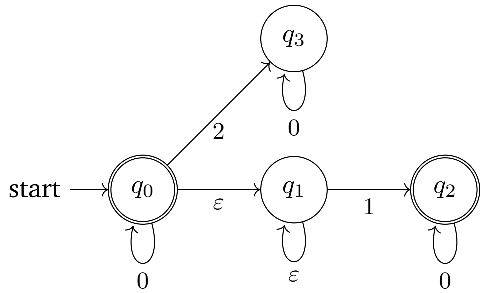
Section 09: Solutions

1. NFAs

(a) What language does the following NFA accept?

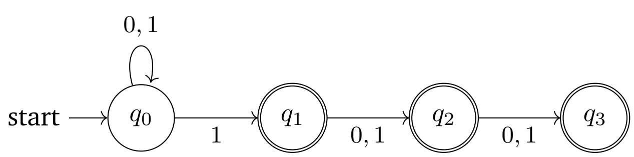


Solution:

All strings of only 0's and 1's not containing more than one 1.

(b) Create an NFA for the language "all binary strings that have a 1 as one of the last three digits".
Solution:

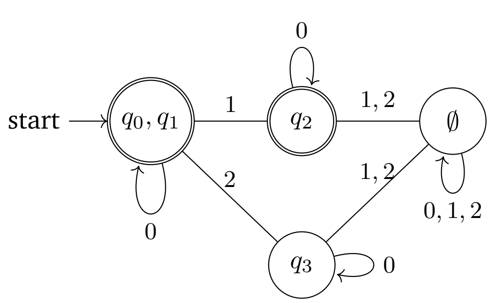
The following is one such NFA:



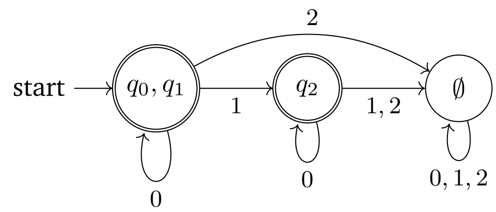
2. DFAs & Minimization

(a) Convert the NFA from 1a to a DFA, then minimize it.

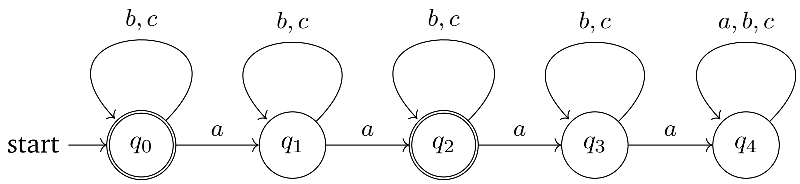
Solution:



Here is the minimized form:



(b) Minimize the following DFA:



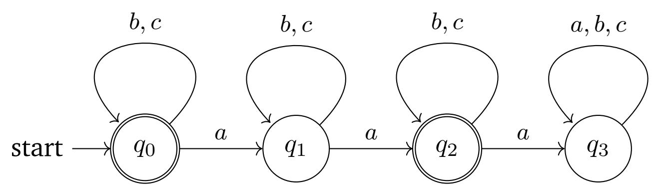
Solution:

Step 1: q_0, q_2 are final states and the rest are not final. So, we start with the initial partition with the following groups: group 1 is $\{q_0, q_2\}$ and group 2 is $\{q_1, q_3, q_4\}$.

Step 2: q_1 is sending a to group 1 while q_3, q_4 are sending a to group 2. So, we divide group 2. We get the following groups: group 1 is $\{q_0, q_2\}$, group 3 is $\{q_1\}$ and group 4 is $\{q_3, q_4\}$.

Step 3: q_0 is sending a to group 3 and q_2 is sending a to group 4. So, we divide group 1. We will have the following groups: group 3 is $\{q_1\}$, group 4 is $\{q_3, q_4\}$, group 5 is $\{q_0\}$ and group 6 is $\{q_2\}$.

The minimized DFA is the following:



3. Review: Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- soy(x) is true iff x contains soy milk.
- whole(x) is true iff x contains whole milk.
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinated.
- vegan(x) is true iff x is vegan.
- RobbieLikes(x) is true iff Robbie likes the drink x.

Translate each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like $=$ and $\neq$.

(a) Coffee drinks with whole milk are not vegan. **Solution:**

$\forall x(\texttt{whole}(x) \rightarrow \neg\,\texttt{vegan}(x))$.

(b) Robbie only likes one coffee drink, and that drink is not vegan. **Solution:**

$\exists x \forall y(\texttt{RobbieLikes}(x) \land \neg\,\texttt{Vegan}(x) \land [\texttt{RobbieLikes}(y) \to x = y])$

OR $\exists x(\texttt{RobbieLikes}(x) \land \neg\,\texttt{Vegan}(x) \land \forall y[\texttt{RobbieLikes}(y) \to x = y])$

(c) There is a drink that has both sugar and soy milk. **Solution:**

$\exists x(\texttt{sugar}(x) \land \texttt{soy}(x))$

Translate the following symbolic logic statement into a (natural) English sentence. Take advantage of domain restriction.

$$\forall x([\texttt{decaf}(x) \land \texttt{RobbieLikes}(x)] \to \texttt{sugar}(x))$$

Solution:

Every decaf drink that Robbie likes has sugar.

Statements like "For every decaf drink, if Robbie likes it then it has sugar" are equivalent, but only partially take advantage of domain restriction.

4. Review: Number Theory

Let p be a prime number at least 3, and let x be an integer such that $x^2 \% p = 1$.

(a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$. (this proof will be short!)
(Try to do this without using the theorem "Raising Congruences To A Power")
Solution:

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod{p}$. Since y is arbitrary, the claim holds.

(b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Solution:

Suppose $x \equiv 1 \pmod{p}$. By the definition of Congruences, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that

$$pk = (x-1)$$

By multiplying both sides of pk = (x - 1) by (x + 1) and re-arranging the equation, we have

$$pk(x+1) = (x-1)(x+1)$$
$$p(k(x+1)) = (x-1)(x+1)$$

Since $(x-1)(x+1) = x^2 - 1$, by replacing $(x-1)(x+1)$ with $x^2 - 1$, we have

$$p(k(x+1)) = x^2 - 1$$

Note that since k and x are integers, (k (x + 1)) is also an integer. Therefore, by the definition of divides $p \mid x^2 - 1$.
Hence, by the definition of Congruences, $x^2 \equiv 1 \pmod{p}$.

(c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Solution:

Suppose $x^2 \equiv 1 \pmod{p}$. By the definition of Congruences,

$$p \mid x^2 - 1$$

Since $(x - 1)(x + 1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x - 1)(x + 1)$, we have

$$p \mid (x - 1)(x + 1)$$

Note that for an integer p if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$. In this case, since p is a prime number, by applying the rule, we have $p \mid (x - 1)$ or $p \mid (x + 1)$.
Therefore, by the definition of Congruences, we have $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.