Green's Theorem & Applications

GOAL: Provide alternate proof for FO = Star free.

The proof will be algebraic. For this we introduce a mathematical object called the monoids.

Defn (Monoid):= A monoid is a set M along with associative binary operator '$\cdot$' and a special element $e \in M$: which acts as an identity element w.r.t '$\cdot$'
Monoid is denoted by $(M, \cdot, e)$.

Example $(\mathbb{N}, +, 0)$ is a monoid.
$(\Sigma^*, \cdot, \epsilon)$ is a monoid.

Monoid is (infinite) finite if the underlying set is (infinite) finite.

Example of finite monoid.

Let F be the set of functions from a finite set S to S $F = \{f \mid f: S \to S\}$.

Then $(F, \circ, Id)$ is an example of finite monoid.

How do Monoids relate to languages?

Theorem: A language L is regular iff it is recognized by some finite monoid.

To understand the above theorem, we need to make clear what the notion of "recognized by finite monoid" means. For this, we need to define some notations.

Defn:= (homomorphism). A morphism from a monoid $(M, \cdot, e)$ to a Monoid $(N, *, f)$ is a function $h: M \to N$ such that $h(x \cdot y) = h(x) * h(y)$ & $h(e) = f$.

Given a monoid $(M, \cdot, e)$, a subset X of M and a morphism h from Σ^* to M, the language defined by X w.r.t h is $h^{-1}(X)$. We say a language L is recognized by a monoid M if there is a morphism h & $X \subseteq M$ s.t $L = h^{-1}(X)$.

Proof of Theorem 1 :

Suppose L is recognized by a finite monoid M via homomorphism h & set X. We construct the required automaton A_M as follows.

$$A_M = (M, \Sigma, \delta, e, X)$$

where $\delta(m, a) = m \cdot h(a)$.

Clearly, $\mathcal{L}(A_M) = \{x \mid h(x) \in X\} = L$.

For the converse, given an automaton $A = (Q, \Sigma, \delta, s, F)$, we define a transition monoid as follows.

$$M_A = (\{\delta_x \mid x \in \Sigma^*\}, \bullet, \delta_\epsilon) \text{ where}$$

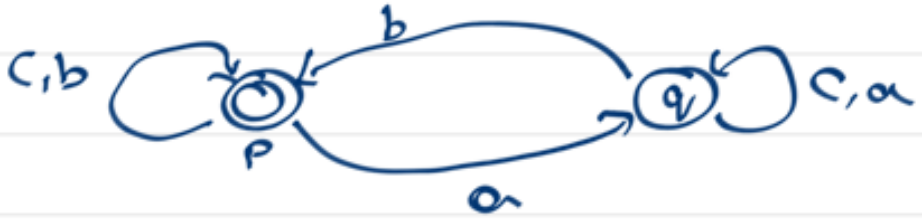
$\delta_x : Q \to Q$ is a function defined by

$$\delta_x(q) = \delta(q, x).$$

Now consider a morphism $h: \Sigma^* \to M_A$ defined by $h(x) = \delta_x$. We further let $X = \{\delta_x \mid \delta(s, x) \in F\}$. Clearly $h^{-1}(X) = L$.

Thus $L(A)$ is recognized by a finite monoid.

Let us take an example.



[language: set of all words in which 'a' does not occur to the right of last 'b'].

What are the different functions

$1 : \delta_a = [q, q]$ $\quad \delta_{ab} = [p, p]$.

$2 = \delta_b = [p, p]$ $\quad \delta_{ba} = [q, q]$

$e = \delta_c = [p, q]$

Monoid

	e	1	2
e	e	1	2
1	1	1	2
2	2	1	2

Given a monoid $(M, \cdot, e)$, we say $i \in M$ is an idempotent if $i \cdot i = i$. A monoid is said to be idempotent if every element is an idempotent. Example the above example is an idempotent.

A monoid is said to be commutative if $\forall p, q \in M$, $p \cdot q = q \cdot p$.

Some properties of Monoids / lang c/o proof.

(1) If L is recognized by a Monoid so is $\bar{L}$.

(2) If L_1 & L_2 are recognized by Monoid so is $L_1 \cup L_2$ & $L_1 \cap L_2$. (Product Monoid).

We will now go on to prove more delicious theorems. More importantly we define a relation called Green's relation. It happens to be an amazing tool in the study of monoid semi-group theory.

We first write down an useful property of idempotents.

