# Automata and Formal Languages - Homework 6 

Due Friday 20th November 2015 (TA: Christopher Broadbent)

Please note that questions marked $\star \star$ are extra-challenging; you should not worry if you are unable to solve them as they are harder than what will be expected in the exam. Only consider them if you have time and are interested!

## Exercise 6.1

Construct DFAs and lazy DFAs that recognise the set of strings containing the patterns (i) mammamia, and (ii) abracadabra.

## Exercise 6.2

Two-way finite automata are an extension of lazy automata in which the reading head may not only move right or stay put, but also move left. The tape extends infinitely long to both the left and to the right of the input with all cells empty. A word is accepted if the control state is a final state at the moment the head reaches an empty cell to the right of the input for the first time.
(i) Give a two-way DFA for the language $(0+1)^{*} 1(0+1)^{4}$. How big is this automaton compared to the smallest ordinary DFA for the same language?
(ii) Show that for every $n \in \mathbb{N}$ there exists a two-way DFA for the language $(0+1)^{*} 1(0+1)^{n}$ with $O(n)$ states. How many states does the minimal ordinary DFA have for each $n \in \mathbb{N}$ ?
(iii) Sketch an algorithm for membership of a two-way DFA
(iv) $\star \star$ Sketch an algorithm for emptiness of two-way DFA
(v) $\star \star$ Prove that the languages recognized by two-way DFA are regular.

## Exercise 6.3

Which of the following relations are regular (with the lsbf-encoding)? Justify your answers.
(i) $\left\{\left(n, n^{2}\right) \mid n \in \mathbb{N}\right\}$
(ii) $\{(n, m) \mid n, m \in \mathbb{N}$ with $m \leq \sqrt{n}\}$
(iii) $\{(n, 5 n) \mid n \in \mathbb{N}\}$
(iv) $\{(n, 7+n) \mid n \in \mathbb{N}\}$
(v) $\{(n, 7+5 n) \mid n \in \mathbb{N}\}$
(vi) $\left\{(n, m) \mid n, m \in \mathbb{N}\right.$ with $2 n+3 m=2^{k}$ for some $\left.k \in \mathbb{N}\right\}$

## Exercise 6.4

$\star \star$ Suppose that $L$ is a regular language. Let us write $|w|$ for the length of the word $|w|$. Prove that the language $|L|:=\{\operatorname{lsbf}(|w|) \mid w \in L\}$ is regular.
[Hint: It follows from the final question of Exercise Sheet 2 that there exist $k_{0}, k_{1}, \ldots, k_{n}$ such that

$$
|L|=\left\{\operatorname{lsbf}\left(k_{0}+\lambda_{1} k_{1}+\cdots+\lambda_{n} k_{n}\right) \mid \lambda_{i} \in \mathbb{N} \text { for each } 1 \leq i \leq n\right\}
$$

(i) Show that the relation $R_{k}:=\{(k, \lambda k) \mid \lambda \in \mathbb{N}\}$ is regular for each $k \in \mathbb{N}$.
(ii) Show also that for any set of numbers $N \subseteq \mathbb{N}$ such that $\operatorname{lsbf}(N)$ is regular, it is the case that the relation

$$
S_{N}:=\{(r, m) \mid r, m \in \mathbb{N}, \text { such that } r=m+K \text { for some } K \in N\}
$$

is regular.
(iii) Then put these facts together to prove the result (using induction on $n$ and the Post operator from the lectures.)]

