

# Logische Complexiteit

## Myhill–Nerode Stelling

Jeroen Goudsmit

14 februari 2012

De Myhill–Nerode stelling karakteriseert reguliere talen; het hangt aan iedere taal een eigenschap, en die geldt precies wanneer de taal regulier is. Sterker nog, het geeft je een manier om bij iedere reguliere taal de *kleinste* DFA te vinden die de taal herkent. In dit document staat een bewijs van de stelling. Ook zijn er een aantal opgaven in opgenomen.

We beginnen eerst met het introduceren van een specifieke equivalentierelatie op een taal. Herinner je dat een *equivalentierelatie*  $R$  op een verzameling  $A$  een relatie  $R \subseteq A \times A$  is zodanig dat de volgende drie eigenschappen gelden:<sup>1</sup>

- (i) de relatie  $R$  is *reflexief*, dat wil zeggen, voor alle  $x \in A$  geldt  $x R x$ ;
- (ii) de relatie  $R$  is *symmetrisch*, dat wil zeggen, voor alle  $x, y \in A$  geldt  $x R y$  wanneer  $y R x$  geldt;
- (iii) de relatie  $R$  is *transitief*, dat wil zeggen, voor alle  $x, y, z \in A$  geldt dat als  $x R y$  en  $y R z$  waar zijn, dan óók  $x R z$ .

Er zijn tal van voorbeelden van equivalentierelaties. Een heel gemakkelijk voorbeeld is *gelijkheid* op welke verzameling dan ook. Het is inderdaad niet lastig om te zien dat  $=$  reflexief, symmetrisch en transitief is. Hier een paar voorbeelden.

**Voorbeeld 1** (Even en Oneven). Bekijk de natuurlijke getallen  $\mathbb{N} = \{0, 1, 2, \dots\}$  en definieer  $R$  als:

$$x R y \text{ dan en slechts dan als } x + y \text{ is even.}$$

Heel concreet zien we dat  $0 R 2$  geldt, want  $0 + 2 = 2$  is even. Iets algemener geldt ook  $2 \cdot n R 2 \cdot m$ , want  $2 \cdot n + 2 \cdot m = 2 \cdot (n + m)$ . Kortom: alle even getallen zijn *equivalent* onder  $R$ .

Laten we nu één voor één de eigenschappen nagaan. Deze relatie is reflexief, want  $x + x = 2 \cdot x$  is even, dus  $x R x$  geldt voor alle  $x \in \mathbb{N}$ . De relatie is symmetrisch, want als  $y R x$  geldt dan is  $y + x$  even. Maar dit is gelijk aan  $x + y$ , wat dus ook even is. Hiermee geldt  $x R y$ . Als laatste gaan we na dat de relatie transitief is, dus neem aan dat  $x R y$  en  $y R z$  geldt. Nu weten we dus dat  $x + y$  even is, en  $y + z$  is ook even. Bekijk nu de som  $(x + y) + (y + z) = x + 2 \cdot y + z$ , die natuurlijk ook even is (want even plus even is even). Hier trekken we een even getal,  $2 \cdot y$ , van af, wat weer een even getal geeft, namelijk  $x + z$ . Dit maakt dat  $x R z$  geldt.

Zijn er ook niet-equivalente getallen? Jazeker, bijvoorbeeld 0 en 1. Immers, als  $0 R 1$  zou gelden, dan moest  $0 + 1 = 1$  even zijn, maar dat is het zeker niet. Overtuig jezelf er van dat alle even getallen equivalent zijn, en alle oneven getallen ook, maar geen enkel even getal is equivalent met een oneven getal.

**Voorbeeld 2** (Even en Oneven Rijtjes). Bekijk het alfabet  $\Sigma = \{a\}$ , en definieer een equivalentierelatie  $R$  op  $\Sigma^*$  als

$$u R v \text{ dan en slechts van als } \text{de lengte van } uv \text{ is even.}$$

---

<sup>1</sup>We schrijven  $x R y$ , en begrijp dat dit betekent dat  $x$  in relatie staat met  $y$  via  $R$ , ook wel te schrijven als  $\langle x, y \rangle \in R$ .