Prop: Let $(M, \cdot, 1)$ be a monoid & let 'i' be an idempotent. Then if $x = i \cdot y$ then $x = i \cdot x$
Similarly if $x = yi$ then $x = xi$.

Proof: Let $x = i \cdot y$. Multiplying both sides by 'i', we get $i \cdot x = i \cdot i \cdot y$. but $x = iy$
$\Rightarrow$ $i \cdot x = x$.

Other direction is similar $\square$.

Now we define the relations $\leq_L$, $\leq_R$, $\leq_J$ as follows.

Def: Let $(M, \cdot, 1)$ be a Monoid. The relations $\leq_L, \leq_R, \leq_S$ are defined as follows.

$$s \leq_L t \triangleq \exists u : s = ut.$$

$$s \leq_R t \triangleq \exists v : s = tv.$$

$$s \leq_S t \triangleq \exists u_1, u_2 : s = u_1 t u_2.$$

Clearly the following holds.

- $s \leq_L t$ iff $M_s \subseteq M_t$.

$\Rightarrow$ follows from $s = ut$, $M \cdot u \subseteq M$.

$\Leftarrow$ $M \cdot s \subseteq M \cdot t \Rightarrow s \in M \cdot t \Rightarrow \exists u : s = ut$.

Similarly

- $s \leq_R t$ iff $sM \subseteq tM$.

- $s \leq_S t$ iff $M s M \subseteq M t M$.

further $\leq_L$ is right congruence ($s \leq_L t \Rightarrow su \leq_L tu$) & $\leq_R$ is a left congruence.

These relations are reflexive and transitive but not anti-symmetric. The equivalence induced by these relations will be the topic of our study.

Proposition For any monoid M

$$\leq_J = \leq_R \circ \leq_L = \leq_L \circ \leq_R .$$

Proof:=

"$\subseteq$"

let $s \leq_J t \Rightarrow$

$s = u_1 t u_2$ for some $u_1, u_2 \in M$.

$\Rightarrow s \leq_L t u_2 \; 4 \; t u_2 \leq_R t$.

$\Rightarrow s \leq_L \circ \leq_R t$.

"$\supseteq$" Notice that $\leq_R$ & $\leq_L$ are contained in $\leq_J$. $s \leq_R \circ \leq_L t \Rightarrow s \leq_J \circ \leq_J t$ $\Rightarrow s \leq_J t$. Since $\leq_J$ is transitive. $\square$.

Definition: Let $(M, \cdot, e)$ be any monoid. The relations $\mathcal{L}, \mathcal{R}$ and $\mathcal{J}$ on M are defined as.

$$s \mathcal{L} t \triangleq s \leq_{\mathcal{L}} t \text{ and } t \leq_{\mathcal{L}} s \triangleq M.s = M.t$$

$$s \mathcal{R} t \triangleq s \leq_{\mathcal{R}} t \text{ and } t \leq_{\mathcal{R}} s \triangleq s.M = t.M.$$

$$s \mathcal{J} t \triangleq s \leq_{\mathcal{J}} t \text{ and } t \leq_{\mathcal{J}} s \triangleq M.s.M = M.t.M.$$

$$s \mathcal{H} t \triangleq s \mathcal{R} t \text{ and } s \mathcal{L} t .$$

Clearly $\mathcal{H} \subseteq \mathcal{L}, \mathcal{R}$. and $\mathcal{L}, \mathcal{R} \subseteq \mathcal{J}$.

These relations are clearly equivalence relations, the corresponding equivalence classes are called $\mathcal{L}$-classes, $\mathcal{R}$-classes, $\mathcal{J}$ classes and $\mathcal{H}$-classes.

For any element x, we write $\mathcal{L}[x]$ to denote its $\mathcal{L}$-class, similarly for other classes.

Proposition: For any finite monoid M,

$$J = R \circ L = L \circ R.$$

Proof:

"$\supseteq$" once again follows from the fact that $L, R \subseteq J$ & J is transitive

"$\subseteq$" Suppose $s \, J \, t$. Then $s = utv$ &

$t = xsy$ for some u, v, x, y. Now

substitute t in s, we get

$$s = uxsyv.$$

Let N be the idempotent power of ux. Iteratively substituting s N many times we get

$$s = \underbrace{(ux)^N} \, s \, (yv)^N.$$ Notice that $(ux)^N$ is an idempotent

we can apply proposition-1 to get the following.

$$s = (ux)^N s. \Rightarrow s = u x^{N-1} u x s$$

$$\Rightarrow s \, L \, xs.$$

using similar technique we can show

$sRsy$. using left congruence property of R we get $xsRxsy$.

$$\Rightarrow s \, L \, xs \, R \, xsy \Rightarrow s L x s R t.$$

The other equality is obtained in a similar manner □.