## Solution 6.2

(i) The following two-way DFA does the job:

$$
A:=\left\langle\{0,1\}, Q, \delta, q_{0},\left\{p_{4}\right\}\right\rangle
$$

where $Q:=\left\{q_{0}, p_{0}, p_{1}, p_{2}, p_{3}, p_{4}, q_{4}, q_{3}, q_{2}, q_{1}\right\}$ and

$$
\delta\left(0, q_{0}\right)=\left(q_{0}, R\right) \quad \delta\left(1, q_{0}\right)=\left(p_{0}, R\right) \quad \delta\left(-, p_{i}\right)=\left(p_{i+1}, R\right) \quad \delta\left(-, q_{i+1}\right)=\left(q_{i}, L\right) \text { for each } i \in[0,3]
$$

We will give a proof of correctness for the more general construction in the next part.
The residuals of $L:=(0+1)^{*} 1(0+1)^{4}$ are as follows (for all $k \geq 0$ ):

$$
\begin{gathered}
L^{0^{k}}=(0+1)^{*} 1(0+1)^{4} \\
L^{0^{k} 1}=(0+1)^{*} 1(0+1)^{4}+(0+1)^{4} \\
L^{0^{k} 10}=(0+1)^{*} 1(0+1)^{4}+(0+1)^{3} \\
L^{0^{k} 11}=(0+1)^{*} 1(0+1)^{4}+(0+1)^{4}+(0+1)^{3}
\end{gathered}
$$

In fact the residuals will be all those languages of the form $L+\sum_{i \in N}(0+1)^{i}$ for a set $N \subseteq[0,4]$ meaning that there are $2^{5}=32$ residuals. Thus the minimal DFA for $L$ must contain 16 states, more than that of the two-way DFA that we have just given.
We will prove the more general case in the next part.
(ii) Let $L_{n}:=(0+1)^{*} 1(0+1)^{n}$ (for each $n \in \mathbb{N}$ ). We claim that each such language is recognised by a 2-way DFA given by:

$$
A_{n}=\left\langle\{0,1\}, Q_{n}, \delta_{n}, q_{0},\left\{p_{n}\right\}\right\rangle
$$

where $Q_{n}:=\left\{q_{i} \mid i \in[0, n]\right\} \cup\left\{p_{i} \mid i \in[0, n)\right\}$ and

$$
\delta\left(0, q_{0}\right)=\left(q_{0}, R\right) \quad \delta\left(1, q_{0}\right)=\left(p_{0}, R\right) \quad \delta\left(-, p_{i}\right)=\left(p_{i+1}, R\right) \quad \delta\left(-, p_{n}\right)=\left(q_{n-1}, L\right) \quad \delta\left(-, q_{j+1}\right)=\left(q_{j}, L\right)
$$

for each $i \in[0, n)$ and $j \in[0, n-1)$ where _ ranges over $\{0,1\}$. We will now prove that $A_{n}$ recognises the intended language.
Consider a word $w \in\{0,1\}^{*}$ that contains $R$ occurrences of the symbol 1 . For each $r$ such that $0 \leq r \leq R$, we inductively define the prefix $r$ of $w$ by the following:

$$
w_{0}=\epsilon \quad w_{r+1} \text { is the shortest prefix of } w \text { ending with } 1 \text { of which } w_{r} \text { is a prefix }
$$

In other words, $w_{r}$ is the prefix of $w$ that ends in the $r$ th occurrence of 1 .
When reading such a word $w$, the automaton maintains the invariant consisting of the conjunction of all of the following:

- If it is in state $p_{i}$, then the head of the automaton will be at a position immediately following a prefix of the form $w_{r+1}(0+1)^{i}$.
- If it is in state $q_{i}$, then (i) the head of the automaton will be at a position immediately following a prefix of the form $w_{r}(0+1)^{i}$, and (ii) for $b_{i+1}, \ldots, b_{n} \in\{0,1\}$ s.t. $w_{r} b_{i+1} \cdots b_{n}$ is a prefix of $w$, it is the case that $w_{r} b_{i+1} \cdots b_{n} \notin L_{n}$