Ook hier kunnen we kijken wat dit concreet betekent. Zie dat  $\varepsilon R aa$ , want  $\varepsilon aa = aa$  heeft een even lengte. Algemeener, alle rijtjes van even lengte zijn met elkaar equivalent, en zo ook alle rijtjes van oneven lengte. Natuurlijk zijn  $a$  en  $\varepsilon$  niet equivalent. Het is gemakkelijk na te gaan dat dit een equivalentierelatie is, op een manier die sterk lijkt op het bewijs in Voorbeeld 1.

**Voorbeeld 3 (Tellen).** Bekijk nu de verzameling  $A = \{0, 1\}^*$ . We kunnen zeggen dat  $x R y$  voor  $x, y \in A$  als er in  $x$  en  $y$  evenveel 0'en zitten. Zo gelden  $101 R 01111$  en  $11111111 R 1$ , maar  $0 R 1$  geldt niet. Ook deze relatie  $R$  is een equivalentierelatie. In  $x$  zitten evenveel nullen als in  $x$ , dus  $x R x$  geldt. Als  $y R x$  geldt, dan zitten er evenveel nullen in  $y$  als in  $x$ , dus ook in  $x$  als in  $y$ . Dit betekent op z'n beurt dat  $x R y$  geldt. Transitiviteit kun je op soortgelijke wijze controleren.

Merk op dat  $\varepsilon R 0$  niet geldt, evenzo gelden  $0 R 00$ ,  $00 R 000$ , ... niet. Er zijn dus oneindig veel niet-equivalente woorden!

Voor we naar het volgende voorbeeld gaan kijken, nemen we even een stap terug. Bij een equivalentierelatie  $R$  kunnen we ons afvragen welke dingen allemaal *equivalent* worden. Neem Voorbeeld 1 in gedachten. We weten daar dat alle even getallen equivalent zijn, en alle oneven getallen zijn dat ook. Dit betekent in het bijzonder dat alle even getallen equivalent zijn aan 0. In het algemeen kunnen we kijken naar alle dingen equivalent aan een zeker element. Dit geeft een verzameling, en deze verzameling noemen we de *equivalentieklasse* van dat gekozen element. Concreet, de equivalentieklasse van 0 in Voorbeeld 1 is  $\{0, 2, 4, \dots\}$ . De equivalentieklasse van 0 in Voorbeeld 3 echter is  $\{\varepsilon, 1, 11, \dots\}$ . We schrijven  $x/R$  voor de equivalentieklasse van  $x$  onder  $R$ , en definiëren dit formeel als de volgende verzameling:

$$x/R := \{y \in A \mid x R y\}.$$

Een equivalentieklasse  $p \in A/R$  is bij definitie altijd gelijk aan  $\{y \in A \mid x R y\}$  voor een zekere  $x \in A$ . Zo'n  $x$  noemen we een *representant* van  $p$ . Er zijn vaak meerdere representanten van een equivalentieklasse. Zo kunnen we bij Voorbeeld 1 de equivalentieklasse  $\{0, 2, 4, \dots\}$  representeren door ieder even getal. Dus 0 is een representant, maar 12 en  $2^{387}$  zijn ook representanten. Representanten zijn dus gewoon elementen uit de equivalentieklasse, dus ze zijn altijd equivalent.

Herinner je dat een *partitie* van een verzameling  $A$  een verzameling  $P$  van deelverzamelingen van  $A$  is zó dat de volgende eigenschappen gelden:

- (i) de partitie  $P$  *overdekt*  $A$ , in dat de vereniging van  $P$  gelijk is aan  $A$
- (ii) de partitie  $P$  is *paarsgewijs disjunct*, wat wilt zeggen dat als  $p, q \in P$  dan  $p \cap q$  is leeg wanneer  $p \neq q$ ;
- (iii) de partitie  $P$  bevat niet de lege verzameling.

Dit geeft aanleiding tot het volgende lemma:

**Lemma 1.** Zij  $R$  een equivalentierelatie op  $A$ . Nu is de verzameling  $A/R := \{x/R \mid x \in A\}$  der equivalentieklassen van  $R$  een partitie op  $A$ .