Definition: The relation D on M is defined as $s \, D \, t$ iff $s \, L \circ R \, t$. for finite monoid, $D = J$.

Next we show that L & R classes are contained inside D-class.

Proposition:- Over any finite monoid, we have

(1) if sJt and $s \leq_L t$ then sLt.
(2) if sJt and $s \leq_R t$ then sRt.

Proof:-

Assume sJt. & $s \leq_R t$. This means $s = tu$ and $t = xsy$. Substituting for s we get $t = xtuy$. Let N be the idempotent for uy. By repeated substitution of t, we get

$$t = x^N t (uy)^N.$$

By proposition 1 we get

$$t = t(uy)^N. \Rightarrow t = t.u.y.(uy)^{N-1}.$$
$$\Rightarrow t = s.y.(uy)^{N-1} \Rightarrow t \leq_R s. \Rightarrow t R s.$$

other direction is similar. □

At this point, it is clear that every J-class decomposes into a set of R-classes as well as into L-classes. Further since $J = L \circ R = R \circ L$, we have L-class & R-class has non-empty intersection.

Proof:- For any finite monoid, if sJt then $\mathcal{L}(s) \cap \mathcal{R}(t) \neq \phi$.

Proof:- Suppose sJt, then $\exists x : s\mathcal{L}x\mathcal{R}t \Rightarrow$

$\mathcal{L}(s) \cap \mathcal{R}(t) \neq \phi$. ∎

A lot more can be said about the structure of these D-Classes. To start with we show $\mathcal{L}$ & $\mathcal{R}$ class within a D class have same size. Also for H-Classes.

Let ρ_u be a map of the form $x \mapsto xu$.
& λ_u be a map of the form $x \mapsto ux$.

lemma (Green's lemma):- Let $(M, \cdot, 1)$ be a finite monoid and let sDt then

(1) If $s\mathcal{R}t$ and $su = t$ & $tv = s$ then the map ρ_u & ρ_v are bijections b/w $\mathcal{L}(s)$ & $\mathcal{L}(t)$. Further they preserve $\mathcal{H}$-class
(2) If $s\mathcal{L}t$ & $us = t$ & $vt = s$. then the maps λ_v & λ_u are bijection b/w $\mathcal{R}(s)$ & $\mathcal{R}(t)$. further they preserver H-classes.

Proof:= $\mathcal{L}$ is congruent w.r.t. to right multiplication i.e. $s\mathcal{L}t$ then $su \mathcal{L} tu$.

$\Rightarrow$ the maps $\cdot u$ maps $\mathcal{L}(s)$ into $\mathcal{L}(t)$ & $\cdot v$ maps $\mathcal{L}(t)$ to $\mathcal{L}(s)$.

Further for any $x \in \mathcal{L}(s)$, we have $x = ys$.

$\Rightarrow$ $x \cdot u \cdot v = y \cdot s \cdot u \cdot v = y \cdot t \cdot v = ys = x$.

Thus $\cdot uv$ is an identity function on $\mathcal{L}(s)$ similarly $\cdot vu$ on $\mathcal{L}(t)$, $\cdot u$ & $\cdot v$ are bijections & inverse of each other.

More over $xu \leq_R x$ for any $x \in \mathcal{L}(s)$. Thus the elements in $H(x)$ are mapped to elements in $H(xu)$. Since $\cdot u$ & $\cdot v$ preserve H-classes.

The other statement is symmetric. $\square$.