This follows from the fact that the initial position of the automaton satisfies the invariant (the first symbol of the input word is in the position immediately following the prefix $w_{0}=\epsilon$ and the initial state is $q_{0}$ ) and it can be checked that each transition preserves the invariant.
It follows that $\mathcal{L}\left(A_{n}\right) \subseteq L_{n}$ since if the accepting state is $p_{n}$ is attained in the position immediately after the last symbol in the word, then the invariant implies that the word must be of the from $w_{r+1}(0+1)^{n}$, i.e. of the form $(0+1)^{*} 1(0+1)^{n}$.
In order to prove that $L_{n} \subseteq \mathcal{L}\left(A_{n}\right)$ we prove that $\overline{\mathcal{L}\left(A_{n}\right)} \subseteq \overline{L_{n}}$. Let $w \in \overline{\mathcal{L}\left(A_{n}\right)}$. Then one of two possibilities must hold: (i) the automaton has reached a non-accepting state with its head just past the end of the word, or (ii) the automaton's head never reaches a position just beyond the end of the word.
In the first case, the invariant tells us that indeed $w \notin L_{n}$. It therefore suffices to rule out the second case. That is we must prove that for every word $w$ the automaton's head eventually reaches the position just beyond its end.

Note that the invariant tells us that the head never moves to the left of the word. Therfore if the head also never moves to the right of the word it must be the case that the automaton has an infinite run on $w$. By inspection of the transition relation we can also see that an infinite run must reach state $q_{0}$ infinitely often.
Let $w^{\prime} b$ be the prefix of $w$ such that $b$ is the right-most position that the head reaches when in state $q_{0}$.
We claim that there is a prefix $w^{\prime} b b_{0}$ of $w$ such that the automaton will also reach $b^{\prime}$ in state $q_{0}$, which gives the required contradition (since we assumed $b$ is the right-most such position).
If $b=0$, then this follows immediately. So consider the case when $b=1$. Then the automaton will move its head to $b_{0}$ and adopt state $p_{0}$. By induction on the length of the run, we can then see that in fact $w$ must have a prefix of the form $w^{\prime} b b_{0} \cdots b_{n}$ such that its head will reach each $b_{i}$ (for $0 \leq i \leq n$ ) in state $p_{i}$ and each $b_{j}$ (for $0 \leq i<n$ ) in state $q_{j}$. In particular it will reach position $b_{0}$ in state $q_{0}$, as required.
So there exists a two-way DFA of linear size (with respect to $n$ ) recognising each $L_{n}$. We now prove that the minimal (ordinary DFA) has exponential size. Since the minimal DFA has size equal to the number of residuals of $L_{n}$, it suffices to prove that $L_{n}$ has exponentially many residuals.
We claim that the residuals of $L_{n}$ are precisely those languages belonging to the following family:

$$
\mathcal{R}:=\left\{R_{N} \mid N \subseteq[0, n]\right\} \quad \text { where } \quad R_{N}=(0+1)^{*} 1(0+1)^{n}+\sum_{i \in N}(0+1)^{i}
$$

Proving this claim is sufficient since $|\mathcal{R}|=2^{n+1}$.

- First we show that every residual of $L_{n}$ belongs to $\mathcal{R}$. Observe that $L_{n}=R_{\emptyset}$ and so $L_{n} \in \mathcal{R}$. We thus just need to check that $\mathcal{R}$ is closed under taking the residual of words of length one (it follows by induction on word-length that the residual of a word of any length belongs to the family).
Below we use bold-face for members of the alphabet $\{\mathbf{0}, \mathbf{1}\}$ to distinguish them from the integers 0 and 1 .

$$
\begin{align*}
R_{N}^{\mathbf{0}}=\left((0+1)(0+1)^{*}\right)^{\mathbf{0}}+ & \left(1(0+1)^{n}\right)^{\mathbf{0}}+\sum_{i \in N}\left((0+1)^{i}\right)^{\mathbf{0}} \\
& =(0+1)^{*} 1(0+1)^{n}+\emptyset+\sum_{i \in\{j \in N \mid j>0\}}(0+1)^{i-1}=R_{\{j-1 \in N \mid j>0\}} \tag{1}
\end{align*}
$$

$$
\begin{align*}
& R_{N}^{1}=\left((0+1)(0+1)^{*}\right)^{\mathbf{1}}+\left(1(0+1)^{n}\right)^{\mathbf{1}}+\sum_{i \in N}\left((0+1)^{i}\right)^{\mathbf{1}} \\
&=(0+1)^{*} 1(0+1)^{n}+(0+1)^{n}+\sum_{i \in\{j \in N \mid j>0\}}(0+1)^{i-1}=R_{\{n\} \cup\{j-1 \in N \mid j>0\}} \tag{2}
\end{align*}
$$