*Bewijs.* We moeten bewijzen dat  $A/R$  voldoet aan de drie eisen van een partitie, laten we dat gewoon stap voor stap doen. Als eerste pakken we (i) aan. Er geldt  $\bigcup A/R \subseteq A$ , omdat  $x/R \subseteq A$  voor alle  $x \in A$ , wat direct volgt uit het feit dat  $R$  een relatie is op  $A$ . Als we nu kunnen laten zien dat  $A \subseteq \bigcup A/R$  dan zijn we klaar. Neem dus een  $x \in A$ , als er nu een equivalentieklasse is waar  $x$  in bevat zit dan klopt 't. Maar dat is geen zware taak, want  $x R x$  geldt wegens reflexiviteit, dus  $x \in x/R$ .

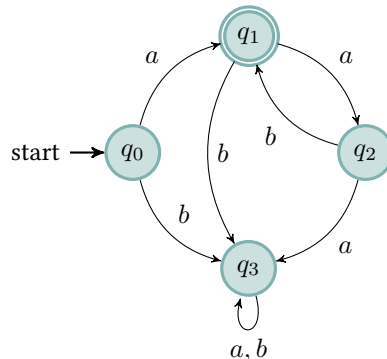
Neem nu  $p, q \in A/R$ . Dit betekent dat  $p = x/R$  en  $q = z/R$  voor zekere representanten  $x, z \in A$ . Overtuig jezelf er van dat we klaar zijn indien we kunnen aantonen dat  $x R z$  geldt. Stel nu dat er iets zit in de doorsnede van  $p$  en  $q$ , en noem dat ding  $y$ . Dit betekent dus dat  $y \in x/R$  en  $y \in z/R$ , waarmee  $y R y$  en  $z R y$  gelden. Symmetrie geeft dat  $y R z$ , en transitiviteit zorgt ervoor dat  $x R z$ .

Stel nu dat  $\emptyset \in A/R$ , dan is  $\emptyset$  een lege equivalentieklasse. Dit betekent dat er een  $x \in A$  is zo dat  $x/R = \emptyset$ . Maar dat kan helemaal niet, want  $x \in x/R$ , een tegenspraak. Dus  $\emptyset \notin A/R$ .  $\square$

We kunnen nu heel concreet kijken naar de partities die horen bij de equivalentierelaties die we nu al kennen.

**Voorbeeld 1**  $\mathbb{N}/R = \{0/R, 1/R, 2/R, 3/R, \dots\} = \{0/R, 1/R\} = \{\text{even getallen}, \text{oneven getallen}\}.$

**Voorbeeld 3**  $\Sigma^*/R = \{\text{woorden zonder nullen}, \text{woorden met één nul}, \text{woorden met twee nullen}, \dots\}.$



Figuur 1: Zomaar een DFA.

**Voorbeeld 4.** Bekijk de DFA  $M$  van Figuur 1. We definiëren nu een relatie  $\approx$  op  $\Sigma^*$  als volgt:

$x \approx y$  dan en slechts dan als  $x$  uitvoeren op  $M$  dezelfde toestand geeft als  $y$  uitvoeren.

Laten we eerst een concreet kijken naar wat er hier gebeurt. We maken een relatie  $\approx$  op  $\Sigma^*$ , en  $\Sigma^*$  is de verzameling

$$\{\varepsilon, a, b, aa, ab, ba, bb, aaa, \dots\}.$$

Als we  $\varepsilon$  nemen en dat uitvoeren op de automaat in Figuur 1 dan komen we op  $q_0$ . Wanneer we  $a$  nemen dan geeft dat  $q_1$ , en  $aab$  geeft dat ook. Uit onze definitie volgt nu dus dat  $a \approx aab$ . Zie ook dat  $\varepsilon \not\approx a$ , omdat  $\varepsilon$  een andere toestand geeft dan  $a$ .

Is deze relatie  $\approx$  een equivalentierelatie? Zeker weten, en dat kunnen we gewoon nagaan. Reflexiviteit is duidelijk, immers  $xw$  geeft dezelfde toestand als  $xw$ . Symmetrie en transitiviteit kun je zelf controleren.

Hoeveel equivalentieklassen heeft  $\approx$ ? Hooguit evenveel als  $Q$  groot is. Dit gaan we zometeen bewijzen.