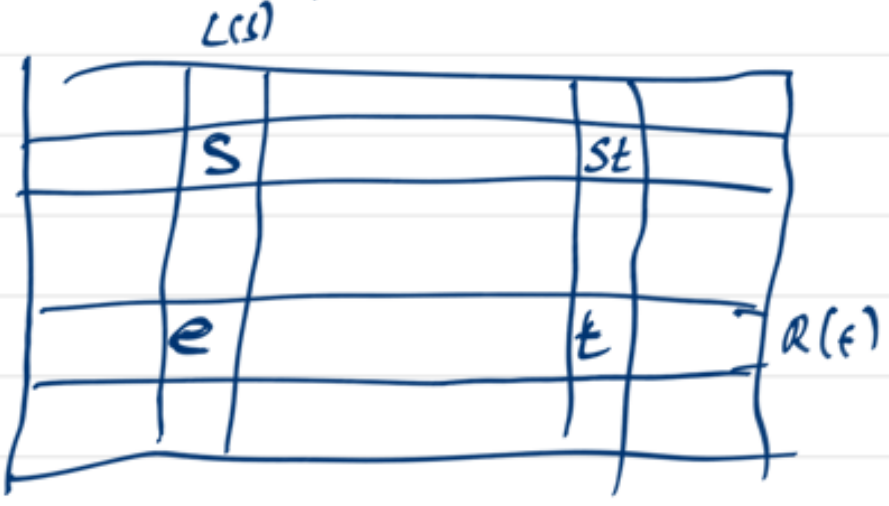
Corollary:= In any D-class of a finite monoid, every $\mathcal{L}$-class & $\mathcal{R}$-class has same size. Every H-class has the same size. Further if $x D y$ then there are

u, v s.t $z \to uzv$ is a bijection b/w $H(x)$ & $H(y)$.

Idempotents and D-classes:

We say a D-class (or H-class, R/L-class) is regular if it contains an idempotent.

Location-Lemma: Let M be any finite monoid and let sDt. $stDs$ (equivalently $stRs$ & $stLt$) iff the H-class $L(s) \cap R(t)$ contains an idempotent.



Note that sDt and $s \leq_R st$ & $t \leq_L st$. By Proposition 7, $sJst$ hold iff $tLst$ and $sRst$. (This proves equivalence in the bracket).

$\Rightarrow$

Suppose $s\,\mathcal{D}\,s\mathcal{D}t$. Then by green's lemma $\cdot t$ is a bijection from $R(s)$ to $R(st)$. But $t \in R(st) \Rightarrow \cdot t$ is a bijection from $R(s)$ to $R(t)$.

$\Rightarrow$ there is an $x \in R(s)$ s.t $xt = t$.

Further since $\cdot t$ preserves H-classes, there is a y s.t $x = ty$. Now substituting for t $xt = t$, we get

$$tyt = t. \Rightarrow tyty = ty.$$

Thus ty is the required idempotent.

$\Leftarrow$ Conversely, suppose e is an idempotent in $R(s) \cap R(t)$. then

$$e = tu,\ t = eu',\ e = vs,\ s = v'e. \text{ for some } u, u', v, v'. \Rightarrow$$

$$sty = s(tu) = se = (v'e)e = v'e = s$$

$\Rightarrow s\,\mathcal{R}\,s$. Similarly we can show $s\,\mathcal{L}\,t$ □

Corollary:= Let M be any monoid & e be an idempotent in M. Then $H(e)$ is a subsemigroup.

Proof Let $s, t \in H(e)$, we need to show $st \in H(e)$. Note that $e \in R(s) \cap R(t)$. Applying location lemma, we get

$st\ R(s)$ & $s \in L(s) \Rightarrow st \in H_e$. $\square$.

Theorem (Green's Theorem):= Let $(M, \cdot, 1)$ be a finite monoid and let e be an idempotent. Then $H(e)$ is a group. Thus for any H-class, $H \cap H^2 \neq \emptyset$ then H is a group.

Proof:= By previous corollary, $H(e)$ is a semigroup. Further for any $s \in H(e)$, there are x, y s.t $e \cdot x = s$ & $y \cdot e = s$. Thus we also have $s = es$, $s = se \Rightarrow e$ is the identity element. Thus it also forms a submonoid.

Further, we know that there are s_ℓ & s_r s.t $s_\ell \cdot s = e$ and $s \cdot s_r = e$. We almost have left & right inverses already. But these inverses need not be from $H(e)$.

However we can manufacture equivalent inverses in $H(e)$.

Let $t_\ell = e s_\ell e$ & $t_r = e s_r e$. Then

$t_\ell \cdot s = e \cdot s_\ell \cdot es = e \cdot s_\ell \cdot s = e$. $\Rightarrow$.

$e \leq_R t_\ell$.

similarly.

$s \cdot t_r = s \cdot e \cdot s_r \cdot e = s \cdot s_r \cdot e = e$

$\Rightarrow e \leq_L t_r$.