Thus $R_{N}^{0} \in \mathcal{R}$ and $R_{N}^{1} \in \mathcal{R}$, as required.

- We now show the converse, that every member of $\mathcal{R}$ is in fact a residual of $L_{n}$. In other words, we must show that for each $N \subseteq[0, n]$ there exists a word $w_{N} \in\{\mathbf{0}, \mathbf{1}\}^{*}$ such that $R_{N}=L_{n}^{w_{N}}$.
We claim that the word $w_{\emptyset}:=\epsilon$ and when $N \neq \emptyset, w_{N}:=b_{\min (N)} \cdots b_{n}$ fits the bill where

$$
b_{i}:= \begin{cases}0 & \text { if } i \notin N \\ 1 & \text { if } i \in N\end{cases}
$$

We argue by induction on the length of $w_{N}$ (up to a maximum length of $n+1$ ) that $L_{n}^{w_{N}}=R_{N}$.
The base case is when $w_{N}=\epsilon$ and thus $N=\emptyset$. Since $R_{\emptyset}=L_{n}=L_{n}^{\epsilon}$, the base case holds.
For the induction step, we assume as induction hypothesis that for a word $w_{N}=b_{n} \cdots b_{\min (N)}$ with $\min (N)>0$ we have $L_{n}^{w_{N}}=R_{N}$. We must show that $L_{n}^{w_{N} b}=R_{N^{\prime}}$ where

$$
N^{\prime}= \begin{cases}\{j-1 \mid j \in N\} & \text { if } b=0 \\ \{n\} \cup\{j-1 \mid j \in N\} & \text { if } b=1\end{cases}
$$

But $L_{n}^{w_{N} b}=R_{N}^{b}=R_{N^{\prime}}$ by equations (1) and (2).
(iii) A semi-algorithm for membership can be obtained simply by simulating a run of the 2 -way DFA on the candidate word. Since the automaton is deterinisitic, if the word is accepted by the automaton, the simulation will terminate.

If the word is rejected by the automaton due to the unique run moving off either end of the word, then the simulation will also terminate.

However if the word is rejected by the automaton because the unique run is infinitely long, then the simulation will not terminate.
Thus to obtain an algorithm for membership, we must simulate the 2-way DFA on the candidate word and additionally for each position $i$ in the word maintain a set of states $Q_{i}$ in which the automaton has been when its head points at $i$. The algorithm will additionally terminate and announce that the word is rejected by the automaton if the simulation moves the automaton's head to a position $i$ in state $q$ such that already $q \in Q_{i}$.

## Solution 6.3

(i) Irregular. The language corresponding to the relation, which we claim is irregular, is by definition the following:

$$
L_{1}:=\left\{\left(a_{1}, b_{1}\right) \cdots\left(a_{l}, b_{l}\right) \mid a_{1} \cdots a_{l} \in l \operatorname{sbf}(n) \text { and } b_{1} \cdots b_{l} \in l s b f\left(n^{2}\right) \text { for } n \in \mathbb{N}\right\}
$$

To show that $L_{1}$ is irregular, we show that it has infinitely many residuals. Suppose for contradiction that it only has finitely many residuals.
For each integer $k \geq 1$, let $t_{k}, u_{k}$ and $v_{k}$ be the following words:

$$
t_{k}:=\underbrace{(0,0) \cdots(0,0)}_{k \text {-times }}(1,0) \quad u_{k}:=\underbrace{(0,0) \cdots(0,0)}_{k \text {-times }}(1,0) \underbrace{(0,0) \cdots(0,0)}_{(k-1) \text {-times }}(0,1) \quad v_{k}:=\underbrace{(0,0) \cdots(0,0)}_{(k-1) \text {-times }}(0,1)
$$

