Actions of $E-$dense semigroups and an application to the discrete log problem

James Renshaw
Mathematical Sciences
University of Southampton
Southampton, SO17 1BJ
England
j.h.renshaw@maths.soton.ac.uk

June 2017

Abstract

We describe the structure of $E-$dense acts over $E-$dense semigroups in an analogous way to that for inverse semigroup acts over inverse semigroups. This is based, to a large extent, on the work of Schein on representations of inverse semigroups by partial one-to-one maps. We consider an application to the discrete log problem in cryptography as well as an application to the same problem using completely regular semigroups.

Key Words Semigroup, monoid, $E-$dense, $E-$inversive, completely regular, semigroup acts, $E-$dense acts, discrete logarithm, cryptography
2010 AMS Mathematics Subject Classification 20M30, 20M50, 20M99.

1 Introduction and Preliminaries

Let S be a semigroup. By a *left $S-$act* we mean a non-empty set X together with an action $S \times X \to X$ given by $(s, x) \mapsto sx$ such that for all $x \in X, s, t \in S, (st)x = s(tx)$. If S is a monoid with identity 1, then we normally require that $1x = x$ for all $x \in X$. A *right $S-$act* is defined dually. If X is a left $S-$act then the semigroup morphism $\rho : S \to \mathcal{T}(x)$ given by $\rho(s)(x) = sx$ is a representation of S. Here $\mathcal{T}(X)$ is the *full transformation* semigroup on X consisting of all maps $X \to X$. Conversely, any such representation gives rise to an action of S on X. If X is both a left $S-$act and a right $T-$act for semigroups/monoids S and T and if in addition $(sx)t = s(xt)$ then X is said to be an $(S, T)-$*biact*. Throughout this paper, unless otherwise stated, all acts will be left $S-$acts. We refer the reader to [7] for basic results and terminology in semigroups and monoids and to [2] and [8] for those concerning acts over monoids. If S is an inverse semigroup then we can replace $\mathcal{T}(X)$ by $\mathcal{I}(X)$, the inverse semigroup of partial one-to-one maps. A comprehensive theory of these types of representations was given by Boris Schein in the early 1960's and an account of that work can be found in [1] and [7]. Here we wish to emulate that approach for *$E-$dense semigroups* and do so in section 2. In section 3, we apply some of these results to the discrete log problem found in cryptography (see for example [9]).

Recall that an *idempotent* in a semigroup S is an element $s \in S$ such that $s^2 = s$. A *band* is a semigroup consisting entirely of idempotents whilst a *semilattice* is a commutative band. We shall denote the idempotents of a semigroup S as $E(S)$ or more generally E. Let S

be a semigroup and let $W(s) = \{s' \in S | s'ss' = s'\}$ be the set of *weak inverses* of s and $V(s) = \{s' \in S | s' \in W(s), s \in W(s')\}$ be the set of *inverses* of s. If S is a group then clearly $W(s) = V(s) = \{s^{-1}\}$ for all $s \in S$, whilst if S is a rectangular band, that is to say a band in which $xyx = x$ for all $x, y \in S$, then $W(s) = V(s) = S$ for each $s \in S$. Notice that if $s' \in W(s)$ then $s's, ss' \in E$. Moreover, if $e \in E$ then $e \in W(e)$. It may of course be the case that for a given element $s \in S, W(s) = \emptyset$. We do however have

Lemma 1.1 ([20, Corollary 3.3]) *Let S be a semigroup in which $E \neq \emptyset$. Then E is a band if and only if for all $s, t \in S, W(st) = W(t)W(s)$.*

From the proof of [5, Lemma 7.14] we can deduce

Lemma 1.2 *Let S be a semigroup with band of idempotents E. Then for all $s \in S, s' \in W(s), e \in E$ it follows that $ses', s'es \in E$.*

If the conclusions of Lemma 1.2 hold, we say that S is *weakly self conjugate*. We shall make frequent use of both the previous properties of semigroups in which E is a band without further reference. Notice also that if $s' \in W(s)$ then $ss's \in V(s') \subseteq W(s')$, a fact that we shall also use frequently. In particular, s' is a regular element of S.