Since $t_\ell = e \cdot s_\ell \cdot e$ & $t_r = e \cdot s_\ell \cdot e$, we already have $t_\ell \mathcal{L} e$ & $t_r \mathcal{R} e$.

$\Rightarrow e R t_\ell$ & $e \mathcal{L} t_r \Rightarrow e \mathcal{J} t_\ell, t_r$.

Now since $e \leq_{\mathcal{L}} t_\ell$ & $e \leq_{\mathcal{R}} t_r$, we also have $e \mathcal{L} t_\ell, t_r$, $e \mathcal{R} t_\ell, t_r$.

$\Rightarrow e \mathcal{H} t_1$ & $e \mathcal{H} t_r$. Thus every element in this monoid has a left & right inverses this means they are identical & forms a group.

finally suppose $H \cap H^2 \neq \emptyset$, then $\exists s, t \in H$ s.t $s.t \in H$. Now by location lemma H contains an idempotent. Thus it forms a group. □

Corollary := The maximal sub-groups of a monoid M are exactly those of the form $H(e)$, e any idempotent.

Proof := clearly $ge = eg = g$. by prop earlier $e = gg^{-1} = g^{-1}g \Rightarrow e \mathcal{H} g$.

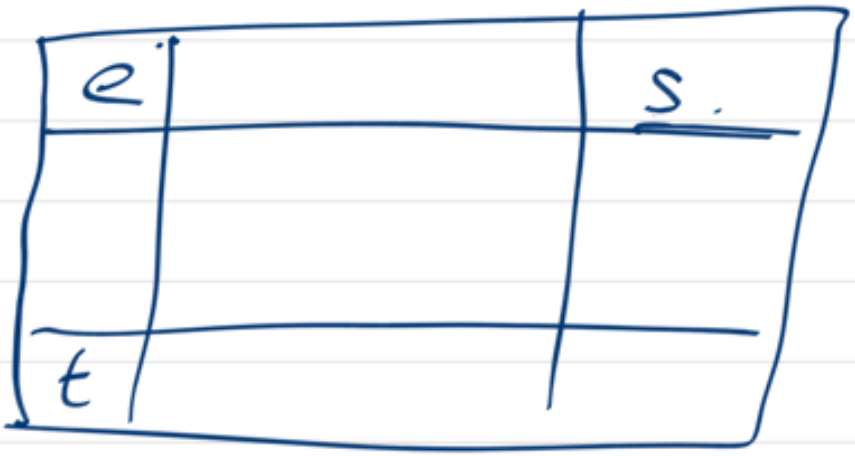
Proof :- Every R-class of a regular D-class contains an idempotent.

Proof :- Let D be a D-class, e be any idempo in D. Let R be any R class of D. The H-class $H = L(e) \cap R$ is non empty. Let t be an element of H. Since $t \in Le$,

$$t = ve \quad \& \quad e = v't.$$

Let $s = ev'$ then $st = ev't = e \cdot e = e$. Moreover sRe since $st = e$ & $s = ev'$.

$\Rightarrow e = st$ is in $R(s) \cap L(t)$. Hence from location lemma $R = R(t)$ contains an idempotent



Defn:= Let $(M, \cdot, 1)$ be a monoid. An element $s \in M$ is said to be regular if there is an element t such that $s = sts$.

Lemma:= Let M be any finite monoid. A D-class is regular iff every element in the class is regular. Furthermore D-class contains a regular element iff it is regular.

We now show that for any finite monoid, if each of its $\mathcal{H}$-classes is trivial (contains a single element) then all its $\mathcal{H}$-classes are trivial. We call such a monoid $\mathcal{H}$-trivial.

Thm: Let $(M, \cdot, 1)$ be a finite monoid s.t every regular $\mathcal{H}$-class is trivial. Then all its $\mathcal{H}$-classes are trivial.

Proof: for such a monoid, $y^N = y^N y$. where N is idempotent power of y.

$$y^N = y^N \cdot y^N = y^N \cdot y \cdot y^{N-1} \Rightarrow y^N \mathcal{J}\, y^N y.$$

since $y^N y \leq_L y^N$ & $y^N \leq_R y^N \cdot y$, we have

$y^N y \; \mathcal{H}\; y^N$. As all regular $\mathcal{H}$-class is trivial, y^N is an idempotent we have $y^N y = y^N$.

Now let H be an $\mathcal{H}$-class & let $s, t \in H$.