Observe that $\pi_{1}\left(u_{k}\right) \in \operatorname{lsbf}\left(2^{k}\right)$ and that $\pi_{2}\left(u_{k}\right) \in \operatorname{lsbf}\left(2^{2 k}\right)$, and so $u_{k} \in L_{1}$ for each $k \geq 1$. It must thus be the case that for each $k \geq 1$ we have $v_{k} \in L_{1}^{t_{k}}$.
Since we are assuming that there are only finitely many residuals, there must exist $k_{1}, k_{2} \geq 1$ such that $k_{1} \neq k_{2}$ and $L^{t_{k_{1}}}=L^{t_{k_{2}}}$. But that means that $v_{k_{2}} \in L^{t_{k_{1}}}$, which is to say that

$$
t_{k_{1}} v_{k_{2}}=\underbrace{(0,0) \cdots(0,0)}_{k_{1} \text {-times }}(1,0) \underbrace{(0,0) \cdots(0,0)}_{\left(k_{2}-1\right) \text {-times }}(0,1) \in L_{1}
$$

This implies that $2^{2 k_{1}}=2^{k_{1}+k_{2}}$ whence $2 k_{1}=k_{1}+k_{2}$ and $k_{1}=k_{2}$, which is a contradiction.
(ii) Irregular. Now consider the following relation:

$$
R_{2}^{\prime}:=\left\{\left(4^{k}, m\right) \mid\left(4^{k}, m\right) \in R_{2} \text { for some } k \geq 1 \text { and there is no } m^{\prime} \text { s.t. }\left(4^{k}, m^{\prime}\right) \in R_{2} \text { and } m^{\prime}>m\right\}
$$

Suppose that $\left(4^{k}, m\right) \in R_{2}^{\prime}$. Then $\left(4^{k}, m\right) \in R_{2}$ and so $m \leq \sqrt{4^{k}}$, that is $m \leq 2^{k}$. Moreover, there is no $m^{\prime}>m$ such that $m^{\prime} \leq 2^{k}$. Thus in fact $m=2^{k}$. So all elements of $R_{2}^{\prime}$ must be of the form ( $4^{k}, 2^{k}$ ) for some $k \geq 2$.
Conversely, since $4^{k}=\left(2^{k}\right)^{2}$, it follows that all elements of the form $\left(4^{k}, 2^{k}\right)$ for $k \geq 2$ belong to $R_{2}^{\prime}$. Thus we can characterise $R_{2}^{\prime}$ by:

$$
R_{2}^{\prime}=\left\{\left(n^{2}, n\right) \mid n=2^{k} \text { for some } k \geq 1\right\}
$$

A very similar argument to that for part (i) shows that $R_{2}^{\prime}$ is not regular.
Now suppose for contradiction that $R_{2}$ is regular. The relation $<$ is also regular [needs proof, but we leave as an exercise] and so the join construction from the lectures tells us that $R_{2} \circ<$ is regular. Thus $R_{2} \cap \overline{\left(R_{2} \circ<\right)}$ is regular. But by definition we must have

$$
R_{2}^{\prime}=\left\{\left(4^{k}, m\right) \mid k \geq 1 \text { and }\left(4^{k}, m\right) \in R_{2} \cap \overline{\left(R_{2} \circ<\right)}\right\}
$$

Since $\bigcup_{k=1}^{\infty} \operatorname{lsb} f\left(4^{k}\right)$ is also regular, we would get that $R_{2}^{\prime}$ is regular, a contradiction.
For the next parts we will first prove that the following relation is regular:

$$
R_{+}\left\{\left(m_{1}, m_{2}, n \mid n=m_{1}+m_{2}, \text { for } n, m_{1}, m_{2} \in \mathbb{N}\right\}\right.
$$

Note that this is a ternary relation and so its elements will be encoded by words over the alphabet $\{0,1\}^{3}$ (instead of $\{0,1\}^{2}$, as is used for binary relations).

