The Myhill-Nerode Theorem
(lecture 20)

Isomorphism of DFAs

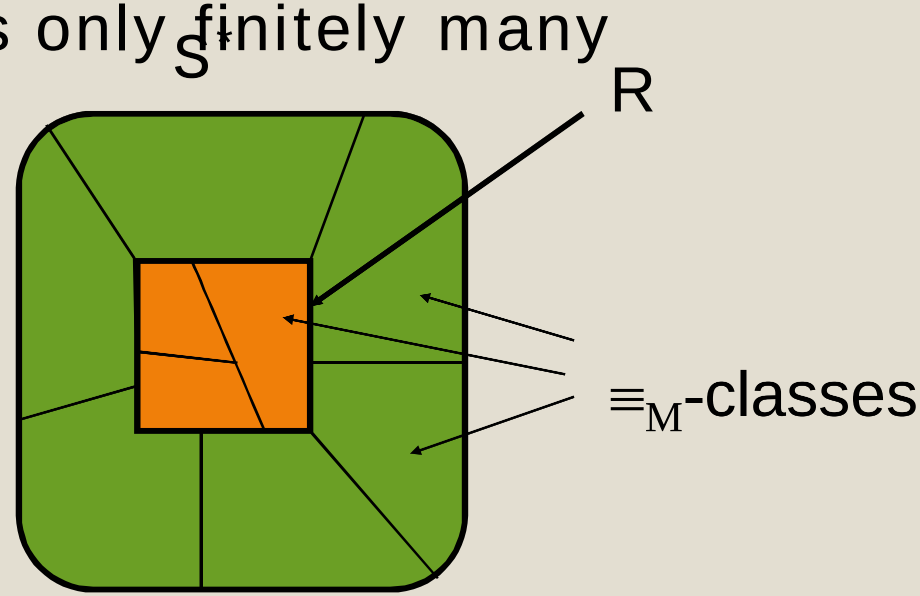
- $M = (Q_M, S, d_M, s_M, F_M)$, $N = (Q_N, S, d_N, s_N, F_N)$: two DFAs
- M and N are said to be isomorphic if there is a (structure-preserving) bijection $f: Q_M \to Q_N$ s.t.
  - $f(s_M) = s_N$
  - $f(d_M(p,a)) = d_N(f(p),a)$ for all $p \in Q_M$, $a \in S$
  - $p \in F_M$ iff $f(p) \in F_N$.
- I.e., M and N are essentially the same machine up to renaming of states.
- Facts:
  - 1. Isomorphic DFAs accept the same set.
  - 2. if M and N are any two DFAs w/o inaccessible states accepting the same set, then the quotient automata $M/\approx$ and $N/\approx$ are isomorphic
  - 3. The DFA obtained by the minimization algorithm (lec. 14) is the minimal DFA for the set it accepts, and this DFA is unique up to isomorphism.

Myhill-Nerode Relations

- R: a regular set, M=(Q, S, d,s,F): a DFA for R w/o inaccessible states.
- M induces an equivalence relation $\equiv_M$ on S* defined by
  - x $\equiv_M$ y iff D(s,x) = D (s,y).
  - i.e., two strings x and y are equivalent iff it is indistinguishable by running M on them (i.e., by running M with x and y as input, respectively, from the initial state of M.)
- Properties of $\equiv_M$:
  - 0. $\equiv_M$ is an equivalence relation on S*.
    (cf: $\approx$ is an equivalence relation on states)
  - 1. $\equiv_M$ is a right congruence relation on S*: i.e., for any x,y $\in$ S* and a $\in$ S, x $\equiv_M$ y => xa $\equiv_M$ ya.
  - pf: if x $\equiv_M$ y => D(s,xa) = d(D (s,x),a) = d(D (s,y),a) = D(s, ya)
    => xa $\equiv_M$ ya.

