Lecture 6c: Green's Relations

We now discuss a very useful tool in the study of monoids/semigroups called Green's relations. Our presentation draws from [1, 2]. As a first step we define three relations on monoids that generalize the prefix, suffix and infix relations over Σ^*. Before that , we write down an useful property of idempotents:

Proposition 1 *Let $(M, ., 1)$ be a monoid and let e be an idempotent. Then, if $x = ey$ then $x = ex$. Similarly, if $x = ye$ then $x = xe$.*

Proof: Let $x = ey$. Multiplying both sides by e on the left we get $ex = eey$, and hence $ex = ey = x$. The other result follows similarly. ∎

Definition 2 *Let $(M, ., 1)$ be a monoid. The relations $\leq_L, \leq_R, \leq_J$ are defined as follows:*

$$\begin{array}{rcl} s \leq_L t & \triangleq & \exists u.\ s = ut \\ s \leq_R t & \triangleq & \exists v.\ s = tv \\ s \leq_J t & \triangleq & \exists u, v.\ s = utv \end{array}$$

Clearly, $s \leq_L t$ iff $Ms \subseteq Mt$, $s \leq_R t$ iff $sM \subseteq tM$ and $s \leq_J t$ iff $MsM \subseteq MtM$.

Observe that 1 is a maximal element w.r.t. to all of these relations. Further, from the definitions, $\leq_L$ is a right congruence (i.e. $s \leq_L t$ implies $su \leq_L tu$) and $\leq_R$ is a left congruence.

These relations are reflexive and transitive, but not necessarily antisymmetric. As a matter of fact, the equivalences induced by these relations will be the topic of much of our study.

Proposition 3 *For any monoid M, $\leq_J \; = \; \leq_R \circ \leq_L \; = \; \leq_L \circ \leq_R$.*

Proof: Since $\leq_R$ and $\leq_L$ are contained in $\leq_J$ and $\leq_J$ is transitive the containment of the last two relations in $\leq_J$ is immediate. Further, $s = utv$ then, $s \leq_R ut \leq_L t$ and $s \leq_L tv \leq_R t$. ∎

Definition 4 *Let $(M, ., 1)$ be a monoid. The relations $\mathcal{L}, \mathcal{R}$ and $\mathcal{J}$ on M are defined as follows:*

$$\begin{array}{rcl} s\mathcal{L}t & \triangleq & s \leq_L t \text{ and } t \leq_L s \\ s\mathcal{R}t & \triangleq & s \leq_R t \text{ and } t \leq_R s \\ s\mathcal{J}t & \triangleq & s \leq_J t \text{ and } t \leq_J s \\ s\mathcal{H}t & \triangleq & s\mathcal{L}t \text{ and } s\mathcal{R}t \end{array}$$

Clearly $\mathcal{H} \subseteq \mathcal{L}, \mathcal{R}$ and $\mathcal{L}, \mathcal{R} \subseteq \mathcal{J}$. Further, $\mathcal{L}$ is a right congruence and $\mathcal{R}$ is a left congruence. These relations are clearly equivalence relations and the corresponding equivalence classes are called $\mathcal{L}$-classes, $\mathcal{R}$-classes,... For any element x, we write $\mathcal{L}(v)$ to denote its $\mathcal{L}$-class and similarly for the other relations.

The following Proposition says that the relation $\mathcal{J}$ also factors via $\mathcal{L}$ and $\mathcal{R}$ for finite monoids.

Proposition 5 *For any finite monoid M, $\mathcal{J} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$.*

Proof: Once again, the containment of the last two relations in $\mathcal{J}$ follows easily. The other side requires some work.

Before we give the proof, we observe that this is not a direct consequence of Proposition 3: Suppose $s\mathcal{J}t$. Using that proposition we can only conclude that there are u' and u'' such that $s \leq_L t' \leq_R t$ and $s \leq_R t'' \leq_L t$ and not that there is a u such that $s \leq_L u \leq_R t$ and $s \leq_R u \leq_L t$.

Let $s\mathcal{J}t$, so that $s = utv$ and $t = xsy$. Substituting for t we get $s = uxsyv$. Iterating, we get $s = (ux)^N s(yv)^N$, where N is the idempotent power of ux. Applying Proposition 1, $s = (ux)^N s$ and thus $xs\mathcal{L}s$.

