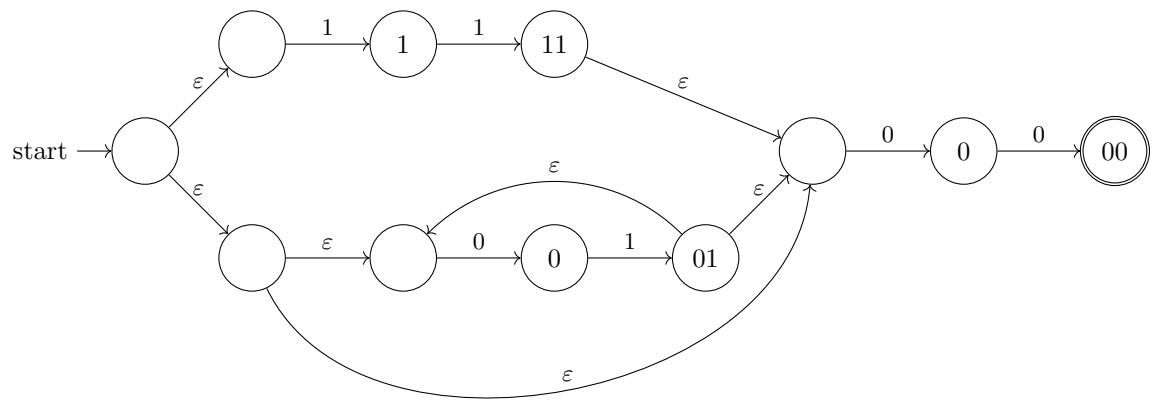
Section 10: Solutions

1. RE to NFA

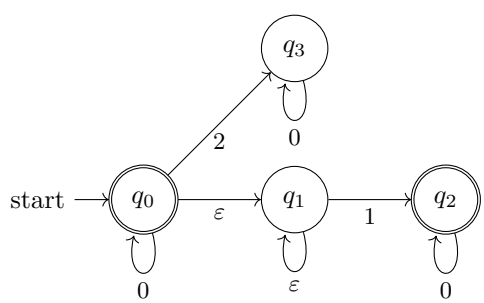
Convert the regular expression "$(11 \cup (01)^*)00$" to an NFA using the algorithm from lecture.

Solution:



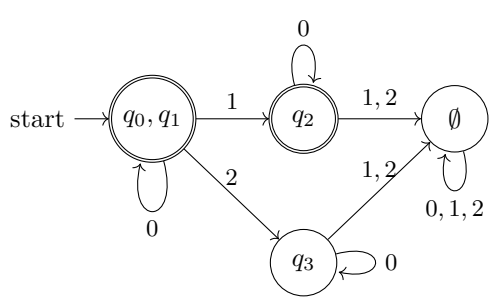
2. NFAs to DFAs

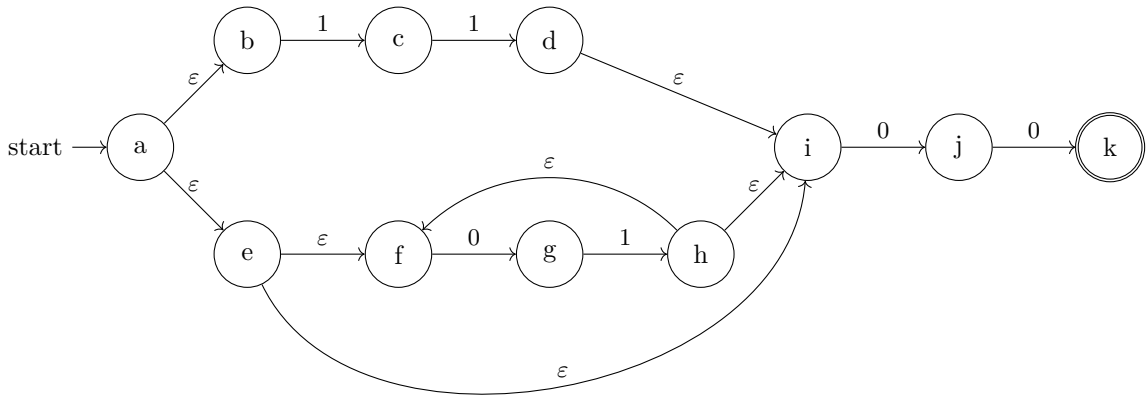
Convert each of the following NFAs to DFAs.