It was shown by Mitsch [12] that the following is a natural partial order on any semigroup S

$$a \leq_{\mathcal{M}} b \text{ if and only if there exists } x, y \in S, a = xb = by, xa = ay = a.$$

Notice that if there exist idempotents e and f such that $a = eb = bf$ then it follows that $a = ea = af$ and so $a \leq_{\mathcal{M}} b$. If a is a regular element of S then it is easy to check that $e = aa'x \in E$ and $f = ya'a \in E$ for any $a' \in V(a)$, and that $a = eb = bf$. Hence if a is regular then

$$a \leq_{\mathcal{M}} b \text{ if and only if there exists } e, f \in E, a = eb = bf.$$

In particular, this is true if $a \in E$. It is also worth noting here that if E is a semilattice then the restriction of $\leq_{\mathcal{M}}$ to E is compatible with multiplication, a fact that we shall use later.

Let A be a subset of a semigroup S and define

$$A\omega_{\mathcal{M}} = \{s \in S | a \leq_{\mathcal{M}} s \text{ for some } a \in A\}.$$

If $A = \{a\}$ then we will write $A\omega_{\mathcal{M}}$ as $a\omega_{\mathcal{M}}$. Notice that $(A\omega_{\mathcal{M}})\omega_{\mathcal{M}} = A\omega_{\mathcal{M}}$ and that if $A \subseteq B$ then $A\omega_{\mathcal{M}} \subseteq B\omega_{\mathcal{M}}$. Also, if $A \subseteq B\omega_{\mathcal{M}}$ then $A\omega_{\mathcal{M}} \subseteq B\omega_{\mathcal{M}}$. We call $A\omega_{\mathcal{M}}$ the *($\omega_{\mathcal{M}}-$)closure* of A and say that A is ($\omega_{\mathcal{M}}-$)closed if $A = A\omega_{\mathcal{M}}$. Notice that if $A \subseteq B$ with B being ($\omega_{\mathcal{M}}-$)closed, then $A\omega_{\mathcal{M}} \subseteq B$.

If T is a subset of a semigroup S then we say that T is *left (resp. right) dense* in S if for all $s \in S$ there exists $s' \in S$ such that $s's \in T$ (resp. $ss' \in T$). We say that T is *dense* in S if it is both left and right dense in S. We are particularly interested in the case where $T = E$ the set of idempotents of S and we shall refer to semigroups in which E is dense in S as *$E-$dense* or *$E-$inversive* semigroups. This concept was originally studied by Thierrin [19] and subsequently by a large number of authors (see Mitsch [15] for a useful survey article, but note that the term $E-$dense has a slightly different meaning there). Included in this class of semigroup are the classes of all regular semigroups, inverse semigroups, groups, eventually regular semigroups (that is to say every element has a power that is regular), periodic semigroups (every element is of finite order) and finite semigroups.

Let S be a semigroup, let $L(s) = \{s' \in S | s's \in E\}$. Then it is well known that $W(s) \subseteq L(s)$. Moreover, for each $s' \in L(s), s'ss' \in W(s)$ and so $W(s) \neq \emptyset$ if and only if $L(s) \neq \emptyset$. The following is then immediate.