We claim that the DFA $A_{+}\left\langle Q_{+},\{0,1\}, \hat{0}, \delta_{+}, F_{+}\right\rangle$recognises the language encoding $R_{+}$, where $Q_{+}=\{\hat{0}, \hat{1}, X\}$, $F_{+}=\{\hat{0}\}$, and $\delta$ is given by
$\delta_{+}\left(\hat{c},\left(b_{1}, b_{2}, b\right)\right):=\hat{c^{\prime}} \quad$ where $\quad b=\left\{\begin{array}{ll}0 & \text { if an even number of } c, b_{1}, b_{2} \text { are } 0 \\ 1 & \text { if an odd number of } c, b_{1}, b_{2} \text { are } 0\end{array} \quad c^{\prime}= \begin{cases}0 & \text { if fewer than two of } c, b_{1}, b_{2} \text { are } 1 \\ 1 & \text { if at least two of } c, b_{1}, b_{2} \text { are } 1\end{cases}\right.$
and $\delta_{+}\left(\hat{c},\left(b_{1}, b_{2}, b\right)\right)=X$ otherwise. Intuitively $A_{+}$implements a half-adder. It represents the 'carry bit' in its state and sums this together with the input bits $b_{1}$ and $b_{2}$ to get the output bit $b$ and the state of the new carry bit. (The sink state $X$ is adopted when it reads an incorrect output bit).

We can formulate this intuition with the following assertion: After reading a word of the form $\left(a_{1}, b_{1}, c_{1}\right) \cdots\left(a_{k}, b_{k}, c_{k}\right)$ (for $k \geq 0$ ) such that $a_{1} \cdots a_{k} \in \operatorname{lsbf}\left(m_{1}\right)$ and $b_{1} \cdots b_{k} \in \operatorname{lsbf}\left(m_{2}\right)$, and $c_{1} \cdots c_{k} \in l s b f(n)$, it will be the case that:

- if $n=\left(m_{1}+m_{2}\right)$, then the automaton will be in state $\hat{0}$
- if $n+2^{k}=\left(m_{1}+m_{2}\right)$, then the automaton will be in state $\hat{1}$
- otherwise the automaton will be in state $X$.

This assertion can be proved by induction on the length $k$ of this word. The base case in when $k=0$, and here the assertion holds since $\epsilon \in \operatorname{lsbf}(0)$ and after 'reading' the empty word the automaton remains in its initial state, which is $\hat{0}$.

For the induction step let us suppose that the automaton has read a word $w=\left(a_{1}, b_{1}, c_{1}\right) \cdots\left(a_{k}, b_{k}, c_{k}\right)\left(a_{k+1}, b_{k+1}, c_{k+1}\right)$ of length $k+1$. Let $A_{k} \in \operatorname{lsbf}\left(a_{1} \cdots a_{k}\right), A_{k+1} \in \operatorname{lsbf}\left(a_{1} \cdots a_{k}, a_{k+1}\right) B_{k} \in \operatorname{lsbf}\left(b_{1} \cdots b_{k}\right), B_{k+1} \in \operatorname{lsbf}\left(b_{1} \cdots b_{k}, b_{k+1}\right)$ $C_{k} \in \operatorname{lsbf}\left(c_{1} \cdots c_{k}\right), C_{k+1} \in \operatorname{lsbf}\left(c_{1} \cdots c_{k}, c_{k+1}\right)$.

Observe that it is always the case that $A_{k+1}+B_{k+1}=A_{k}+B_{k}+a_{k+1} \cdot 2^{k}+b_{k+1} \cdot 2^{k}$ and that $C_{k+1}=C_{k}+c_{k+1} \cdot 2^{k}$. We consider each of several cases in turn.

