Minimal DFA's for Divisibility Testing (LSB first)

Jez Snelson & Joshua Obayomi

January 24, 2026

1 Introduction

2 Non-Distinguishability Criteria

2.1 Initial ND Criteria

Lemma 2.1. *For all* $Sx, Sy \in \Sigma^*$ $Sx =_{d,p} Sy$ *if and only if* $\forall d \in \mathbb{N}\ r_2(x)d + x \equiv 0 \iff r_2(x)d + y \equiv 0$

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. $(r_2(x))^{-1}x \equiv (r_2(y))^{-1}y$ *(mod p) if and only if* $\forall d \in \mathbb{N}\ r_2(x)d + x \equiv 0 \iff r_2(x)d + y \equiv 0$

3 Equivalence Relation Classes

As we have shown our distinguishability equivalence relation $_{d,p}$ is equivalent to $r_2(y)x \equiv r_2(x)y \pmod{p}$ 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 $|\{[Sx]_{d,p} | Sx \in \Sigma^*\}| = p$

Proof. Firstly since there is only p possible values for the numbers to be congruent to mod 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 so that $\square$

4 Even Numbers