Het laatste voorbeeld kunnen we iets algemener maken. We gebruiken immers helemaal niets specifiek aan de DFA in Figuur 1, maar alleen dat het ding in Figuur 1 een DFA is.

**Definitie 1.** Als  $M = \langle Q, \Sigma, \delta, q_0, F \rangle$  een DFA is dan definiëren we de relatie  $\approx$  op  $\Sigma^*$  als volgt:

$x \approx y$  dan en slechts dan als  $x$  uitvoeren op  $M$  dezelfde toestand geeft als  $y$  uitvoeren.

**Lemma 2.** Voor elke DFA  $M = \langle Q, \Sigma, \delta, q_0, F \rangle$  geldt dat de bijbehorende equivalentierelatie  $\approx$  hooguit zoveel equivalentieklassen heeft als er toestanden zijn.

*Bewijs.* We bewijzen dit door per ieder woord in  $\Sigma^*$  een toestand aan te wijzen, op zo'n manier dat de aangewezen toestanden van twee woorden hetzelfde zijn precies wanneer de woorden equivalent zijn. Dit laat zien dat er per toestand hooguit een equivalentieklasse is, en dat wilde we laten zien.

Merk op dat we een woord  $w \in \Sigma^*$  kunnen sturen naar de toestand  $Q$  waar  $M$  in komt na het uitvoeren van  $w$ . Als  $w \equiv v$  dan is de toestand waar  $w$  in uitkomt dezelfde als die van  $v$ . Hiermee hebben we dus per equivalentieklasse één toestand aangewezen. Stel nu dat  $w$  en  $v$  naar dezelfde toestand wijzen. Dan moet het zo zijn dat  $w \approx v$ , want  $w$  en  $v$  geven dezelfde toestand na het uitvoeren op  $M$ . Dit bewijst wat we wilde bewijzen.  $\square$

Gegeven een willekeurige taal  $\mathcal{L}$  op alfabet  $\Sigma$  kunnen we een equivalentierelatie  $\equiv$  maken op  $\Sigma^*$  als volgt:

$$u \equiv v \quad \text{dan en slechts dan als} \quad \text{voor alle } w \in \Sigma^* \text{ geldt } uw \in \mathcal{L} \text{ precies als } vw \in \mathcal{L} \quad (1)$$

Als je een DFA  $M$  op het alfabet  $\Sigma$  hebt zijn er nu twee equivalentierelaties op  $\Sigma^*$ , namelijk  $\approx$  en  $\equiv$ . We kunnen heel cryptisch zeggen  $\approx \subseteq \equiv$ , wat betekent dat als  $u \approx v$  dan ook  $u \equiv v$ . Ga voor jezelf na dat dit betekent dat  $\Sigma^*/\approx$  altijd hoogstens zo groot is als  $\Sigma^*/\equiv$ .

Bij een equivalentierelatie  $R$  op  $\Sigma^*$  en een deelverzameling  $S \subseteq \Sigma^*$  kunnen we ook een DFA maken, en wel op de volgende wijze.

- De verzameling toestanden  $Q$  wordt  $\Sigma^*/R$ ;
- Het alfabet is vanzelfsprekend gewoon  $\Sigma$ ;
- De transitiefunctie  $\delta : Q \times \Sigma \rightarrow Q$  stuurt  $\langle w/R, x \rangle$  naar  $wx/R$ ;
- De begintoestand  $q_0$  is  $\varepsilon/R$ ;
- De eindtoestanden  $F$  zijn  $\{w/R \mid w \in S\}$ .

Laten we deze truc eens gebruiken op de equivalentierelatie  $R$  als gedefinieerd in Voorbeeld 2. De equivalentie-  
klassen van  $\Sigma^*$  onder  $R$  zijn  $\varepsilon/R = \{\varepsilon, aa, aaaa, \dots\}$  en  $a/R = \{a, aaa, aaaaa, \dots\}$ , dus de toestanden worden  
 $Q = \{\varepsilon/R, a/R\}$ . De transitiefunctie stuurt  $\langle \varepsilon, a \rangle$  naar  $a/R$  en  $\langle a/R, a \rangle$  naar  $aa/R = \varepsilon/R$ . De begintoestand  
is  $\varepsilon/R$ .