(a)

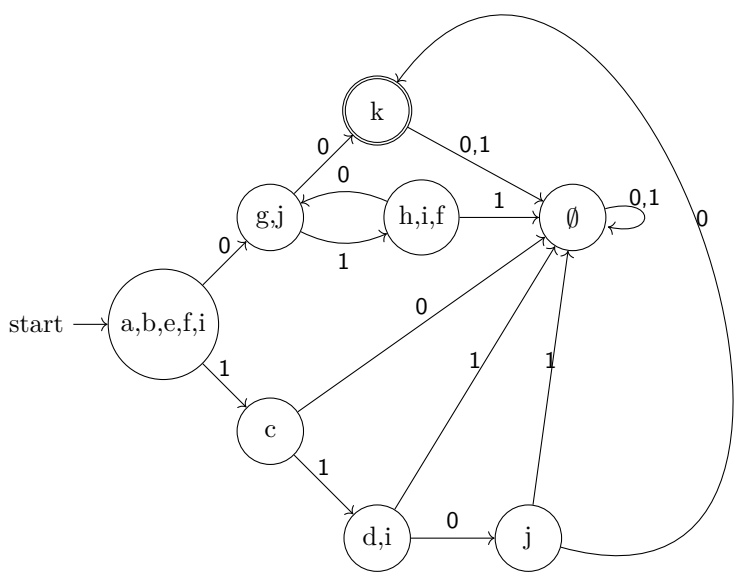
Solution:





(b)

Solution:



3. Irregularity

(a) Let $\Sigma = \{0, 1\}$. Prove that $\{0^n 1^n 0^n \ : \ n \geq 0\}$ is not regular.

Solution:

Let $L = \{0^n 1^n 0^n \ : \ n \geq 0\}$. Let D be an arbitrary DFA, and suppose for contradiction that D accepts L. Consider $S = \{0^n 1^n : n \geq 0\}$. Since S contains infinitely many strings and D has a finite number of states, two strings in S must end up in the same state. These strings are the form $0^i 1^i$ and $0^j 1^j$ for some

$i, j \geq 0$,and we have $i \neq j$ since these are two different strings.

Now, we append the string 0^i to both of these strings. The two resulting strings are:

$a = 0^i 1^i 0^i$ Note that $a \in L$.

$b = 0^j 1^j 0^i$ Note that $b \notin L$, since $i \neq j$.

Since a and b end up in the same state, D must either accept both strings or reject both strings. However, since $a \in L$ and $b \notin L$, it must give the wrong answer for one string, which contradicts that it accepts L. Thus, our only remaining assumption, that D exists, must be false.

Since D was arbitrary, there is no DFA that recognizes L, so L is not regular.

(b) Let $\Sigma = \{0, 1, 2\}$. Prove that $\{0^n(12)^m \ : \ n \geq m \geq 0\}$ is not regular.
Solution:

Let $L = \{0^n(12)^m \ : \ n \geq m \geq 0\}$. Let D be an arbitrary DFA, and suppose for contradiction that D accepts L. Consider $S = \{0^n : n \geq 0\}$. Since S contains infinitely many strings and D has a finite number of states, two strings in S must end up in the same state. These strings are of the form 0^i and 0^j for some $i, j \geq 0$, and since they are different strings we must have $i \neq j$.

Suppose first that $i > j$. In that case, we append the string $(12)^i$ to both of these strings. The two resulting strings are:

$a = 0^i(12)^i$ Note that $a \in L$.

$b = 0^j(12)^i$ Note that $b \notin L$, since $i > j$.

Since a and b end up in the same state, D must either accept both strings or reject both strings. However, since $a \in L$ and $b \notin L$, it must give the wrong answer for one string, which contradicts that it accepts L.

Now, suppose that $i < j$. In that case, we append the string $(12)^j$ to both of these strings. Here, we will have $0^i(12)^j \notin L$ and $0^j(12)^j \in L$ but both strings are taken to the same state, so we again get a contradiction.

Since $i \neq j$, we must have either $i > j$ or $i < j$, so we have proven a contradiction by cases. Thus, our only remaining assumption, that D exists, must be false.

Since D was arbitrary, there is no DFA that recognizes L, so L is not regular.