$\Rightarrow s = xt$ & $t = sy$.

Now

$S = xSy$. substituting repeatedly we get

$S = x^N S y^N$ where N is idempotent of y.

$S = x^N . S . y^N = x^N . S . y^N y = Syy = t$. □..

Now we want to prove Schutzenberger's theorem. For this we need to introduce the notion of aperiodic monoids.

A monoid is said to be aperiodic if there is a N such that $a^N = a^{N+1}$ for each $a \in M$.

What we want to show is Star free languages co-incide with a-periodic Monoids.

Star-free → aperiodic Monoids is not difficult. aperiodic Monoids → star free is the ugly guy.

aperiodic - Monoid ⇒ Star free

Prop A monoid $(M, \cdot, I)$ is aperiodic iff it is $\mathcal{H}$-trivial.

Proof:- It can be shown that if M is aperiodic iff it is group free. Assuming this, $\mathcal{H}$-class of any idempotent is $\mathcal{H}$-trivial

$\Rightarrow$ monoid must be $\mathcal{H}$-trivial.

($\Leftarrow$) $\mathcal{H}$-trivial $\Rightarrow$ no non trivial groups $\Rightarrow$ aperiodic

□

Theorem: Every language recognized by an aperiodic monoid is a star free regular language.

Proof:- For this it is sufficient to show that for any M an aperiodic monoid & $h: \Sigma^* \to M$, for each $s \in M$, $h^{-1}(s)$ is star free

For this we assume a pre-order among the J-classes & proceed by induction on $\leq_J$.

More precisely, we assume that $h^{-1}(t)$ is star free for all $s <_J t$ & prove that $h^{-1}(s)$ is also star free.

For the base case, 1 is the maximal element under $\leq_J$. further $J(1) = H(1)$. (easy to check). Since aperiodic monoid is H-trivial $J(1) = \{1\}$.

$$\Rightarrow h^{-1}(1) = \{a \mid h(a) = 1\}^*.$$

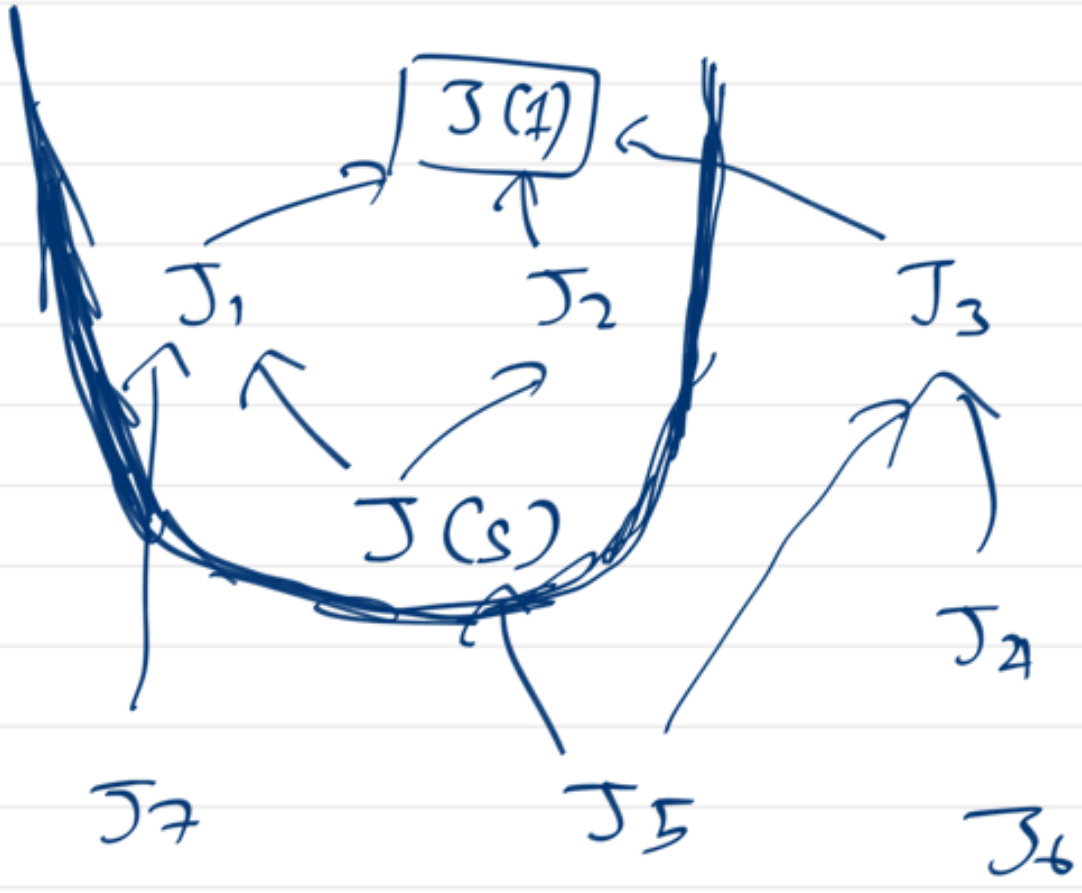
The inductive step is carried out in 3-steps.