Denk nu terug aan opgave Voorbeeld 4. We hebben hier een DFA, dus we hebben de equivalentierelatie  $\approx$ . Maar  
de DFA definieert natuurlijk een taal, dus we hebben ook de equivalentierelatie  $\equiv$  die hoort bij  $\mathcal{L}(M)$ . Wat zijn  
de equivalentieklassen van deze twee relaties? Hieronder staan de klassen van  $\approx$ , je kunt gemakkelijk nagaan  
dat dit klopt.

$$\Sigma^*/\approx = \left\{ \{\varepsilon\}, \{a(ab)^i \mid i \in \mathbb{N}\}, \{bw \mid w \in \Sigma^*\}, \{aa(ba)^i \mid i \in \mathbb{N}\} \right\} \quad (2)$$

Dit zijn ook de equivalentieklassen van  $\equiv$ . Alles wat onder  $\approx$  equivalent is, is dat ook onder  $\equiv$ . We hoeven  
dus alleen te laten zien dat de klassen onderling *niet* equivalent zijn met  $\equiv$ . Bekijk hiervoor de volgende ta-  
bel.

| $x/y$         | $\varepsilon$ | $a$           | $b$           | $aa$ |
|---------------|---------------|---------------|---------------|------|
| $\varepsilon$ | $\varepsilon$ | $a$           | $b$           |      |
| $a$           | $\varepsilon$ | $\varepsilon$ | $\varepsilon$ |      |
| $b$           | $a$           | $\varepsilon$ |               | $b$  |
| $aa$          | $b$           | $\varepsilon$ | $b$           |      |

Horizontaal en verticaal zijn representanten van de klassen van  $\approx$  gegeven, zoals je gemakkelijk kan teruglezen  
uit (2). Voor  $x$  en  $y$  die ongelijke klassen (onder  $\approx$ ) representeren is er een woord  $w \in \Sigma^*$  gegeven zó dat “ $xw \in \mathcal{L}$   
dan en slechts dan als  $yw \in \mathcal{L}$ ” niet geldt. Zo zie je dat  $a\varepsilon = a \in \mathcal{L}$ , maar  $\varepsilon\varepsilon = \varepsilon \notin \mathcal{L}$ , en ook dat  $aab \in \mathcal{L}$ , maar  
 $\varepsilon b = b \notin \mathcal{L}$ . Dit toont dus aan dat  $x \not\approx y$  impliceert  $x \not\equiv y$ . Eigenlijk hadden we alles onder de diagonaal weg  
kunnen laten, want als  $x \not\equiv y$  dan  $y \not\equiv x$ . Merk op dat dit laat zien dat de DFA in Figuur 1 de kleinste DFA is die  
 $\mathcal{L}(M)$  herkent!

Met al het bovenstaande hebben we nu de benodigde machinerie om de Myhill–Nerode stelling te bewijzen.

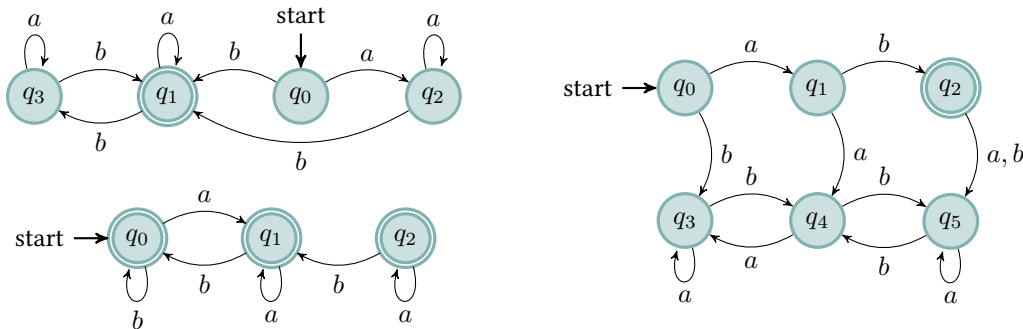
**Theorem 1** (Myhill–Nerode). *Zij  $\mathcal{L}$  een taal over het alfabet  $\Sigma^*$ , en schrijf  $\equiv$  voor de bijbehorende equivalentiere-  
latie als in (1). De taal  $\mathcal{L}$  is regulier dan en slechts dan als  $\Sigma^*/\equiv$  eindig is.*

