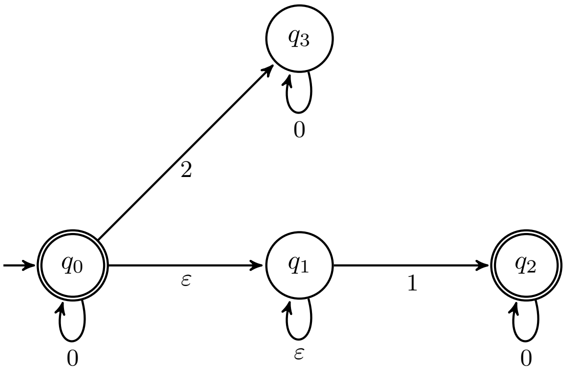
Section 9: NFAs, Subset Construction, and Review

1. NFAs

(a) Recall the following NFA from last section. What language does the NFA accept?

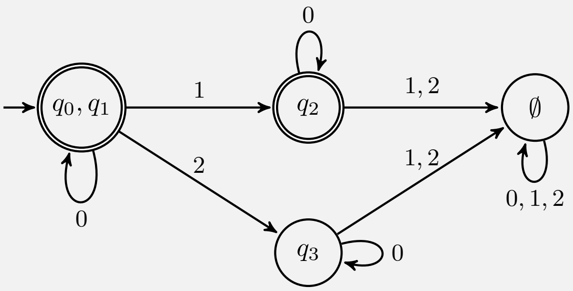


Solution:

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

(b) Convert the NFA form part (a) to a DFA.

Solution:



2. Translate to Logic

Express each of these system specifications using predicates, quantifiers, and logical connectives.

(a) Every user has access to an electronic mailbox.

Solution:

Let the domain be users and mailboxes. Let $\mathsf{User}(x)$ be "x is a user", let $\mathsf{Mailbox}(y)$ be "y is a mailbox", and let $\mathsf{Access}(x, y)$ be "x has access to y".

$$\forall x\ (\mathsf{User}(x) \rightarrow (\exists y\ (\mathsf{Mailbox}(y) \land \mathsf{Access}(x, y))))$$

(b) The system mailbox can be accessed by everyone in the group if the file system is locked.

Solution:

Solution1: Let the domain be people in the group. Let $\mathsf{CanAccessSM}(x)$ be "x has access to the system mailbox". Let FileSystemLocked be the proposition (predicate that is just a constant function) "the file system is locked."

$$\mathsf{FileSystemLocked} \to \forall x\ \mathsf{CanAccessSM}(x).$$

Solution2: Let the domain be people and mailboxes and use $\mathsf{Access}(x, y)$ as defined in the solution to part (a), and then also add $\mathsf{InGroup}(x)$ for "x is in the group", and let SystemMailBox be the name for the system mailbox. Then the translation becomes

$$\mathsf{FileSystemLocked} \to \forall x\ (\mathsf{InGroup}(x) \to \mathsf{Access}(x, \mathsf{SystemMailBox})).$$

(c) The firewall is in a diagnostic state only if the proxy server is in a diagnostic state.

Solution:

Let the domain be all applications. Let $\mathsf{Firewall}(x)$ be "x is the firewall", and let $\mathsf{ProxyServer}(x)$ be "x is the proxy server." Let $\mathsf{Diagnostic}(x)$ be "x is in a diagnostic state".

$$\forall x\ \forall y\ ((\mathsf{Firewall}(x) \land \mathsf{Diagnostic}(x)) \to (\mathsf{ProxyServer}(y) \to \mathsf{Diagnostic}(y))$$

(d) At least one router is functioning normally if the throughput is between 100kbps and 500 kbps and the proxy server is not in diagnostic mode.

Solution:

Let the domain be all applications and routers. Let $\mathsf{Router}(x)$ be "x is a router", and let $\mathsf{ProxyServer}(x)$ be "x is the proxy server." Let $\mathsf{Diagnostic}(x)$ be "x is in a diagnostic state". Let ThroughputNormal be "the throughput is between 100kbps and 500 kbps". Let $\mathsf{Functioning}(y)$ be "y is functioning normally".

$$(\mathsf{ThroughputNormal} \land \forall x\ (\neg\mathsf{ProxyServer}(x) \lor \neg\mathsf{Diagnostic}(x))) \to \exists y\ (\mathsf{Router}(y) \land \mathsf{Functioning}(y))$$

3. Palindromes

We say an integer is *palindromic* if the digits read the same when written forward or backward. Prove that every palindromic integer with an even number of digits is divisible by 11. (No induction proofs.)