- Suppose first that $C_{k+1}=A_{k+1}+B_{k+1}$. Then $C_{k}+c_{k+1} \cdot 2^{k}=A_{k}+B_{k}+a_{k+1} 2^{k}+b_{k+1} 2^{k}$. It must then be the case that one of the following holds:
$-C_{k}=A_{k}+B_{k}$. Then by the induction hypothesis the automaton will be in state $\hat{0}$ prior to reading the symbol $\left(a_{k+1}, b_{k+1}, c_{k+1}\right)$. Also it must be the case that $c_{k+1} \cdot 2^{k}=a_{k+1} 2^{k}+b_{k+1} 2^{k}$.
Suppose first that $c_{k+1}=0$. Then it must be the case that $a_{k+1}=b_{k+1}=0$. Then it must be the case that $\delta_{+}\left(\hat{0},\left(a_{k+1}, b_{k+1}, c_{k+1}\right)\right)=\hat{0}$.
Suppose now that $c_{k+1}=1$. Then it must be the case that $\left\{a_{k+1}, b_{k+1}\right\}=\{0,1\}$ and that $\delta_{+}\left(\hat{0},\left(a_{k+1}, b_{k+1}, c_{k+1}\right)\right)=$ 0. So in these cases we end up in state $\hat{0}$ and we also satisfy the requirement that $C_{k+1}+0.2^{k+1}=A_{k+1}+B_{k+1}$.
$-C_{k}+2^{k}=A_{k+1}+B_{k+1}$. By the induction hypothesis the automaton will be in state $\hat{1}$ prior to reading the symbol $\left(a_{k+1}, b_{k+1}, c_{k+1}\right)$. Also it must be the case that $c_{k+1} \cdot 2^{k}=2^{k}+a_{k+1} \cdot 2^{k}+b_{k+1} \cdot 2^{k}$. Thus it must be the case that $c_{k+1}=1$ and $a_{k+1}=b_{k+1}=0$.
Thus again by the definition of $\delta_{+}$we end up in state $\hat{0}$ with the required $C_{k+1}+0.2^{k+1}=A_{k+1}+B_{k+1}$.
- Suppose now that $C_{k+1}+2^{k+1}=A_{k+1}+B_{k+1}$. We can perform a similar case analysis to the above to get that we end up in state $\hat{1}$ (with the required $C_{k+1}+2^{k+1}=A_{k+1}+B_{k+1}$ ). This will use the fact that $2^{k}+2^{k}=2.2^{k}=2^{k+1}$.
- The final case is when neither $C_{k+1}=A_{k+1}+B_{k+1}$ nor $C_{k+1}+2^{k+1}=A_{k+1}+B_{k+1}$. We can again perform a case analysis to check that we must end up in state $X$. (This time we must check three possibilities for the induction hypothesis. $C_{k}=A_{k}+B_{k}, C_{k}+2^{k}=A_{k}+B_{k}$ and 'other', giving us states $\hat{0}, \hat{1}$ and $X$ respectively immediately after reading the $k$ th element.

Since $\hat{0}$ is the only final state, it follows immediately that $\mathcal{L}\left(A_{+}\right) \subseteq \mathcal{L}\left(R_{+}\right)$. We can also see that $\overline{\mathcal{L}\left(A_{+}\right)} \subseteq \overline{\mathcal{L}\left(R_{+}\right)}$since for $w \in \overline{\mathcal{L}\left(A_{+}\right)}$either a run of $A_{+}$in $w$ will end in $\hat{1}$, in which case the assertion tells us that $w$ represents a triple of the form ( $m_{1}, m_{2}, m_{1}+m_{2}+1$ ), or else it will end in state $X$, which tells us in particular that $w$ does not represent a triple of the form $\left(m_{1}, m_{2}, m_{1}+m_{2}\right)$.