Properties of the Myhill-Nerode relations

- Properties of $\equiv_M$:
  - 2. $\equiv_M$ refines R. I.e., for any x,y $\in$ S*,
  - $x \equiv_M y \Rightarrow x \in R$ iff $y \in R$
  - pf: $x \in R$ iff $D(s,x) \in F$ iff $D(s,y) \in F$ iff $y \in R$.
  - Property 2 means that every $\equiv_M$-class has either all its elements in R or none of its elements in R. Hence R is a union of some $\equiv_M$-classes.
  - 3. It is of finite index, i.e., it has only finitely many equivalence classes.
  - (i.e., the set { $[x]_{\equiv_M}$ | $x \in S^*$ }
  - is finite.
  - pf: $x \equiv_M y$ iff $D(s,x) = D(s,y) = q$
  - for some $q \in Q$. Since there
  - are only |Q| states, hence
  - S* has |Q| $\equiv_M$-classes



Definition of the Myhill-Nerode relation

- $\equiv$: an equivalence relation on S*,
  R: a language over S^*.
- $\equiv$ is called an Myhill-Nerode relation for R if it satisfies property 1~3. i.e., it is a right congruence of finite index refining R.
- Fact: R is regular iff it has a Myhill-Nerode relation.
  - (to be proved later)
  - 1. For any DFA M accepting R, $\equiv_M$ is a Myhill-Nerode relation for R
  - 2. If $\equiv$ is a Myhill-Nerode relation for R then there is a DFA $M_\equiv$ accepting R.
  - 3. The constructions $M \rightarrow \equiv_M$ and $\equiv \rightarrow M_\equiv$ are inverse up to isomorphism of automata. (i.e. $\equiv = \equiv_{M_\equiv}$ and $M = M_{\equiv_M}$)

From ≡ to M≡

- R: a language over S, ≡ : a Myhill-Nerode relation for R;
  - the ≡-class of the string x is $[x]_{\equiv} =_{def} \{y \mid x \equiv y\}$.
  - Note: Although there are infinitely many strings, there are only finitely many ≡ -classes. (by property of finite index)
- Define DFA M≡ = (Q,S,d,s,F) where
  - Q = { [x] | x ∈ S* },   s = [e],
  - F = { [x] | x ∈ R },   d([x],a) = [xa].
- Notes:
  - 0: $M_{\equiv}$ has |Q| states, each corresponding to an ≡ -class of ≡. Hence the more classes ≡ has, the more states M≡ has.
  - 1. By right congruence of ≡ , d is well-defined, since, if y,z ∈[x] => y ≡ z ≡ x => ya ≡ za ≡ xa => ya, za ∈ [xa]
  - 2. x ∈ R iff [x] ∈ F.
  - pf: =>: by definition of M≡ ;
  - <=: [x] ∈ F => $y s.t. y ∈ R and x ≡ y => x ∈ R. (property 2)

$M \rightarrow \equiv_M$ and $\equiv \rightarrow M_\equiv$ are inverses

Lemma 15.1: $D([x],y) = [xy]$

pf: Induction on $|y|$. Basis: $D([x],e) = [x] = [xe]$.

Ind. step: $D([x],ya) = d(D([x],y),a) = d([xy],a) = [xya]$. QED

Theorem 15.2: $L(M_\equiv) = R$.

pf: $x \in L(M_\equiv)$ iff $D([e],x) \in F$ iff $[x] \in F$ iff $x \in R$. QED

Lemma 15.3: $\equiv$: a Myhill-Nerode relation for R, M: a DFA for R w/o inaccessible states, then

1. if we apply the construction $\equiv \rightarrow M_\equiv$ to $\equiv$ and then apply $M \rightarrow \equiv_M$ to the result, the resulting relation $\equiv_{M_\equiv}$ is identical to $\equiv$.
2. if we apply the construction $M \rightarrow \equiv_M$ to M and then apply $\equiv \rightarrow M_\equiv$ to the result, the resulting relation $M_{\equiv_M}$ is identical to M.