Similarly, we can show that $s = s(yv)^M$ and conclude that $s\mathcal{R}sy$. Using the left congruence property for $\mathcal{R}$ we get $xs\mathcal{R}xsy$.

Thus we have $s\mathcal{L}xs\mathcal{R}xsy = t$. By substituting for s in t and following the same route we can show that $t\mathcal{L}ut\mathcal{R}utv = s$. Thus $\mathcal{J}$ is contained in both $\mathcal{L} \circ \mathcal{R}$ and $\mathcal{R} \circ \mathcal{L}$. So $\mathcal{J} = \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$. ■

It turns out that the equality $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$ holds for arbitrary monoids and consequently this relation defines an equivalence on M as well. The proof of this result is not difficult and is left as an exercise.

Definition 6 *The relation $\mathcal{D}$ on M is defined as $s\mathcal{D}t$ iff $s\ \mathcal{L} \circ \mathcal{R}\ t$ (ore equivalently $s\ \mathcal{R} \circ \mathcal{L}\ t$). Over finite monoids $\mathcal{D} = \mathcal{J}$.*

The following says that over finite monoids, any pair of elements of a $\mathcal{D}$-class are either equivalent or incomparable w.r.t to the $\leq_L$ and $\leq_R$ relations.

Proposition 7 *Over any finite monoid we have*

1. *If $s\mathcal{J}t$ and $s \leq_L t$ then $s\mathcal{L}t$.*
2. *If $s\mathcal{J}t$ and $s \leq_R t$ then $s\mathcal{R}t$.*

Proof: Suppose $s \leq_R t$ and $s\mathcal{J}t$. Then we may assume that $s = tu$ and $t = xsy$. Substituting for s we get $t = xtuy$. Iterating, we get $t = x^N t(uy)^N$ for the idempotent power N of uy. By Proposition 1, we then have $t = t(uy)^N$ and thus $t = tu.y.(uy)^{N-1}$, so that $t \leq_R tu = s$ and hence $t\mathcal{R}s$. The other result is proved similarly. ■

At this point we note that every $\mathcal{J}$-class decomposes into a set of $\mathcal{R}$-classes as well as into a set of $\mathcal{L}$-classes. (Those in turn decompose into a set of $\mathcal{H}$-classes.) Further, since $\mathcal{J} = \mathcal{D} = \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$ we see that, every such $\mathcal{L}$-class and $\mathcal{R}$-class has a non-empty intersection.

Proposition 8 *For any finite monoid if $s\mathcal{J}t$ then $\mathcal{L}(s) \cap \mathcal{R}(t) \neq \emptyset$.*

Proof: For a finite monoid $s\mathcal{J}t$ implies $s\mathcal{D}t$ and hence there is an x such that $s\mathcal{L}x\mathcal{R}t$. So, $\mathcal{L}(s) \cap \mathcal{R}(t) \neq \emptyset$. ■

As a consequence of this, we have what is called the *egg box* diagram for any $\mathcal{J}$-class ($\mathcal{D}$-class) of any finite monoid, where every row is an $\mathcal{R}$-class, each column is an $\mathcal{L}$-class and the small squares are the $\mathcal{H}$-classes. And by the previous proposition, every one of these $\mathcal{H}$-classes is non-empty.

		...	
	$\mathcal{H}(x)$	$\mathcal{R}(x)$	
	$\mathcal{L}(x)$	. . . . .	
		...	

A lot more remains to be said about the structure of these $\mathcal{D}$-classes. To start with, we shall show that every $\mathcal{R}$-class ($\mathcal{L}$-class) in a $\mathcal{D}$-class has the same size and the same holds for $\mathcal{H}$-classes.

Given an element u of the monoid M we write $.u$ to denote the map given by $x \mapsto xu$ and write $u.$ to denote the map given by $x \mapsto ux$.