Lemma 1.3 *Let S be an $E-$dense semigroup. Then for all $s \in S$ there exists $s' \in S$ such that $s's, ss' \in E$.*

Let S be an $E-$dense semigroup with a band of idempotents E and define a partial order on S by

$$s \leq t \text{ if and only if either } s = t \text{ or there exists } e, f \in E \text{ with } s = te = ft$$

and note that $\leq \subseteq \leq_{\mathcal{M}}$ and that if E is a semilattice then $\leq$ is compatible with multiplication by weak inverses. If s is regular (in particular idempotent) then $s \leq t$ if and only if $s \leq_{\mathcal{M}} t$. If A is a subset of S then define

$$A\omega = \{s \in S | a \leq s \text{ for some } a \in A\}$$

and notice that $A \subseteq A\omega \subseteq A\omega_{\mathcal{M}}$. It is also clear that $(A\omega)\omega = A\omega$. Note from above that if $A \subseteq E$ then $A\omega_{\mathcal{M}} = A\omega$. We shall make use of ω in Section 2.

Weak inverses of elements will not in general be unique and in section 2 we will often need to deal with more than one weak inverse of a given element. The following useful result is easy to establish.

Lemma 1.4 *Let S be an $E-$dense semigroup with a semilattice of idempotents E.*

1. *If $s' \in W(s)$ and $e, f \in E$ then $es'f \in W(s)$.*
2. *If $s', s^* \in W(s)$ then $s'ss^* \in W(s)$ and $s'ss^* = s' \wedge s^*$.*
3. *If $s' \in W(s)$ and $s'^* \in W(s')$ then $s'^* = s'^*s's = ss's'^*$ and for all $e \in E, es'^* \leq s$. In particular $s'^* \leq s$.*
4. *If $s' \in W(s)$ then $W(s') = sW(s)s$ and $V(s') = \{ss's\}$. In particular if $s^* \in W(s)$ then $W(s') = W(s^*)$ and $ss'ss^*s \in W(s')$.*
5. *Let $W = \{s' \in W(s) | s \in S\}$. Then W is an inverse subsemigroup of S.*
6. *For all $s \in S$, $W(W(W(s))) = W(s)$.*

Proof. Let E and S be as stated.

1. Suppose that $e, f \in E$ and $s' \in W(s)$. Then $(es'f)s(es'f) = es'fss'f = es'f$ and so $es'f \in W(s)$
2. This is straightforward on noting that $(s'ss^*)s(s'ss^*) = s'ss'ss^*ss^* = s'ss^*$. Note that $s'ss^* = s^*ss'$. It is clear that $s'ss^* \leq s', s^*$, so suppose that $t \leq s', s^*$. Then there exist $e, f, g, h \in E(S)$ such that $t = es' = s'f = gs^* = s^*h$. Hence since $t = s'st = (s'ss^*)h$ and $t = tss' = gs^*ss' = g(s'ss^*)$ then $t \leq s'ss^*$ as required.
3. If $s'^* \in W(s')$ then $s'^* = s'^*s's'^* = s'^*s'ss's'^* = ss's'^*s's'^* = ss's'^* = s'^*s's'^*s's = s'^*s's$. Finally notice that for all $e \in E$,

   $$s(s's'^*s'es'^*s's) = (ss's'^*s'es'^*s')s = s'^*s'es'^* = es'^*s's = es'^*$$

   and so $es'^* \leq s$.
4. Clearly $sW(s)s \subseteq W(s')$. Let $s'^* \in W(s')$ so that by part (3), $s'^* = ss's'^* = ss's'^*s's$ and $s's'^*s' \in W(s)$.

   Now let $s'^* \in V(s') \subseteq W(s')$. Since $s's'^* = s's'^*s's = s's$ then $s'^* = ss's'^* = ss's$.

   If $s^* \in W(s)$ then $W(s^*) = sW(s)s = W(s')$ and since $s'ss^* \in W(s)$ then $ss'ss^*s \in W(s')$.

5. Clearly $W \neq \emptyset$. Let $s', t' \in W$ with $s' \in W(s), t' \in W(t)$ then it is easy to check that $s't' \in W(ts) \subseteq W$ and by part (4), $|V(s')| = 1$ for each $s' \in W$ and so W is an inverse subsemigroup of S. Alternatively, note that $W =$ Reg(S) the set of regular elements of S.