4. Cardinality

(a) You are a pirate. You begin in a square on a 2D grid which is infinite in all directions. In other words, wherever you are, you may move up, down, left, or right. Some single square on the infinite grid has treasure on it. Find a way to ensure you find the treasure in finitely many moves.
Solution:

Explore the square you are currently on. Explore the unexplored perimeter of the explored region until you find the treasure (your path will look a bit like a spiral).

(b) Prove that $\{3x \ : \ x \in \mathbb{N}\}$ is countable.
Solution:

We can enumerate the set as follows:

$$f(0) = 0$$
$$f(1) = 3$$
$$f(2) = 6$$
$$f(i) = 3i$$

Since every natural number appears on the left, and every number in S appears on the right, this enumeration spans both sets, so S is countable.

(c) Prove that the set of irrational numbers is uncountable.
Hint: Use the fact that the rationals are countable and that the reals are uncountable.
Solution:

We first prove that the union of two countable sets is countable. Consider two arbitrary countable sets C_1 and C_2. We can enumerate $C_1 \cup C_2$ by mapping even natural numbers to C_1 and odd natural numbers to C_2.
Now, assume that the set of irrationals is countable. Then the reals would be countable, since the reals are the union of the irrationals (countable by assumption) and the rationals (countable). However, we have already shown that the reals are uncountable, which is a contradiction. Therefore, our assumption that the set of irrationals is countable is false, and the irrationals must be uncountable.

(d) Prove that $\mathcal{P}(\mathbb{N})$ is uncountable.
Solution:

Assume for the sake of contradiction that $\mathcal{P}(\mathbb{N})$ is countable.
This means we can define an enumeration of elements S_i in $\mathcal{P}$.
Let s_i be the binary set representation of S_i in $\mathbb{N}$. For example, for the set $0, 1, 2$, the binary set representation would be $111000\ldots$
We then construct a new subset $X \subset \mathbb{N}$ such that $x[i] = s_i[i]$ (that is, $x[i]$ is 1 if $s_i[i]$ is 0, and $x[i]$ is 0 otherwise).
Note that X is not any of S_i, since it differs from S_i on the ith natural number. However, X still represents a valid subset of the natural numbers, which means our enumeration is incomplete, which is a contradiction. Since the above proof works for any listing of $\mathcal{P}(\mathbb{N})$, *no* listing can be created for $\mathcal{P}(\mathbb{N})$, and therefore $\mathcal{P}(\mathbb{N})$ is uncountable.

5. Countable Unions

(a) Show that $\mathbb{N} \times \mathbb{N}$ is countable.

Hint: How did we show the rationals were countable?

Solution:

We use dovetailing to create a sequence of elements of $\mathbb{N} \times \mathbb{N}$ that includes the entirety of $\mathbb{N} \times \mathbb{N}$.

For a fixed integer $k \geq 2$, consider subset S_k of $\mathbb{N} \times \mathbb{N}$ consisting of the elements (a, b) such that $a + b = k$. There can be at most $k - 1$ such elements because for each value of $a = 1, 2, \ldots, k - 1$, there can only be one possible value for b, namely $k - a$. Thus, if we create a sequence consisting of all the elements of S_2, then S_3, then S_4, etc. because each set is of finite size, any pair $(a, b) \in \mathbb{N} \times \mathbb{N}$ will eventually show up in this sequence in S_{a+b}.

Thus, because we can enumerate the elements of $\mathbb{N} \times \mathbb{N}$, it must be countable.

(b) Show that the countable union of countable sets is countable. That is, given a collection of sets $S_1, S_2, S_2, \ldots$ such that S_i is countable for all $i \in \mathbb{N}$, show that

$$S = S_1 \cup S_2 \cup \cdots = \{x : x \in S_i \text{ for some } i\}$$

is countable.

Hint: Find a way labeling the elements and see if you can apply the previous part to construct an onto function from $\mathbb{N}$ to S.

Solution:

Because each S_i is countable, the elements can be enumerated. Let the elements of S_i be $a_{i,1}, a_{i,2}, a_{i,3}, \ldots$. Next, because $\mathbb{N} \times \mathbb{N}$ is countable, there exists an onto function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Then define the function $g : \mathbb{N} \to S$ as follows. For each $n \in \mathbb{N}$, let $(i_n, j_n) = f(n)$. The define $g(n)$ to be a_{i_n, j_n}.