$M \to \equiv_M$ and $\equiv \to M_\equiv$ are inverses (cont'd)

Pf: (of lemma 15.3) (1) Let $M_\equiv$ =(Q,S,d,s,F) be the DFA constructed as described above. then for any x,y in S*,

$x \equiv_{M_\equiv} y$ iff D([e], x) = D([e],y) iff [x] = [y] iff $x \equiv y$.

(2) Let M = (Q, S ,d,s,F) and let $M_{\equiv_M}$ = (Q', S , d',s',F'). Recall that

- [x] = {y | $y \equiv_M x$} = {y | D(s,y) = D(s,x) }
- Q' = {[x] | $x \in S^*$}, s' = [e], F' = {[x] | $x \in R$}
- d'([x], a) = [xa].

Now let f:Q'-> Q be defined by f([x]) = D(s,x).

- 1. By def., [x] = [y] iff D(s,x) = D(s,y), so f is well-defined and 1-1. Since M has no inaccessible state, f is onto.
- 2. f(s') = f([e]) = D(s, e) = s
- 3. [x] $\in$ F' <=> $x \in R$ <=> D(s,x) $\in$ F <=> f([x]) $\in$ F.
- 4. f(d'([x],a)) = f([xa]) = D(s,xa) = d(D(s,x),a) = d(f([x]), a)
- By 1~4, f is an isomorphism from $M_{\equiv_M}$ to M. QED

Relations b/t DFAs and Myhill-Nerode relations

Theorem 15.4: R: a regular set over S. Then up to isomorphism of FAs, there is a 1-1 correspondence b/t DFAs w/o inaccessible states accepting R and Myhill-Nerode relations for R.

- I.e., Different DFAs accepting R correspond to different Myhill-Nerode relations for R, and vice versa.
- We now show that there exists a coarsest Myhill-Neorde relation $\equiv_R$ for any R, which corresponds to the unique minimal DFA for R.

Def 16.1: $\equiv_1$, $\equiv_2$: two relations. If $\equiv_1 \subseteq \equiv_2$ (i.e., for all x,y, x $\equiv_1$ y => x $\equiv_2$ y) we say $\equiv_1$ refines $\equiv_2$.

Note:1. If $\equiv_1$ and $\equiv_2$ are equivalence relations, then $\equiv_1$ refines $\equiv_2$ iff every $\equiv_1$-class is included in a $\equiv_2$-class.

2. The refinement relation on equivalence relations is a partial order. (since $\subseteq$ is ref, transitive and antisymmetric).

The refinement relation

Note:

3. If , $\equiv_1 \subseteq \equiv_2$,we say $\equiv_1$ is the finer and $\equiv_2$ is the coarser of the two relations.
4. The finest equivalence relation on a set U is the identity relation $I_U = \{(x,x) \mid x \in U\}$
5. The coarsest equivalence relation on a set U is universal relation $U^2 = \{(x,y) \mid x, y \in U\}$

Def. 16.1: R: a language over S (possibly not regular). Define a relation $\equiv_R$ over S* by

$$x \equiv_R y \text{ iff for all } z \in S^* \ (xz \in R <=> yz \in R)$$

i.e., x and y are related iff whenever appending the same string to both of them, the resulting two strings are either both in R or both not in R.

Properties of $\equiv_R$

Lemma 16.2: Properties of $\equiv_R$:

- 0. $\equiv_R$ is an equivalence relation over S*.
- 1. $\equiv_R$ is right congruent
- 2. $\equiv_R$ refines R.
- 3. $\equiv_R$ the coarsest of all relations satisfying 0,1 and 2.
- [4. If R is regular => $\equiv_R$ is of finite index.]

Pf: (0) : trivial; (4) immediate from (3) and theorem 15.2.

(1) $x \equiv_R y$ => for all $z \in S^*$ ($xz \in R$ <=> $yz \in R$)

=> $\forall a \forall w$ ($xaw \in R$ <=> $yaw \in R$)

=> $\forall a$ ($xa \equiv_R ya$)

(2) $x \equiv_R y$ => ($x \in R$ <=> $y \in R$)

(3) Let $\equiv$ be any relation satisfying 0~2. Then

$x \equiv y$ => $\forall z\ xz \equiv yz$ --- by ind. on |z| using property (1)

=> $\forall z$ ($xz \in R$ <=> $yz \in R$) --- by (2) => $x \equiv_R y$.