6. Let $s' \in W(s), s'^* \in W(s'), s'^{*'} \in W(s'^*)$. Then by part (3), $s'^{*'}ss'^{*'} = s'^{*'}ss's'^*s'^{*'} = s'^{*'}s'^*s'^{*'} = s'^{*'}$. On the other hand $s' = s'ss' = s'(ss's)s' \in W(W(s'))$ and the result follows easily.

■

Lemma 1.5 ([13, Proposition 2]) *A semigroup S is a group if and only if for every element $s \in S$, $|L(s)| = 1$.*

It is also easy to see that

Lemma 1.6 *Let S be an $E-$dense monoid. Then S is a group if and only if $|E| = 1$.*

A subset A of a semigroup S is called *unitary* in S if whenever $sa \in A$ or $as \in A$ it necessarily follows that $s \in A$. If E is a unitary subset of S then we shall refer to S as an *$E-$unitary semigroup.*

Lemma 1.7 ([17], [15, Theorem 6.8]) *Let S be an $E-$dense semigroup. Then S is $E-$unitary if and only if E is a band and $E\omega = E$.*

Lemma 1.8 ([3, Proposition 1.2]) *Let S be an $E-$unitary semigroup. For all $s \in S$, if $s' \in L(s)$ then $s \in L(s')$.*

2 $E-$dense actions of $E-$dense semigroups

In this section we take inspiration from the theory of inverse semigroup actions, which in turn is based on Schein's representation theory of inverse semigroups by partial one-to-one maps (see [1] and [7]).

Let S be an $E-$dense semigroup, let X be a non-empty set and let $\phi : S \times X \to X$ be a partial map with the property that $\phi(st, x)$ exists if and only if $\phi(s, \phi(t, x))$ exists and then

$$\phi(st, x) = \phi(s, \phi(t, x)).$$

We will, as is usual, denote $\phi(s, x)$ as sx and simply write $(st)x$ as stx when appropriate. By a partial map we of course mean that not every element of S need act on every element of X. A more formal definition can be found in [7]. We say that ϕ is an *$E-$dense action* of S on X, and refer to X as an *$E-$dense $S-$act*, if

1. the action is *cancellative*; meaning that whenever $sx = sy$ then $x = y$;

2. the action is *reflexive*; that is to say, for each $s \in S$, if sx exists then there exists $s' \in W(s)$ such that $s'(sx)$ exists.

The *domain* of an element $s \in S$ is the set

$$D_s^X = \{x \in X | sx \text{ exists}\}.$$

We shall denote D_s^X as simply D_s when the context is clear. We shall denote the *domain* of an element $x \in X$ by

$$D^x = \{s \in S | sx \text{ exists}\}.$$

Clearly $x \in D_s$ if and only if $s \in D^x$. Notice also that it follows from the definition that $x \in D_s$ if and only if $x \in D_{s's}$ for some $s' \in W(s)$.

If S is a group then an $E-$dense act X is simply an $S-$set, while if S is an inverse semigroup then an $E-$dense act is an inverse semigroup act defined by the Wagner-Preston representation $\rho : S \to \mathcal{I}(X)$ where $sx = \rho(s)(x)$ and $D_s = \mathrm{dom}(\rho(s))$ (see Example 2.2 below for a generalisation).

Let X be an $E-$dense $S-$act and let $x \in X$. We define the *stabilizer* of an element x as the set $S_x = \{s \in S | sx = x\}$. The following is easy to establish.