Firstly we show that $h^{-1}(J(s))$ is star free and then that $h^{-1}(R(s))$ & $h^{-1}(L(s))$ is also star free. From this we get $h^{-1}(H(s))$ $= h^{-1}(L(s)) \cap h^{-1}(R(s))$ is also star free Now $H(s) = \{s\}$ completing the proof.

claim $h^{-1}(J(s))$ is star free

let $F(s) = \bigcup_{J(s) \not\leq_J J} J$.

clearly $\overline{F(s)} = \{t \mid s \leq_J t\}$.



we will show that $h^{-1}(F(s))$ is star free.
Once proved, we get

$$h^{-1}(J(s)) = h^{-1}(F(s)) \cup \bigcup_{s<t} h^{-1}(t)$$

since $F(s) = \bigcup_{s} M_s M$,

$\Sigma^* a \Sigma^* \subseteq h^{-1}(f(s))$ whenever $h(a) \in f(s)$

Let $L_0 = \bigcup_{h(a) \in F(s)} \Sigma^* a \Sigma^*$, this is clearly star free

Let $L_1 = h^{-1}(f(s)) \setminus L_0$.

Let $\omega \in L_1$, let u be the shortest subword of ω that also belongs to $h^{-1}(F(s))$. Clearly $|u| \geq 2$.

Let $u = a v b$ $a, b \in \Sigma$, $v \in \Sigma^*$.

Let $h(v) = t$.

we have

$$\{h(a),\ t,\ h(b),\ h(a)\cdot t,\ t\cdot h(b)\} \subseteq \overline{F(s)}.$$

Since t is outside of $F(s)$, either

$s \mathrel{J} t$ or $s <_J t$.

Suppose $s \mathrel{J} t$ → Contradiction.

Then $s \leq_J h(a)t$ & $h(a)\cdot t \leq_{\mathcal{L}} t$.

$\Rightarrow h(a)\cdot t \mathrel{\mathcal{L}} t$. $\Rightarrow h(a)\cdot t\cdot h(b) \mathrel{\mathcal{L}} t\cdot h(b)$ ↯.

$\Rightarrow s <_J t$. By induction hypothesis,

$$h^{-1}(F(s)) = L_0 \cup \bigcup \left\{ \Sigma^* \cdot a \cdot h^{-1}(t) \cdot b \cdot \Sigma^* \;\middle|\; \begin{array}{l} s <_J t,\ h(a)\cdot t \notin F(s), \\ t\cdot h(b) \notin F(s) \ \& \\ h(a)\cdot t\cdot h(b) \in F(s) \end{array} \right\}.$$

Claim 2: $h^{-1}(R(s))$ is star-free.

Let $h(w) \in R(s)$. Let u be the shortest prefix such that $h(u) \in R(s)$. If $u = \epsilon$ then $1 R s$, we are in base case.

w.log. we assume $u = va$. & $h(v) = t$.

$w = uau'$, $h(w) = h(u) \cdot h(a) \cdot h(u')$.

$\Rightarrow s \leq_R t \cdot h(a)$ & $s \leq_R t$.

So either $s <_J t$ or $s J t$.

sJt gives a contradiction:

So we assume $s <_J t$.

By induction hypothesis $L_{ta} = h^{-1}(s) \cdot a \cdot \Sigma^*$.

but L_{ta} can contain word not in $R(s)$.

for this we can easily show that

$$h^{-1}(R(s)) = L_{t,a} \cap h^{-1}(J(s)).$$

Now we have

$$h^{-1}(R(s)) = h^{-1}(J(s)) \cap \bigcup \{ L_{t,a} \mid s < t, \; t \cdot h(a) \mathrel{R} s \}.$$

□.