I claim g is onto. Indeed, let $a_{i,j}$ be an arbitrary element of S. Because f is onto, there exists an n such that $f(n) = (i, j)$. Then $g(n) = a_{i,j}$. This shows g is onto and thus S is countable.

6. Review: Number Theory

Let the domain of discourse be positive integers and let $z = gcd(m, n)$. Consider the following claim:

$$\forall n\ \forall m\ \forall a\ \forall b\ \forall c\ ((a \equiv_m b \wedge a \equiv_n c) \to (b \equiv_z c))$$

(a) Translate the claim into English. **Solution:**

For any positive integers n, m, a, b, and c, if $a \equiv_m b$ and $a \equiv_n c$ then $b \equiv_z c$ where $z = gcd(m, n)$.

(b) Write a formal proof that the claim holds. You may use the following fact:

$$\textbf{Fact: } (gcd(a, b) \mid a) \wedge (gcd(a, b) \mid b)$$

Solution:

1.	$z = gcd(m, n)$	[Given]
2.	Let a, b, c, n and m be arbitrary.	
3.1.	$a \equiv_m b \wedge a \equiv_n c$	[Assumption]
3.2.	$a \equiv_m b$	[Elim $\wedge$: 3.1]
3.3.	$m \mid a - b$	[Def of Congruence: 3.2]
3.4.	$\exists k(a - b = km)$	[Def of Divides: 3.3]
3.5.	$a - b = km$	[Elim $\exists$: 3.4]
3.6.	$a \equiv_n c$	[Elim $\wedge$: 3.1]
3.7.	$n \mid a - c$	[Def of Congruence: 3.6]
3.8.	$\exists j(a - c = jn)$	[Def of Divides: 3.7]
3.9.	$a - c = jn$	[Elim $\exists$: 3.8]
3.10.	$b - c = jn - km$	[Algebra: Subtract 3.5 from 3.9]
3.11.	$(z \mid m) \wedge (z \mid n)$	[Fact 1: 2]
3.12.	$z \mid m$	[Elim $\wedge$: 3.11]
3.13.	$\exists p(m = pz)$	[Def of Divides: 3.12]
3.14.	$m = pz$	[Elim $\exists$: 3.13]
3.15.	$z \mid n$	[Elim $\wedge$: 3.11]
3.16.	$\exists q(n = qz)$	[Def of Divides: 3.15]
3.17.	$n = qz$	[Elim $\exists$: 3.16]
3.18.	$b - c = jqz - kpz = (jq - kp)z$	[Substitute: 3.10, 3.14, 3.17]
3.19.	$\exists r(b - c = rz)$	[Intro $\exists$: 3.18]
3.20.	$z \mid b - c$	[Def of Divides: 3.19]
3.21.	$b \equiv_z c$	[Def of Congruence: 3.20]
3.	$(a \equiv_m b \wedge a \equiv_n c) \rightarrow (b \equiv_z c))$	[Direct Proof]
4.	$\forall n\, \forall m\, \forall a\, \forall b\, \forall c\, ((a \equiv_m b \wedge a \equiv_n c) \rightarrow (b \equiv_z c))$	[Intro $\forall$: 1-3]

(c) Translate your proof to English. **Solution:**

Let n, m, a, b and c be arbitrary positive integers.

Suppose $a \equiv_m b$ and $a \equiv_n c$. By definition of congruence, it follows that $m \mid a - b$ and $n \mid a - c$. By definition of divides, there is some integer k such that $a - b = km$ and some integer j such that $a - c = jn$. Subtracting the first equation from the second, we know that $b - c = jn - km$.

We were given that $z = gcd(m, n)$, and by Fact 1, we know that $z \mid m$ and $z \mid n$ must hold. By definition of divides, it must also hold that $m = pz$ and $n = qz$ for some integers p and q. Substituting these equations for m and n back into our equation for $b - c$, we find that $b - c = jqz - kpz = (jq - kp)z$. Then, since j, q, k and p are integers, $jq - kp$ is also an integer. So, there is an integer r such that $b - c = rz$. By definition, $z \mid b - c$ and so $b \equiv_z c$.

Since n, m, a, b and c were arbitrary, we have proven the desired result.