Myhill-Nerode theorem

Thorem16.3: Let R be any language over S. Then the following statements are equivalent:

(a) R is regular;

(b) There exists a Myhill-Nerode relation for R;

(c) the relation $\equiv_R$ is of finite index.

pf: (a) =>(b) : Let M be any DFA for R. The construction $M \rightarrow \equiv_M$ produces a Myhill-Nerode relation for R.

(b) => (c): By lemma 16.2, any Myhill-Nerode relation for R is of finite index and refines R => $\equiv_R$ is of finite index.

(c)=>(a): If $\equiv_R$ is of finite index, by lemma 16.2, it is a Myhill-Nerode relation for R, and the construction $\equiv \rightarrow M_\equiv$ produce a DFA for R.

Relations b/t $\equiv_R$ and collapsed machine

Note: 1. Since $\equiv_R$ is the coarsest Myhill-Nerode relation for a regular set R, it corresponds to the DFA for R with the fewest states among all DFAs for R.

(i.e., let M = (Q,…) be any DFA for R and M = (Q',…) the DFA induced by $\equiv_R$, where Q' = the set of all $\equiv_R$-classes

==> |Q| = | the set of $\equiv_M$-classes | >= | the set of $\equiv_R$ -classes |

= |Q'|.

Fact: M=(Q,S,s,d,F): a DFA for R that has been collapsed (i.e., M = M/≈). Then $\equiv_R = \equiv_M$ (hence M is the unique DFA for R with the fewest states).

pf: x $\equiv_R$ y iff $\forall$ z $\in$ S* (xz $\in$ R <=> yz $\in$ R)

iff $\forall$ z $\in$ S* (D(s,xz) $\in$ F <=> D(s,yz) $\in$ F)

iff $\forall$ z $\in$ S* (D(D(s,x),z) $\in$ F <=> D(D(s,y),z) $\in$ F)

iff D(s,x) ≈ D(s,y) iff D(s,x) = D(s,y) -- since M is collapsed

iff x $\equiv_M$ y Q.E.D.

An application of the Myhill-Nerode relation

- Can be used to determine whether a set R is regular by determining the number of $\equiv_R$ -classes.
- Ex: Let $A = \{a^n b^n \mid n \geq 0\}$.
  - If $k \neq m$ => a^k not $\equiv_A$ a^m, since $a^k b^k \in A$ but $a^m b^k \notin A$.

    Hence $\equiv_A$ is not of finite index => A is not regular.
  - In fact $\equiv_A$ has the following $\equiv_A$-classes:
  - $G_k = \{a^k\}, k \geq 0$
  - $H_k = \{a^{n+k} b^n \mid n \geq 1\}, k \geq 0$
  - $E = S^* - \bigcup_{k \geq 0} (G_k \cup H_k) = S^* - \{a^m b^n \mid m \geq n \geq 0\}$

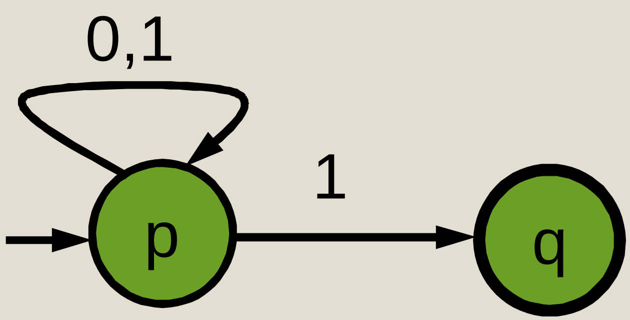
Minimal NFAs are not unique up to isomorphism