Hint 1: $10 \equiv -1 (\text{mod } 11)$.
Hint 2: Write the number in terms of its $2n$ decimal digits as $d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \cdots d_{2n-1} \cdot 10^{2n-1}$

Solution:

Consider any palindrome with an even number of digits: $d_{2n-1}d_{2n-2}\cdots d_1 d_0$. Since this number is base 10, we can write it as the following summation:

$$(d_{2n-1}d_{2n-2}\cdots d_1 d_0)_{10} \bmod 11 \equiv \sum_{i=0}^{2n-1} d_i 10^i \pmod{11}$$

Since the number is a palindrome, we know $d_i = d_{(2n-1)-i}$. So, we have:

$$\equiv \sum_{i=0}^{n-1} d_i(10^i + 10^{(2n-1)-i}) \pmod{11}$$

We know $(10)^i \equiv (-1)^i (\text{mod } 11)$. So by the addition and multiplication theorems of modular arithmetic:

$$\equiv \sum_{i=0}^{n-1} d_i((-1)^i + (-1)^{(2n-1)-i}) \pmod{11}$$

Finally, note that because $2n-1$ is odd, $(2n-1)-i$ will always have opposite parity from i. Also, $(-1)^{2k} = ((-1)^2)^k = 1^k = 1$ and $(-1)^{2k+1} = (-1)(-1)^{2k} = -1$. So:

$$\begin{aligned}&\equiv \sum_{i=0}^{n-1} d_i(-1+1) \pmod{11}\\ &\equiv 0 \pmod{11}\end{aligned}$$

So, every palindromic integer with an even number of digits is divisible by 11.

4. Multiplicative Inverses

For p a prime number, show that for all $n \in [p-1]$, there exists a unique multiplicative inverse of n mod p. In other words for all $n \in [p-1]$, there exists a unique $m \in [p-1]$ so that $n \cdot m \equiv 1 \pmod{p}$.

Solution:

We know a multiplicative inverse exists for all $n \in [p-1]$ because $\gcd(n,p) = 1$ for all $n \in [p-1]$ from Bezout's theorem, in particular one can run the Extended Euclidean Algorithm and find the multiplicative inverse. It remains to see the multiplicative inverse is unique.

Assume for sake of deriving a contradiction that the inverse is not unique and there exists distinct $j, k \in [p-1]$ such that $nj \equiv 1 \pmod{p}$ and $nk \equiv 1 \pmod{p}$. Recall from Bezout's theorem, there exists integers s, t such that $nj + ps = 1$ and $nk + pt = 1$. Subtracting these equations from each other, $nj - nk + ps - pt = 0$, and so modulo p, $n(j-k) \equiv 0 \pmod{p}$. We proved on HW5 that if $p \mid ab$ then $p \mid a$ or $p \mid b$ (recall you can prove this by examining the prime factorizations). Since $\gcd(n,p) = 1$, it follows that $p \mid (j-k)$, or in other words $(j-k) \equiv 0 \pmod{p}$. As $j, k \in [p-1]$, it must be that $j = k$, which is a contradiction on the distinctness of j, k.

5. Polygonal chords

A polygon is a 2 dimensional shape made of straight line segments with at least 3 vertices. We define a chord of a polygon to be a straight line joining two non-adjacent vertices of the polygon. A convex polygon is a polygon such that any chord lies in its interior. What is the maximum number of non-intersecting chords a convex polygon on n vertices can have?

The insight for this problem is challenging! If you don't get it after some thought, be sure to look at the solution.

Solution:

Fix an arbitrary convex polygon P on n vertices. Fix an arbitrary vertex v of P and consider the set of all chords from v, call this set S. As v is adjacent to exactly 2 vertices of P and non-adjacent to the other $n-3$ vertices (excluding itself, here), S contains $n-3$ chords. Further all chords in S are non-intersecting, and it follows that the maximum number of non-intersecting chords in a convex polygon on n vertices is at $\geq n-3$.

Let $P(n)$ be "A set containing only non-intersecting chords of an n-vertex convex polygon contains at most $n-3$ elements."

Base Cases ($n = 3$). There are no chords here as every vertex is incident to every other vertex (excluding itself) in a triangle. As $0 = 3 - 3$, $P(3)$ holds.

Induction Hypothesis. Suppose that $P(j)$ is true for all integers $3 \leq j \leq k$ for some arbitrary integer k.

Induction Step. Consider a polygon P on $k+1$ vertices where $k \geq 3$, and let S be a set of non-intersecting chords of P. We will show the number of elements in S is at most $k + 1 - 3$. If S is empty, then the number of elements in S is 0 which is less than $k + 1 - 3$, since $k \geq 3$. If S is not empty, then let s be an arbitrary chords in S. As P is on at least 4 vertices, s divides P into 2 polygons, P_1 and P_2, on n_1 vertices and n_2 vertices, respectively, so that $n_1 + n_2 = k + 1 + 2$ and $n_1, n_2 \geq 3$.

As all chords in S were non-intersecting, the chords in $S \setminus \{s\}$ lie in the interior of exactly one of P_1 or P_2. [(This extra detail is not necessary for a correct solution) More specifically, a chord $t \in S \setminus \{s\}$ cannot lie in neither P_1 or P_2 because that would mean one of t's vertices is in P_1 and one is in P_2, so it would intersect s; on the other hand, t cannot lie in both P_1 and P_2 because P_1 and P_2 only share the vertices of s.] Thus to count the number of chords in S, we add 1 to the sum of the number of chords from S in P_1 and the number of chords from S in P_2. As n_1 and n_2 are in $[3, k]$ and the chords from S in P_1/P_2 are non-intersecting and disjoint, we can invoke the induction hypotheses $P(n_1)$ and $P(n_2)$ to see that the number of chords in S is at most $1+n_1-3+n_2-3 = n_1+n_2-5 = k+1+2-5 = k+1-3$, proving $P(k + 1)$.

Conclusion. Therefore $P(n)$ holds for all integers $n \geq 3$ by strong induction.