^q l^{2T} p^T$ with $q > T$. This string cannot be in L. We thus have obtained the needed contradiction showing that the language L cannot be regular.

11) Let M be the language

$$\{0101,\ 001001,\ 00010001,\ 0000100001,\ \dots\}$$

whose words consist of some positive number n of occurrences of the digit 0, followed by the digit 1, followed by n further occurrences of the digit 0, and followed by the digit 1. (In particular, the number of occurrences of 0 preceding the first 1 is equal to the number of occurrences of 0 preceding the second 1.)

(a) Use the Pumping Lemma to show this language is not regular.
(b) Write down the production rules of a context-free grammar that generates exactly M. Justify your answer.

Solution: (a) If M is regular, then it has a pumping length p. Consider $w = 0^p 10^p 1 \in M$ and the decomposition $w = xuy$ with $|u| \geq 1$ and $|xu| \leq p$. Since $|xu| \leq p$, u can only consist of zeroes. Let $u = 0^{n_1}$, for some $n_1 \geq 1$. Clearly, $xu^2y \notin M$ as $xu^2y = 0^{p+n_1}10^p1$, so the length of the first sequence of zeroes is greater than that of the second sequence of zeroes violating the pattern of the language.

(b) Consider the following production rules:

(1) $\langle S\rangle \to 0\langle A\rangle 01$,
(2) $\langle A\rangle \to 0\langle A\rangle 0$,
(3) $\langle A\rangle \to 1$.

We can show by induction that a string w generated by these production rules is of is of one of the following forms:

- $w = \langle S\rangle$,
- $w = 0^n\langle A\rangle 0^n 1$,
- $w = 0^n 10^n 1$.

Here $n \geq 1$. These rules will then generate exactly M. Note how these rules differ from the production rules of a regular grammar as non-terminals occur on both sides of the non-terminal in the first two production rules.

12) Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae.

(a) Draw this graph. Write down its incidence table and its incidence matrix.
(b) Write down this graph's adjacency table and its adjacency matrix.
(c) Is this graph complete? Justify your answer.
(d) Is this graph bipartite? Justify your answer.
(e) Is this graph regular? Justify your answer.
(f) Does this graph have any regular subgraph? Justify your answer.
(g) Give an example of an isomorphism from the graph (V, E) specified at the beginning of this problem to the graph (V', E') with vertices p, q, r, s, and t, and edges pq, ps, rt, st, rs, and rq.

Solution: Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae.

(a) The graph is drawn at the end of the solutions. If we keep the same order of the vertices and edges given in the statement of the problem, the incidence table is:

	ab	bd	be	ac	cd	ae
a	1	0	0	1	0	1
b	1	1	1	0	0	0
c	0	0	0	1	1	0
d	0	1	0	0	1	0
e	0	0	1	0	0	1

The corresponding incidence matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b) If we keep the same order of the vertices given in the statement of the problem, the adjacency table is:

	a	b	c	d	e
a	0	1	1	0	1
b	1	0	0	1	1
c	1	0	0	1	0
d	0	1	1	0	0
e	1	1	0	0	0

The corresponding adjacency matrix is

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

(c) No, as for example edge bc does not belong to the graph, so not every vertex is connected to every other vertex.

(d) No, as the graph contains the complete subgraph $V' = \{a, b, e\}$ and $E' = \{ab, ae, be\}$, which cannot be partitioned.

(e) No, as vertices a and b have degree 3, whereas the other vertices have degree 2.

(f) Any two vertices that have an edge between them taken with that edge form a regular subgraph (1-regular) as do $\{a, b, e\}$ and the edges between them (2-regular) and $\{a, b, c, d\}$ and the edges between them (2-regular).

(g) It does NOT suffice to show the two graphs have the same structure. An isomorphism is a MAP, so you must provide the map on vertices. Two possible isomorphisms are $\varphi(a) = s$, $\varphi(b) = r$, $\varphi(c) = p$, $\varphi(d) = q$, and $\varphi(e) = t$ or the following: $\varphi(a) = r$, $\varphi(b) = s$, $\varphi(c) = q$, $\varphi(d) = p$, and $\varphi(e) = t$.

