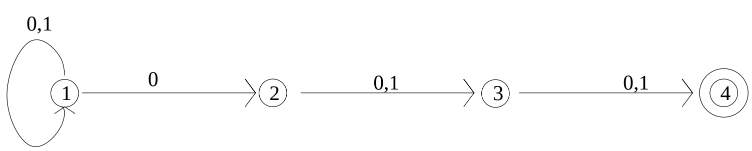
Some answers to Homework 7

May 5, 2004

Question 1. Define a Non-Deterministic Finite State Automaton N on the alphabet $A = \{0, 1\}$ which accepts exactly the language $\mathcal{L} = \{u \in A^* \mid u = w0xy\}$, i.e., precisely the words on A where the third letter from the end is 0. Define a Deterministic Finite State Automaton M equivalent to N and find the minimal deterministic automaton equivalent to N.

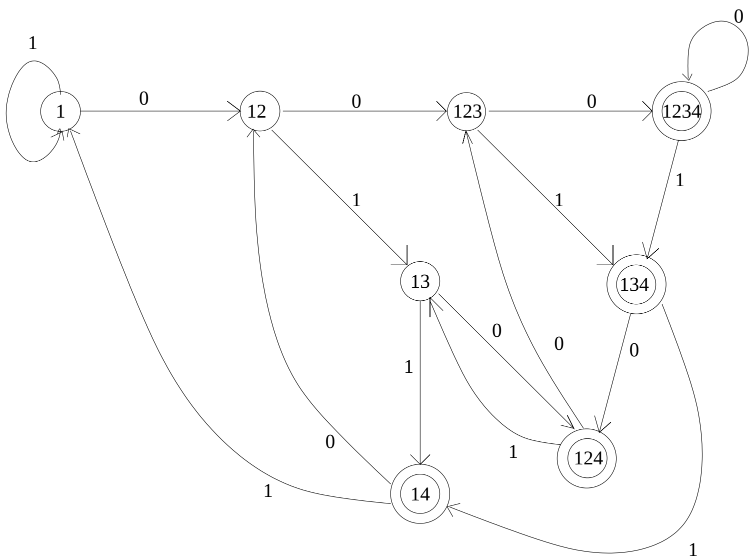
Answer. $N = \{S, A, \nu, 1, F\}$ where the set of states S is $\{1, 2, 3, 4\}$, the initial state is 1, the only final state in F is 4 and the transition function ν is given by the following transition diagram:



A Deterministic Finite State Automaton equivalent to N is $M = \{S', A, \nu', \{1\}, F'\}$ where the set of states S' is

$$\{\ \{1\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{1,2,3,4\}\ \},$$

the set of final states F is $\{\{1,4\}, \{1,2,4\}, \{1,3,4\}, \{1,2,3,4\}\}$ and the transition function ν' is given by the following diagram:



We need to show that the automaton M is minimal, i.e., that all states in S' are distinguishable from one another. To this purpose we construct the following table:

	{1,2}	00						
	{1,2,3}	0	0					
(F)	{1,2,3,4}	X	X	X				
	{1,3}	0	0	00	X			
(F)	{1,3,4}	X	X	X	00	X		
(F)	{1,2,4}	X	X	X	0	X	0	
(F)	{1,4}	X	X	X	0	X	0	00
		{1}	{1,2}	{1,2,3}	{1,2,3,4}	{1,3}	{1,3,4}	{1,2,4}

Since all states are distinguishable (by words of length at most 2), the automaton M is minimal.

Notice that we have applied the powerset construction in an abbreviated form: the states of M are the set S' of all subsets of S that are reachable from the state $\{1\}$ according to the definition of transition used in the powerset construction. In fact, we could have defined $M = \{\wp(S), A, \nu', \{1\}, F'\}$, taking the set of all subsets of S (the *powerset* $\wp(S)$ of S) as the set of states, defining ν' as in the powerset construction. Later, when we look for a minimal deterministic automaton, we find that the subsets in the set $S'' = \{\ \emptyset,$

$\{2\}$, $\{3\}$, $\{4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, $\{2,3,4\}$ } are not reachable from the initial state $\{1\}$. Since the cardinality $|\wp(S)| = 2^{|S|} = 16$ and $S' = \wp(S) \setminus S''$ and also we have shown that M is minimal, our construction yields precisely the deterministic automaton obtained by applying first the powerset construction to N and then eliminating unreachable states.

Question 5. Show that there are infinitely many prime numbers of the form $6n - 1$.