*Bewijs.* Stel dat  $\mathcal{L}$  regulier is. Dit geeft een DFA  $M$  zodanig dat  $\mathcal{L} = \mathcal{L}(M)$ . Dan weten we dat  $\Sigma^*$  hoogstens  
zoveel equivalentieklassen onder  $\equiv$  heeft als het heeft onder  $\approx$ . Maar er zijn hoogstens zoveel equivalentieklassen  
onder  $\approx$  als  $M$  toestanden heeft, en dit getal is altijd eindig. Dit bewijst de ene richting.

Nu bekijken we de andere richting, dus neem aan dat  $\Sigma^*/\equiv$  eindig is. Neem  $S := \mathcal{L}$  en bekijk de DFA  $M =$   
 $\langle Q, \Sigma, \delta, q_0, F \rangle$  die hoort bij  $\equiv$  en  $S$ . We claimen dat  $\mathcal{L}(M) = \mathcal{L}$ . Natuurlijk geldt  $w \in \mathcal{L}(M)$  dan en slechts  
dan als  $\delta^\bullet(w)(q_0) \in F$ . Met inductie langs de lengte van  $w$  is het gemakkelijk te bewijzen dat  $\delta^\bullet(w)(q_0) = w/\equiv$ .  
En omdat  $F = \{u/\equiv \mid u \in \mathcal{L}\}$  volgt het gewenste hier direct uit.  $\square$

## Opgave 1 — Equivalentieklassen

Geef de equivalentieklassen van  $\approx$  en  $\equiv$  voor de volgende drie automaten.



## Opgave 2 — Veelvouden

Neem het alfabet  $\Sigma = \{0, 1\}$ . Een woord  $w \in \Sigma^*$  lijkt erg veel op een binair getal, het enige verschil is dat woorden in op  $\Sigma$  kunnen beginnen met meer dan een nullen. Zo staat 0 voor 0, 1 voor 1, 10 voor 2 en 11111011100 voor 2012. Per natuurlijk getal  $n$  kunnen de onderstaande taal definiëren.

$$\mathcal{L}_n = \{w \in \Sigma^* \mid w \text{ als binair getal stelt een } n\text{-voud voor}\}.$$

- Geef de equivalentieklassen van  $\mathcal{L}_n$  onder  $\equiv$ .
- Laat zien dat  $|\mathcal{L}_n / \equiv| = n$  voor alle  $n \geq 1$ .
- Bewijs dat  $\mathcal{L}_n$  regulier is voor alle  $n \in \mathbb{N}$ .
- Bewijs nu voor  $n \geq 1$  dat er geen enkele DFA is met hooguit  $n - 1$  toestanden die  $\mathcal{L}_n$  herkent.

## Opgave 3 — Is 't Regulier?

Hieronder zijn een aantal talen gegeven, allen over het alfabet  $\Sigma = \{a, b\}$ . Bewijs of ze al dan niet regulier zijn middels de Myhill–Nerode stelling. Als de taal regulier is, geef dan ook de DFA die je van de Myhill–Nerode stelling krijgt.

$$\begin{aligned} \mathcal{L}_1 &= \{a^i b^i \mid i \in \mathbb{N}\} \\ \mathcal{L}_2 &= \{w \in \Sigma^* \mid w \text{ begint met } ab\} \\ \mathcal{L}_3 &= \{w \in \Sigma^* \mid w \text{ eindigt op } ab\} \\ \mathcal{L}_4 &= \{w \in \Sigma^* \mid w \text{ bevat meer } a\text{'s dan } b\text{'s}\} \\ \mathcal{L}_5 &= \{w \in \Sigma^* \mid w \text{ bevat een even aantal } b\text{'s}\} \\ \mathcal{L}_6 &= \{a^i b^j a^k \mid i, j, k \in \mathbb{N} \text{ en als } i = 1 \text{ dan } i = j\} \end{aligned}$$