Lemma 9 *(Green's Lemma) Let $(M, ., 1)$ be a finite monoid and let $s\mathcal{D}t$ (or equivalently $s\mathcal{J}t$). Then*

1. *If $s\mathcal{R}t$ and $su = t$ and $tv = s$ then the maps $.u$ and $.v$ are bijections between $\mathcal{L}(s)$ and $\mathcal{L}(t)$. Further, they preserve $\mathcal{H}$-classes.*

2. *If $s\mathcal{L}t$ and $us = t$ and $vt = s$ then the maps $u.$ and $v.$ are bijections between $\mathcal{R}(s)$ and $\mathcal{R}(t)$. Further, they preserve $\mathcal{H}$-classes.*

Proof: $\mathcal{L}$ is a congruence w.r.t. right multiplication and hence $.u$ ($.v$) maps $\mathcal{L}(s)$ into $\mathcal{L}(t)$ ($\mathcal{L}(t)$ into $\mathcal{L}(s)$). Further, for any $x \in \mathcal{L}(s)$, we have $x = ys$. Therefore, $xuv = ysuv = ytv = ys = x$. Thus, $.uv$ is the identity function on $\mathcal{L}(s)$ and similarly $.vu$ is the identify function on $\mathcal{L}(t)$ and $.u$ and $.v$ are bijections (and inverses of each other).

Moreover, $xu \leq_L x$ for any $x \in \mathcal{L}(s)$. Thus, the elements in $\mathcal{H}(x)$ are mapped to elements in $\mathcal{H}(xu)$. So, $.u$ (and $.v$) preserve $\mathcal{H}$-classes.

The other statement is proved similarly. ■

Corollary 10 *In any $\mathcal{D}$-class of a finite monoid, every $\mathcal{L}$-class ($\mathcal{R}$-class) has the same size. Every $\mathcal{H}$-class has the same size and if $x\mathcal{D}y$ then there are u, v such that the map $z \mapsto uzv$ is a bijection between $\mathcal{H}(x)$ and $\mathcal{H}(y)$.*

Idempotents and $\mathcal{D}$-classes

We say that a $\mathcal{D}$-class (or a $\mathcal{H}$-class or $\mathcal{R}$-class or $\mathcal{L}$-class) is *regular* if it contains an idempotent. Regular $\mathcal{D}$-classes have many interesting properties. First, we prove a very useful lemma.

Lemma 11 *(Location Lemma (Clifford/Miller)) Let M be a finite monoid and let $s\mathcal{D}t$. Then $st\mathcal{D}s$ (or equivalently, $st\mathcal{R}s$ and $st\mathcal{L}t$) iff the $\mathcal{H}$-class $\mathcal{L}(s) \cap \mathcal{R}(t)$ contains an idempotent.*

Proof: In effect, this lemma can be summarized by the following egg box diagram.

		s			st	
	...		...		...	
		e			t	

First note that since $s\mathcal{J}t$ and $s \leq_R st$ and $t \leq_L st$, using Proposition 7, $s\mathcal{J}st$ holds iff $s\mathcal{R}st$ and $t\mathcal{L}st$ hold. This proves the equivalence claimed in paranthesis in the statement of the Lemma.

Suppose $st\mathcal{J}s\mathcal{J}t$. Then, by Green's Lemma, $.t$ is bijection from $\mathcal{L}(s)$ to $\mathcal{L}(t)$. Therefore, there is an $x \in \mathcal{L}(s)$ such that $xt = t$. Further, since $.t$ preserves $\mathcal{H}$-classes, there is a y such that $x = ty$. Thus, substituting for x we get $tyt = t$ and hence $tyty = ty$. Thus, $ty = x$ is an idempotent in $\mathcal{L}(s) \cap \mathcal{R}(t)$.

Conversely, suppose e is an idempotent in $\mathcal{L}(s) \cap \mathcal{R}(t)$. So, there are x and y such that $xe = s$ and $ey = t$. But by Proposition 1 we have $se = e$ and $et = t$. Thus, by Green's Lemma, $.t$ is a $\mathcal{H}$-class preserving bijection from $\mathcal{L}(e)$ to $\mathcal{L}(t)$ and hence $st\mathcal{R}s$ and $st\mathcal{L}t$. ■

An immediate corollary of this result is that every $\mathcal{H}$-class containing an idempotent is a sub-semigroup.

Corollary 12 *Let M be a monoid and e be an idempotent in M. Then $\mathcal{H}(e)$ is a subsemigroup.*

Proof: If $s, t \in \mathcal{H}(e)$ then by the location lemma $st\mathcal{L}s$ and $st\mathcal{H}t$ and $st\mathcal{H}e$. ■

But something much stronger holds. In fact $\mathcal{H}(e)$ is a group.