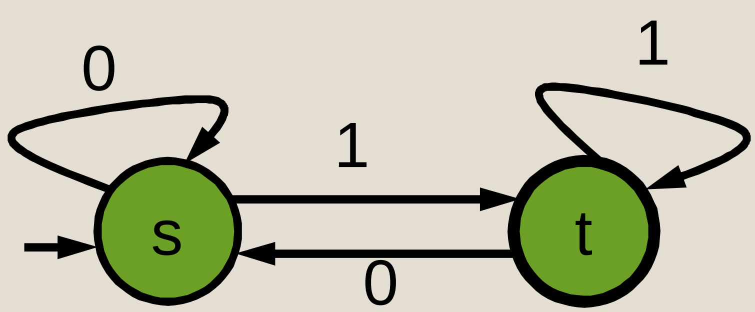
- Example: let L = { x1 | x ∈ {0,1} }*

1. What is the minimum number k of states of all FAs accepting L ?

Analysis : k ≠ 1. Why ?

2. Both of the following two 2-states FAs accept L.





Collapsing NFAs

- Minimal NFAs are not unique up to isomorphism
- Part of the Myhill-Nerode theorem generalize to NFAs based on the notion of *bisimulation.*
- *Bisimulation:*

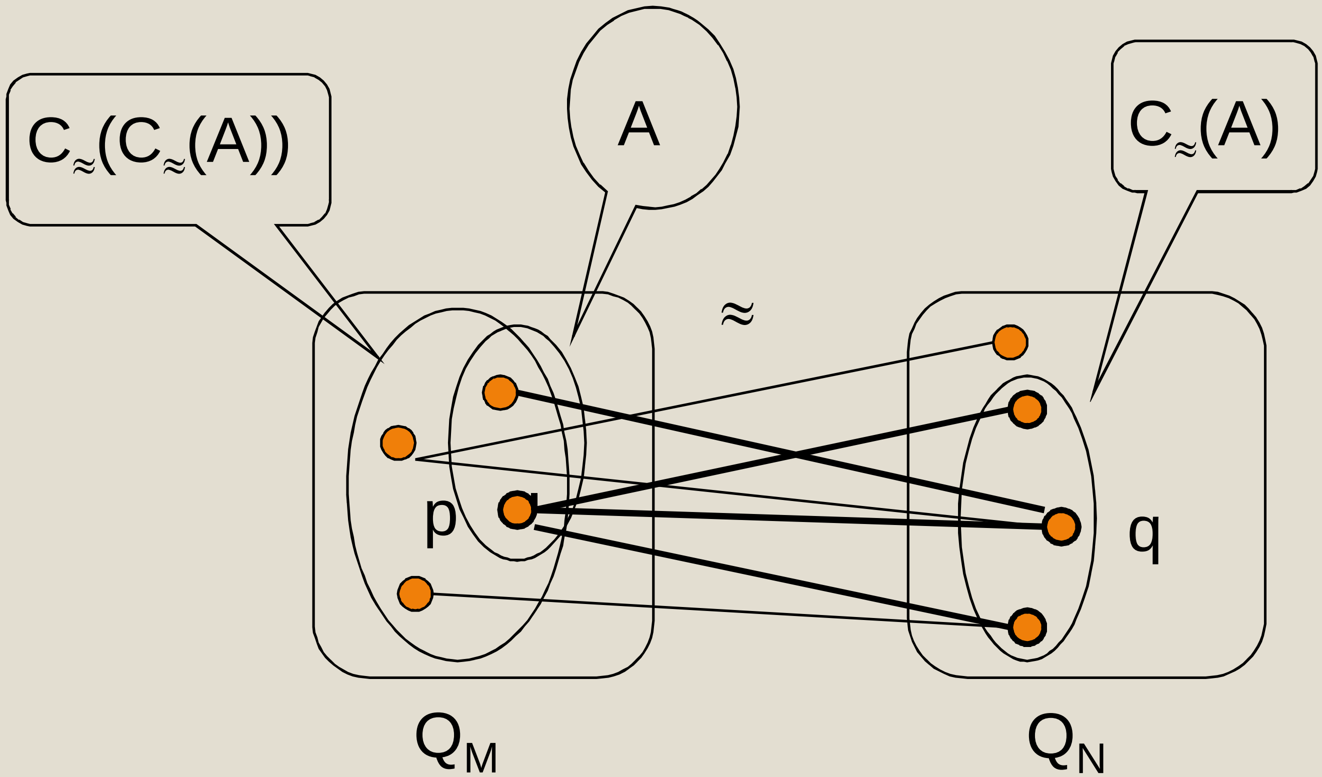
Def: $M=(Q_M, S, d_M, S_M, F_M)$, $N=(Q_N, S, d_N, S_N, F_N)$: two NFAs,