Thus $\mathcal{L}\left(A_{+}\right)=\mathcal{L}\left(R_{+}\right)$.
For technical reasons it will be helpful to consider a variant of $R_{+}$which we call $R_{+}^{=}$. This differs in two ways: (i) it makes a copy of the first number being summed, and (ii) although $R_{+}^{=}$can naturally be seen as a quarternary relation, we in fact view it as a binary relation consisting of pairs of pairs (this will allow us to use Post below):

$$
R_{+}^{=}:=\left\{\left(\left(m_{1}, m_{2}\right),\left(m_{1}, m_{1}+m_{2}\right)\right) \mid m_{1}, m_{2} \in \mathbb{N}\right\}
$$

The regularity of $R_{+}^{=}$follows from the regularity of $R_{+}$.
(iii) Regular We prove something a bit more general: for every $\lambda \in \mathbb{N}$ it is the case that the relation

$$
R_{\lambda}:=\{(n, \lambda . n) \mid n \in \mathbb{N}\}
$$

is regular. (The relation in the question is the special case when $\lambda=5$ ).
We argue by induction on $\lambda \in \mathbb{N}$. The base case is when $\lambda=0$, which is trivial, since $R_{0}=\{(n, 0) \mid n \in \mathbb{N}\}=$ $(\{0,1\} \times\{0\})^{*}$.
For the induction step, suppose that we have already shown that $R_{\lambda}$ is regular. We can view $R_{\lambda}$ as a regular set of pairs of numbers and we have

$$
R_{\lambda+1}=\{(n, n+\lambda . n) \mid n \in \mathbb{N}\}=\left\{p \mid((n, \lambda . n), p) \in R_{+}^{=}\right\}=\left\{p \mid\left(p_{0}, p\right) \in R_{+}^{=} \text {for some } p_{0} \in R_{\lambda}\right\}=\text { Post }_{R_{+}^{=}}\left(R_{\lambda}\right)
$$

Since $R_{+}^{=}$and $R_{\lambda}$ are both regular, the lectures tell us that $\operatorname{Post}_{R_{+}^{=}}\left(R_{\lambda}\right)$ and thus $R_{\lambda+1}$ is also regular.
(iv) Regular The set of pairs $L_{7}=\{(n, 7) \mid n \in \mathbb{N}\}$ is regular since it is represented by the language given by the following regular expression

$$
\left(\sum_{b_{1}, b_{2}, b_{3} \in\{0,1\}}\left(b_{1}, 1\right)\left(b_{2}, 1\right)\left(b_{3}, 1\right)\right)(\{0,1\} \times\{0\})^{*}
$$

The required language is thus given by $\operatorname{Post}_{R_{+}^{\overline{+}}}\left(L_{7}\right)$.
(v) Regular The required relation is given by taking the join $R_{5} \circ L_{7}$ of the relations from (iii) and (iv). We saw in lectures that taking the join of regular relations produces a regular relation.
(vi) Regular Let us consider the following variant of $R_{+}$(which must also be regular):

$$
\widehat{R_{+}}:=\left\{\left(n_{1}, m_{1}\right),\left(n_{2}, m_{2}\right),\left(\left(n_{1}, n_{2}\right), m_{1}+m_{2}\right) \mid n_{1}, n_{2}, m_{1}, m_{2} \in \mathbb{N}\right\}
$$

Note that $n_{1}$ and $n_{2}$ are only treated trivially by $\widehat{R_{+}}$(they are copied).
We then get

$$
P:=\{((n, m), 2 n+3 m) \mid n, m \in \mathbb{N}\}=\text { Post }_{\text {Post }_{\overparen{R}}\left(R_{2}\right)}\left(R_{3}\right)
$$

(using $R_{2}$ and $R_{3}$ from part (iii)). Thus $P$ is also regular.
The language $K:=0^{*} 10^{*}$ is regular and encodes the set $\left\{2^{k} \mid k \in \mathbb{N}\right\}$. The required relation is equal to

$$
\operatorname{Pre}_{P}(K)
$$

and is thus regular (using the theorem concerning the preservation of regularity by Pre from the lectures).