Lemma 2.1 *Let S be an $E-$dense semigroup and X an $E-$dense $S-$act. Let $s, t \in S, x, y \in X$. Then*

1. *$E \cap D^x \subseteq S_x$,*
2. *if $s' \in W(s)$ then $x \in D_{s'}$ if and only if $x \in D_{ss'}$,*
3. *if $s \in D^x$ then $sx = y$ if and only if there exists $s' \in W(s) \cap D^y$ such that $x = s'y$,*
4. *if $s, t \in D^x$ then $sx = tx$ if and only if there exists $s' \in W(s)$ such that $s't \in S_x$. In addition, any such s' necessarily satisfies $s' \in D^{sx}$,*

Example 2.2 (Wagner-Preston action) *Let S be an $E-$dense semigroup with semilattice of idempotents E and X a set on which S acts (on the left) via the representation $\rho : S \to \mathcal{T}(X)$. In other words the action on X is a total action. For each $s \in S$ define*

$$D_s = \{x \in X | \text{ there exists } s' \in W(s), x = s'sx\} = \{s'sx | x \in X, s' \in W(s)\}$$

and define an $E-$dense action of S on X by $s * x = sx$ for all $x \in D_s$.

To see that $*$ really is an $E-$dense action suppose that $x \in D_{st}$ so that there exists $(st)' \in W(st)$ such that $x = (st)'(st)x$. By Lemma 1.1 there exists $s' \in W(s), t' \in W(t)$ such that $(st)' = t's'$ and so $x = t's'stx$. Then $t'tx = t'tt's'stx = t's'stx = x$ and so $x \in D_t$. In addition, $s'stx = s'stt's'stx = tt's'stx = tx$ and $tx \in D_s$. Conversely, suppose that $x \in D_t$ and $tx \in D_s$. Then there exists $t' \in W(t), s' \in W(s)$ such that $x = t'tx$ and $tx = s'stx$ and so $x = t's'stx \in D_{st}$. Clearly, $(st) * x = s * (t * x)$. Finally, if $x, y \in D_s$ and $s * x = s * y$ then there exists $s' \in W(s), s^* \in W(s)$ such that $x = s'sx, y = s^*sy$ and such that $sx = sy$. Hence

$$x = s'sx = s'sy = s'ss^*sy = s^*ss'sy = s^*ss'sx = s^*sx = s^*sy = y.$$

In addition, if $x \in D_s$ then $x = s'sx$ for some $s' \in W(s)$, and so letting $(s's)' = s's \in W(s's)$ then

$$(s's)'(s's)x = s'sx = x$$

and $x \in D_{s's}$ as required. Hence $*$ satisfies the conditions of an $E-$dense action.

In particular, we can take $X = S$, or indeed any left ideal of S, with (total) action given by the multiplication in S.

A element x of X is said to be *effective* if $D^x \neq \emptyset$. An $E-$dense $S-$act X is *effective* if all its elements are effective. An $E-$dense $S-$act is *transitive* if for all $x, y \in X$, there exists $s \in S$ with $y = sx$. Notice that this is equivalent to X being *locally cyclic* in the sense that for all $x, y \in X$ there exists $z \in X, s, t \in D^z$ with $x = sz, y = tz$. We shall consider transitive acts in more detail in Section 2.2.

If X is an $E-$dense $S-$act and Y is a subset of X then we shall say that Y is an $E-$dense $S-$*subact* of X if for all $s \in S, y \in D_s^X \cap Y \Rightarrow sy \in Y$. Notice that this makes Y an $E-$dense $S-$act with the action that induced from X and $D_s^Y = D_s^X \cap Y$ for all $s \in S$.

Let X and Y be two $E-$dense $S-$acts. A function $f : X \to Y$ is called an *$(E-$dense$)$ $S-$map* if for all $s \in S$, $x \in D_s^X$ *if and only if* $f(x) \in D_s^Y$ and then $f(sx) = sf(x)$.

For example, if Y is an $S-$subact of an $E-$dense $S-$act X, then the inclusion map $\iota : Y \to X$ is an $S-$map.