$\approx$: a binary relation from Q_M to Q_N.

- For $B \subseteq Q_N$, define $C_{\approx}(B) = \{p \in Q_M \mid \$q \in B \;\; p \approx q \}$
- For $A \subseteq Q_M$, define $C_{\approx}(A) = \{q \in Q_N \mid \$P \in A \;\; p \approx q \}$

Extend $\approx$ to subsets of Q_M and Q_N as follows:

- $A \approx B <=>_{def} A \subseteq C_{\approx}(B)$ and $B \subseteq C_{\approx}(A)$
- iff $\forall p \in A \; \$q \in B$ s.t. $p \approx q$ and $\forall q \in B \; \$p \in A$ s.t. $p \approx q$



C≈(C≈(A))
A
C≈(A)
≈
p
q
Q_M
Q_N

Bisimulation

- Def B.1: A relation $\approx$ is called a bisimulation if
  - 1. $S_M \approx S_N$
  - 2. if $p \approx q$ then $\forall a \in S$, $d_M(p,a) \approx d_N(q,a)$
  - 3. if $p \approx q$ then $p \in F_M$ iff $q \in F_N$.
- M and N are *bisimilar* if there exists a bisimulation between them.
- For each NFA M, the *bisimilar class* of M is the family of all NFAs that are bisimilar to M.
- Properties of bisimulaions:

1. Bisimulation is symmetric: if $\approx$ is a bisimulation b/t M and N, then its reverse $\{(q,p) \mid p \approx q\}$ is a bisimulation b/t N and M.
2. Bisimulation is transitive: $M \approx_1 N$ and $N \approx_2 P \Rightarrow M \approx_1 \approx_2 P$
3. The union of any nonempty family of bisimulation b/t M and N is a bisimulation b/t M and N.

Properties of bisimulations

Pf: 1,2: direct from the definition.

(3): Let $\{\approx_i \mid i \in I\}$ be a nonempty indexed set of bisimulations b/t M and N. Define $\approx =_{def} U_{i \in I} \approx_i$.

Thus $p \approx q$ means $\$i \in I\ p \approx_i q$.

1. Since I is not empty, $S_M \approx_i S_N$ for some $i \in I$, hence $S_M \approx S_N$
2. If $p \approx q \Rightarrow \$i \in I\ p \approx_i q \Rightarrow d_M(p,a) \approx_i d_N(q,a) \Rightarrow d_M(p,a) \approx d_N(q,a)$
3. If $p \approx q \Rightarrow p \approx_i q$ for some $i \Rightarrow (p \in F_M \Leftrightarrow q \in F_N)$

Hence $\approx$ is a bisimulation b/t M and N.

Lem B.3: $\approx$: a bisimulation b/t M and N. If $A \approx B$, then for all x in S^*, $D(A,x) \approx D(B,x)$.

pf: by induction on $|x|$. Basis: 1. $x = e \Rightarrow D(A,e) = A \approx B = D(B,e)$.

2. $x = a$: since $A \subseteq C_\approx(B)$, if $p \in A \Rightarrow \$q \in B$ with $p \approx q$. $\Rightarrow d_M(p,a) \subseteq C_\approx(d_N(q,a)) \subseteq C_\approx(D_N(B,a))$. $\Rightarrow D_M(A,a) = U_{p \in A}\, d_M(p,a) \subseteq C_\approx(D_N(B,a))$.
   By a symmetric argument, $D_N(B,a) \subseteq C_\approx(D_M(A,a))$.
   So $D_M(A,a) \approx D_N(B,a)$).