13) Let (V, E) be the graph with vertices a, b, c, d, and e and edges ab, bd, be, ac, cd, and ae. Does this graph have a Hamiltonian circuit? Justify your answer.

14) For what type of n does the complete graph K_n have an Eulerian circuit? Justify your answer.

15) For what type of n does the complete graph K_n have an Eulerian trail? Justify your answer.

16) For what type of n does the complete graph K_n have a Hamiltonian circuit? Justify your answer.

17) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian circuit? Justify your answer.

18) For what type of p and q does the complete bipartite graph $K_{p,q}$ have an Eulerian trail? Justify your answer.
19) For what type of p and q does the complete bipartite graph $K_{p,q}$ have a Hamiltonian circuit? Justify your answer.

20) Consider the language over the binary alphabet $A = \{0, 1\}$ given by $L = \{0^m 1^{2m} \mid m \in \mathbb{N}\}$.

(a) Use the Pumping Lemma to show L is not a regular language.

(b) Write down the algorithm of a Turing machine that recognizes L. Process the following strings according to your algorithm: ϵ, 01, 011, and 010.

(c) Write down the transition diagram of the Turing machine from part (a) carefully labelling the initial state, the accept state, the reject state, and all the transitions specified in your algorithm.

(d) Is the language L finite, countably infinite, or uncountably infinite? Justify your answer.

Solution: (a) If L is a regular language, then it has a pumping length p. In order to consider just one case, we work with $w = 0^p 1^{2p} \in L$. According to the Pumping Lemma, w is to be decomposed as xuy, where $|u| \geq 1$ and $|xu| \leq p$. Since $|xu| \leq p$, u can only consist of zeroes. Let $u = 0^{n_1}$, for some $n_1 \geq 1$. Clearly, $xu^2y \notin L$ as $xu^2y = 0^{p+n_1}1^{2p}$, so the length of the first sequence of zeroes is not one half that of the second sequence of zeroes violating the pattern of the language.

(b) Here is the algorithm for recognising $L = \{0^m 1^{2m} : m \in \mathbb{N}\}$.

(1) If there is a blank in the first cell, ACCEPT. If there is anything else, apart from 0, then REJECT.
(2) If 0 is in the current cell, delete it, then move right to the first 1.
(3) If there is no first 1, REJECT. Otherwise change 1 to x.
(4) Move to the leftmost non blank symbol. If 0, go to step 2. If 1, REJECT. If x, go to step 5. If y, go to step 6.
(5) Delete x, move right to the nearest 1. If none, REJECT. Otherwise change it to y and go to step 4.
(6) Move right to the rightmost non blank character. If anything but y is found, REJECT. Otherwise, ACCEPT.

Here is how the following strings are treated:

- ϵ is accepted immediately.
- $01 \to \sqcup 1 \to \sqcup x \to \sqcup\sqcup \to$ REJECT.

- $011 \to \sqcup 11 \to \sqcup x1 \to \sqcup\sqcup 1 \to \sqcup\sqcup y \to$ ACCEPT.
- $010 \to \sqcup 10 \to \sqcup x0 \to \sqcup\sqcup 0 \to$ REJECT.

(c) The transition diagram for

$$T = (\{i, s_1, s_2, s_3, s_4, s_5, s_{\text{acc}}, s_{\text{rej}}\}, \{0, 1\}, \{0, 1, x, y, \sqcup\}, t, i, s_{\text{acc}}, s_{\text{rej}})$$

is at the end of the solution set, along with an example of an accepted string.

(d) The language L is countably infinite. Consider the function $f : \mathbb{N} \to L$ given by $f(m) = 0^m 1^{2m}$. It is easy to see that f is both injective and surjective hence bijective. Therefore, L is in one-to-one correspondence with $\mathbb{N}$, hence L is countably infinite.