Minimal DFA's for Divisibility Testing (LSB first)

Jez Snelson & Joshua Obayomi

January 27, 2026

1 Introduction

2 Non-Distinguishability Criteria

2.1 Initial ND Criteria

Lemma 2.1. *The strings s_x, s_y are non distinguishable if and only if*
$\forall d \in \mathbb{N}\ r_2(s_x)d + x \equiv 0 \iff r_2(s_y)d + y \equiv 0$

2.2 Revised ND Criteria

Lemma 2.2. *For all $\alpha \in \mathbb{Z}/p\mathbb{Z}$ there exists $\alpha^{-1} \in \mathbb{Z}/p\mathbb{Z}$ if a, p are coprime and $a \neq 0$*

Proof. If we pick a and we have that α and p are coprime we have by Bezout's identity we have that there exists integers x and y such that $\alpha x + py = 1$ which implies that

$$\alpha x + py \equiv \alpha x + 0 \equiv \alpha x \equiv 1 \pmod{p}$$

And so we take $\alpha^{-1} = x$ ◻

Lemma 2.3. *The strings s_x, s_y are non distinguishable if and only if*
$(r_2(s_x))^{-1}x \equiv (r_2(s_y))^{-1}y$ *(mod p)*

3 Equivalence Relation Classes

As we have shown our distinguishability equivalence relation $_{d,p}$ is equivalent to $r_2(s_y)x \equiv r_2(s_x)y \pmod{p}$ and we want to construct our distinguishing set from this which leads us to.

Lemma 3.1. *The amount of equivalence classes under $=_{d,p}$ is exactly p*
Also said as $\Sigma^*/ND = p$

Proof. Firstly since there is only p possible values for the numbers to be congruent to mod p as they are integers we have that the amount of equivalence classes is $\leq p$.
Now all we need to do is find p possible equivalence classes of distinguishability which will force it to be p.
Consider the strings of 0 to $p-1$.
Prepend 0s to the start of these strings to make them all the same length so we have $r_2(s_x) = \alpha$ for all of them.
We then have that they are all distinct under $=_{d,p}$ as for any two such strings $s_x, s_y, x \neq y$ assuming they are non distinguishable we have by 2.3

$$(r_2(s_x))^{-1}x \equiv (r_2(s_y))^{-1}y \pmod{p}$$
$$\alpha^{-1}x \equiv \alpha^{-1}y \pmod{p}$$
$$x \equiv y \pmod{p}$$

This forms a contradiction as we picked them to be distinct numbers between 0 and $p-1$ and so they must all be distinguishable and hence in different equivalence classes.
Thus we have found p distinct equivalence classes and so the amount of equivalence classes is exactly p. $\square$

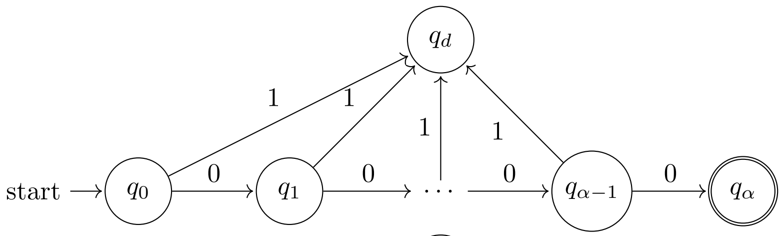
4 Even Numbers

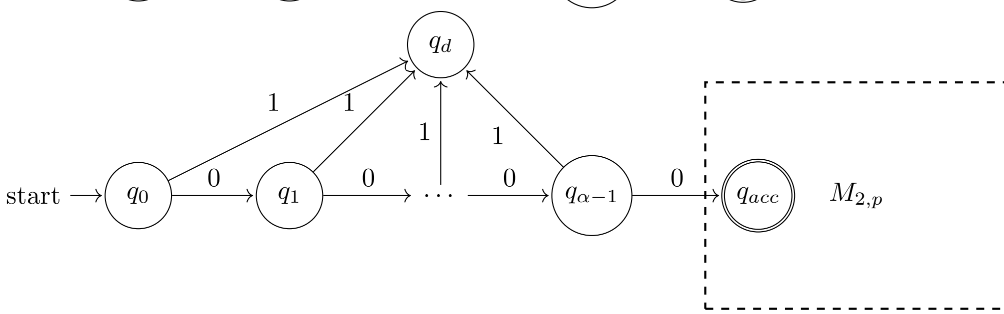
Now we aim to extend our Minimal DFA's to work with even numbers specifically numbers of the form $2^\alpha p$ where $\alpha, p \in \mathbb{N}$ and p is odd.

4.1 Construction

We will construct a proposed minimal DFA

4.1.1 Checking for Divisibility by 2^α





4.2 Proof of it working

4.3 Reachability

4.4 Distinguishability

Lemma 4.1. *For all S_m S_n in the states of $M_{2,2^\alpha p}$ we have that S_m is distinguishable from S_n*

Proof. We split S_m and S_n into cases based on which part of the DFA they are in we consider 3 cases for each of them being the dead state q_d, being any other state in the divisibility by 2^α part $q_l, 0 < l < \alpha - 1$ or being any state in $M_{2,p}$. $\square$