Bisimilar automata accept the same set.

3. Ind. case: assume $D_M(A,x) \approx D_N(B,x)$. Then $D_M(A,xa) = D_M(D_M(A,x), a) \approx D_N(D_N(B,x),a) = D_N(B,xa)$. Q.E.D.

Theorem B.4: Bisimilar automata accept the same set.

Pf: assume $\approx$: a bisimulation b/t two NFAs M and N.

Since $S_M \approx S_N \Rightarrow D_M(S_M,x) \approx D_N(S_N,x)$ for all x.

Hence for all x, $x \in L(M) \Leftrightarrow D_M(S_M, x) \cap F_M \neq \{\}$ $\Leftrightarrow D_N(S_N,x) \cap F_N \neq \{\}$ $\Leftrightarrow x \in L(N)$. Q.E.D.

Def: $\approx$: a bisimulation b/t two NFAs M and N

The support of $\approx$ in M is the states of M related by $\approx$ to some state of N, i.e., $\{p \in Q_M \mid p \approx q \text{ for some } q \in Q_N\} = C_{\approx}(Q_N)$.

Autobisimulation

Lem B.5: A state of M is in the support of all bisimulations involving M iff it is accessible.

Pf: Let ≈ be any bisimulation b/t M and another FA.

By def B.1(1), every start state of M is in the support of ≈.

By B.1(2), if p is in the support of ≈, then every state in d(p,a) is in the support of ≈. It follows by induction that every accessible state is in the support of ≈.

Conversely, since the relation B.3 = {(p,p) | p is accessible} is a bisimulation from M to M and all inaccessible states of M are not in the support of B.3. It follows that no inaccessible state is in the support of all bisimulations. Q.E.D.

Def. B.6: An autobisimulation is a bisimlation b/t an automaton and itself.

Property of autobisimulations

Theorem B.7: Every NFA M has a coarsest autobisimulation $\equiv_M$, which is an equivalence relation.

Pf: let B be the set of all autobisimulations on M.

B is not empty since the identity relation $I_M = \{(p,p) \mid p \text{ in } Q\}$ is an autobisimulation.

1. let $\equiv_M$ be the union of all bisimualtions in B. By Lem B.2(3), $\equiv_M$ is also a bisimualtion on M and belongs to B. So $\equiv_M$ is the largest (i.e., coarsest) of all relations in B.
2. $\equiv_M$ is ref. since for all state p $(p,p) \in I_M \subseteq \equiv_M$.
3. $\equiv_M$ is sym. and tran. by Lem B.2(1,2).
4. By 2,3, $\equiv_M$ is an equivalence relation on Q.

Find minimal NFA bisimilar to a NFA

- M = (Q,S,d,S,F) : a NFA.
- Since accessible subautomaton of M is bisimilar to M under the bisimulation B.3, we can assume wlog that M has no inaccessib states.
- Let $\equiv$ be $\equiv_M$, the maximal autobisimulation on M.

  for p in Q, let [p] = {q | p $\equiv$ q } be the $\equiv$-class of p, and

  let « be the relation relating p to its $\equiv$-class [p], i.e.,

  « $\subseteq$ Qx2^Q $=_{def}$ {(p,[p]) | p in Q }

  for each set of states A $\subseteq$ Q, define [A] = {[p] | p in A }. Then

Lem B.8: For all A,B $\subseteq$ Q,

- 1. A $\subseteq$ $C_\equiv$ (B) iff [A] $\subseteq$ [B], 2. A $\equiv$ B iff [A] = [B], 3. A « [A]

of:1. A $\subseteq$ $C_\equiv$(B) <=> $\forall$p in A $\forall$ q in B s.t. p $\equiv$ q <=> [A] $\subseteq$ [B]

