Exercise 1.3

Prove that every DFA recognizing $L_n = \{a^k \mid k \text{ is divisible by } n \text{ or } n-1\}$ has at least $n(n-1)$ states.

Solution:

We prove that $\varepsilon, a, aa, \dots, a^{n(n-1)-1}$ all belong to different residuals, hence there are at least $n(n-1)$ residuals and thus also states.

Consider two arbitrary but different elements a^x, a^{x+d} from above, i.e. we assume

$$0 \le x < x + d < n(n-1)$$

We need to find $z \in \mathbb{N}$ such that exactly one of $a^x a^z, a^{x+d}a^z$ is in L, which proves a^x, a^{x+d} belong to diferent residuals.

Case 1 Neither n nor $n-1$ divides d: let $z = n(n-1) - x$.

> On the one hand $a^x a^z = a^{n(n-1)} \in L$ as n divides $n(n-1)$. On the other hand $a^{x+d}a^z = a^{n(n-1)+d} \notin L$ as n divides $n(n-1)$ but neither d, thus nor their sum.

Case 2 n divides d, but $n-1$ does not: let $z = n(n-1) - x - (d\%(n-1))$. Observe that $z \ge 0$.

> On the one hand $a^x a^z = a^{n(n-1)-(d\%(n-1))} \notin L$ as neither n nor $n-1$ divides $d\%(n-1) < n-1 < n$. On the other hand $a^{x+d}a^z = a^{n(n-1)+d-(d\%(n-1))} \in L$ as $n-1$ divides $d-(d\%(n-1))$.

Case 3 $n-1$ divides d, but n does not: similar.

Case 4 Both $n-1$ and n divide d: cannot happen as $d \le x + d < n(n-1) = \text{lcm}(n, n-1)$.

Homework

Show that $M = \{a^{2^n} \mid n \in \mathbb{N}\}$ is not regular.

Hint: Show that M has infinitely many residuals.