Answer: Write q_n for the n-th prime of the form $6k - 1$, i.e., q_n is the n-th prime equivalent to 5 (mod 6). Clearly $q_1 = 5$. For the inductive step, suppose

$$q_1, \ldots, q_n \text{ are all the prime numbers of the form } 6k - 1 \qquad (*)$$

and let $c = 6(q_1 \cdot \ldots \cdot q_n) - 1$. Notice that $c > q_n > \ldots > q_1$, hence if assumption $(*)$ is true, then c cannot be prime, hence it must be divisible by some prime. Now we consider all possible prime divisor p of c and look at p mod 6: by considering all possible cases we show that at least one prime divisor p of c must be equivalent to 5 (mod 6); thus it follows from our assumption (*) that p must be one of the q_i and from this we derive a contradiction.

Let $c = p_1 \cdot \ldots \cdot p_\ell$ be the prime factorization of c (thus $p_1, \ldots, p_\ell$ are prime numbers). We have the following cases:

1. for some $j \leq \ell$, $p_j \equiv 2 \pmod 6$; this is impossible, because *c is odd.*
2. for some $j \leq \ell$, $p_j \equiv 3 \pmod 6$; this is also impossible. Indeed, if $b \equiv 3 \pmod 6$ and $a \equiv 1$ or 3 or $5 \pmod 6$, then also $a \cdot b \equiv 3 \pmod 6$. Therefore if we had $p_j \equiv 3 \pmod 6$, then we would have also $p_1 \cdot \ldots \cdot p_\ell \equiv 3 \pmod 6$; but $c \equiv 5 \equiv -1 \pmod 6$.
3. for all $j \leq \ell$ $p_j \equiv 1 \pmod 6$; this is impossible, because in this case $p_1 \cdot \ldots \cdot p_\ell \equiv 1 \pmod 6$, but $c \equiv 5 \equiv -1 \pmod 6$. Hence *$c$ cannot be divided only by prime numbers of this form.*

Therefore for some $j \leq \ell$, $p_j \equiv 5 \pmod 6$. Our assumption (*) is that $q_1, \ldots, q_n$ are all the prime numbers of the form $6k-1$. Therefore $p_j = q_i$ for some $i \leq n$, and q_i divides c, let's write

$$c = q_i \cdot a. \qquad (\dagger)$$

Now q_i divides $q_1 \cdot \ldots \cdot q_n$: indeed, letting $b = q_1 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_n$, we have

$$q_i \cdot b = q_1 \cdot \ldots \cdot q_n = c - 1. \tag{‡}$$

But then by (†) and (‡) we have

$$1 = (q_i \cdot a) - (q_i \cdot b) = q_i \cdot (a - b) \tag{**}$$

and this is impossible, because no prime number divides 1.

Therefore our assumption (∗) that $q_1, \ldots, q_n$ are all the prime numbers equivalent to 5 (mod 6) is false and there is a prime number p in the prime factorization of c which is greater than q_n and $p \leq c$. This concludes the proof.

Notice that the argument remains valid if we define

$$c = 6(q_n! - 1)$$

where $a!$ is the factorial function.

Notice that implicit in the proof there is an algorithm to compute the function

$$f(n) = q_n, \qquad \text{the } n\text{-th prime number of the form } 6k - 1.$$

We can show that f is *primitive recursive*. Indeed define $f(1) = 5$ and

$$f(n + 1) = \text{ the least } p \leq c \text{ such that } p \text{ is prime, } p > f(n) \text{ and } rm(p, 6) = 5$$

where $rm(p, 6)$ is the remainder of the division of p by 6. Notice that

- f is defined by primitive recursion;
- in the base case f is the constant function 5;
- in the recursive step the function f is defined by *bounded minimization* with bound c, using the predicate *p is prime* and the function $rm(x, y)$;
- the function $rm(x, y)$ has been shown to be primitive recursive in the Homework assignment 3;
- the bound c defined as $6(q_n!) - 1$ is primitive recursive, because multiplication and subtraction are primitive recursive and the factorial function is also primitive recursive, as it is defined by primitive recursion from the constant function 1 and multiplication:

$$0! = 1, \qquad (n + 1)! = n! \cdot (n + 1);$$

- the predicate "*p is prime*", defined as

$$p \text{ } is \text{ } prime \equiv_{df} p > 1 \wedge \forall x \leq p.(x \text{ divides } p \rightarrow x = 1 \vee x = p)$$

  is primitive recursive, because it is defined using conjunction, disjunction implication and bounded quantification from the primitive recursive predicates "$x > y$" and "x *divides* y".

Therefore f is primitive recursive.