2. Direct from 1 and the fact that A $\equiv$ B iff A $\subseteq$ $C_\equiv$(B) and B $\subseteq$ $C_\equiv$(

3. p $\in$ A => p $\in$ [p] $\in$ [A], B $\in$ [A] => \$ p $\in$ A with p « [p] = B

Minimal NFA bisimilar to an NFA (cont'd)

- Now define M' = {Q', S, d', S',F'} = M/≡ where
  - Q' = [Q] = {[p] | p ∈ Q},
  - S' = [S] = {[p] | p ∈ S} , F' = [F] = {[p] | p ∈ F} and
  - d'([p],a) = [d(p,a)],
  - Note that d' is well-defined since

    [p] = [q] => p ≡ q => d(p,a) ≡ d(q,a) => [d(p,a)] = [d(q,a)]

    => d'([p],a) = d'([q],a)

Lem B.9: The relation « is a bisimulation b/t M and M'.

pf: 1. By B.8(3): S ⊆ [S] = S'.

2. If p « [q] => p ≡ q => d(p,a) ≡ d(q,a)

   => [d(p,a)] = [d(q,a)] => d(p,a) « [d(p,a)] = [d(q,a)].

3. if p ∈ F => [p] ∈ [F] = F' and

   if [p] ∈ F'= [F] => $q ∈ F with [q] = [p] => p ≡ q => p

By theorem B.4, M and M' accept the same set.

Autobisimulation

Lem B.10: The only autobisimulation on M' is the identity relation =.

Pf: Let ~ be an autobisimulation of M'. By Lem B.2(1,2

the relation « ~ » is a bisimulation from M to itself.

1. Now if there are [p] $\neq$ [q] (hence not p $\equiv$ q) with [

~ [q]

=> p « [p] ~ [q] » q => p « ~ » q => « ~ » $\not\subset \equiv$, a contradiction !.

On the other hand, if [p] not~ [p] for some [p] => fo

any [q],

[p] not~ [q] (by 1. and the premise)

=> p not (« ~ ») q for any q (p « [p] [q] » q)

=> p is not in the support of « ~ »

Quotient automata are minimal FAs

- Theorem B11: M: an NFA w/t inaccessible states, $\equiv$: maximal autobisimulation on M. Then M' = M /$\equiv$ is the minimal automata bisimilar to to M and is unique up to isomorphism.

pf: N: any NFA bisimilar to M w/t inaccessible states.

N' = N/ $\equiv_N$ where $\equiv_N$ is the maximal autobisimulation on N.

=> M' bisimiar to M bisimilar to N bisimiar to N'.

Let $\approx$ be any bisimulation b/t M' and N'.

Under $\approx$, every state p of M' has at least on state q of N' with p $\approx$ q and every state q of N' has exactly one state p of M' with p $\approx$ q.

O/w $p \approx q \approx^{-1} p' \neq p$ => $\approx \approx^{-1}$ is a non-identity autobisimulation on M, a contradiciton!.

Hence $\approx$ is 1-1. Similarly, $\approx^{-1}$ is 1-1 => $\approx$ is 1-1 and onto and hence is an isomorphism b/t M' and N'. Q.E.D.

Algorithm for computing maximal bisimulation

- a generalization of that of Lec 14 for finding equivalent states of DFAs

The algorithm: Find maximal bisimulation of two NFAs M and N

- 1. write down a table of all pairs (p,q) of states, initially
- unmarked
- 2. mark (p,q) if $p \in F_M$ and $q \notin F_N$ or vice versa.
- 3. repeat until no more change occur: if (p,q) is unmarked and if for some $a \in S$, either

  $\$p' \in d_M(p,a)$ s.t. $\forall q' \in d_N(q,a)$, (p',q') is marked, or

  $\$q' \in d_N(q,a)$ s.t. $\forall p' \in d_M(p,a)$, (p',q') is marked,

  then mark (p,q).
- 4. define $p \equiv q$ iff (p,q) are never marked.
- 5. If $S_M \equiv S_N$ => $\equiv$ is the maximal bisimulation
- o/w M and N has no bisimulation.