Theorem 13 *(Green's Theorem) Let $(M, ., 1)$ be a finite monoid and let e be an idempotent. Then $H(e)$ is a group. Thus, for any $\mathcal{H}$-class H, if $H \cap H^2 \neq \emptyset$ then H is a group.*

Proof: By the previous corollary, $H(e)$ is a subsemigroup. Further for any $s \in \mathcal{H}(e)$, there are x, y such that $ex = s$ and $ye = s$ and thus by Proposition 1, $es = s$ and $se = s$. Thus, it forms a sub-monoid with e as the identity.

Further, we know that there are s_l and s_r such that $s_l s = e$ and $ss_r = e$ so that we almost already have left and right inverses. But, there are no guarantees that such s_l and s_r are in $\mathcal{H}(e)$. However, we can manufacture equivalent inverses inside $\mathcal{H}(e)$ by conjugating with e.

Let $t_l = es_l e$ and $t_r = es_r e$. Then, $t_l.s = es_l es = es_l s = ee = e$. Similarly $s.t_r = e$. Moreover, this also shows that $e\mathcal{L}t_l$ and $e\mathcal{R}t_r$. And quite clearly $e\mathcal{L}t_l, t_r$ and $e\mathcal{R}t_l, t_r$. Thus, by Proposition 7, $e\mathcal{H}t_l$ and $e\mathcal{H}t_r$. Thus, every element in this monoid has a left and right inverse and this means they are identical and they form a group.

Finally, if $H \cap H^2$ is not empty then there is $s, t \in H$ such that $st \in H$, which by the Location Lemma means H contains an idempotent. Thus, it forms a group. ■

Suppose $(M, ., 1)$ is a monoid and $(G, ., e)$ is a subgroup of this monoid (as a sub-semigroup, hence e need not be 1). Then, $G \subseteq H(e)$. This is because, for any $g \in G$, $eg = ge = g$ (by Proposition 1) and $e = gg^{-1} = g^{-1}g$ and thus $e\mathcal{H}g$. Thus, any group is contained in a group of the form $\mathcal{H}(e)$. Thus we have the following result.

Theorem 14 *(Maximal Subgroups) The maximal subgroups (as sub-semigroups) of a monoid M are exactly those of the form $\mathcal{H}(e)$, e an idempotent.*

Further, if a $\mathcal{D}$-class contains an idempotent then it contains many!

Proposition 15 *Every $\mathcal{R}$-class ($\mathcal{L}$-class) of a regular $\mathcal{D}$-class contains an idempotent.*

Proof: Let D be a $\mathcal{D}$-class, e is an idempotent in D and $s \in D$. Let $t \in \mathcal{R}(e) \cap \mathcal{L}(s)$. Then, there is u such that $tu = e$. So, $utut = uet = ut$ is an idempotent. Moreover, $tut = et = t$ thus $ut\mathcal{L}t\mathcal{L}s$.

■

Definition 16 *Let $(M, ., 1)$ be a monoid. An element $s \in M$ is said to be* regular *if there is an element t such that $s = sts$.*

First we relate regular elements and regular $\mathcal{D}$-classes.

Lemma 17 *Let M be any finite monoid. A $\mathcal{D}$-class is regular if and only if every element in the class is regular. Further a $\mathcal{D}$-class contains a regular element if and only if it is regular.*

Proof: Suppose s is a regular element in a $\mathcal{D}$-class D. Therefore, there is t such that $s = sts$ and thus $st = stst$ is an idempotent. Further, since $sts = s$, $s \leq_R st \leq_R s$ and so $st\mathcal{D}s$ and so D is a regular $\mathcal{D}$-class.

On the other hand if D is a regular $\mathcal{D}$-class then we know that every $\mathcal{R}$ class in D contains an idempotent. So if $s \in D$ then there is an idempotent e and t such that $st = e$. Right multiplying by s we get $sts = es = s$ and thus every element is regular. ■

References

[1] J.E.Pin: *Mathematical Foundations of Automata Theory*, MPRI Lecture Notes.

[2] T. Colcombet: "Green's Relations and their Use in Automata Theory", *Proceedings of LATA 2011*, Spring LNCS 6638 (2011) 1-21.