Let $x \in X$ and define the *$S-$orbit* of x as

$$Sx = \{sx | s \in D^x\} \cup \{x\}.$$

Notice that if x is effective, then there exists $s \in D^x$ and so for any $s' \in W(s) \cap D^{sx}, x = s'sx \in \{sx|s \in D^x\} = Sx$. However if x is not effective then $\{sx|s \in D^x\} = \emptyset$ and $Sx = \{x\}$. Notice also that Sx is an $E-$dense $S-$subact of X (the *subact generated by* x) and that the action is such that, for all $tx \in Sx$ and all $s \in S$, $tx \in D_s^{Sx}$ if and only if $x \in D_{st}^X$ and in which case $s(tx) = (st)x$. Then we have

Lemma 2.3 *For all $x \in X$, if x is effective then so is Sx, in which case Sx is a transitive $E-$dense $S-$act. Conversely, if an $E-$dense $S-$act is effective and transitive then it has only one $S-$orbit.*

Proof. Suppose that x is effective. Then let $s \in D^x$ so that $sx \in Sx$, and notice that there exists $s' \in W(s) \cap D^{sx}$. Therefore $ss'(sx) = sx \in Sx$ and hence Sx is effective. If $y = s_1x$ and $z = s_2x$ then put $t = s_1s_2'$, where $s_2' \in W(s_2) \cap D^z$, to get $y = tz$ (if $x = y \neq z$ then take $t = s_2'$; if $x = z \neq y$ then take $t = s_1$ while if $x = y = z$ take $t = s's$ where $s \in D^x, s' \in W(s) \cap D^{sx}$).
The converse is easy. Note that in this case $Sx = \{sx|s \in D^x\}$. ∎

Notice that $Sx = Sy$ if and only if $y \in Sx$ and so the orbits partition X.

Recall that Green's $\mathcal{L}-$relation is given by $a\mathcal{L}b$ if and only if $S^1a = S^1b$. As is normal, we shall denote the $\mathcal{L}-$class containing a as L_a.

Proposition 2.4 *Let S be an $E-$dense semigroup with semilattice of idempotents E and consider S as an $E-$dense $S-$act with the Wagner-Preston action.*

1. *If $e \in E$ then $S_e = e\omega$ and $Se = L_e$.*
2. *For all $s \in S$ and for all $s' \in W(s)$, $S_s \subseteq (ss')\omega$ and $Ss \subseteq L_s$. In addition $S_s = (ss')\omega$ for some $s' \in W(s)$ if and only if s is regular, in which case $Ss = L_s$ and we can assume that $s' \in V(s)$.*
3. *For all $se \in Se$ (the orbit of e), $S_{se} = (ses')\omega$ for some $s' \in W(s)$ and $Sse = L_{se}$.*
4. *For all $s \in S, s' \in W(s)$ it follows that $S_{s'} = (s's)\omega$ and $Ss' = L_{s'}$.*

Proof. 1. If $t \in S_e$ then there exists $t' \in W(t)$ such that $e = t'te = t'e$. Hence $e = e(t't) = (tet')t$ and so $e \leq t$ and $t \in e\omega$.

Conversely, if $e \leq t$ then there exists $f, g \in E$ such that $e = ft = tg$ and it is easy to check that $e = et = te$. Since $e \in W(e)$ then there exist $e' \in W(e), t' \in W(t)$ such that $e = e't'$ and so $t'te = t'tee't' = ee't' = e$ and $t \in D^e$ and since $te = e$ then $t \in S_e$ as required.

If $te \in Se$ then there exists $t' \in W(t)$ such that $e = t'te$. Hence $te\mathcal{L}e$. On the other hand, if $s\mathcal{L}e$ then there exist $u, v \in S^1$ such that $us = e, ve = s$, from which we deduce that $se = s$. If $s = e$ then obviously $s \in Se$, otherwise note that $s' = eu \in W(s)$ and so since $s'se = euse = e$ then $s \in D^e$ and $s = se \in Se$ and hence the orbit of e and $\mathcal{L}-$class containing e coincide.

2. Let $t \in S_s$ so that there exists $t' \in W(t)$ such that $s = t'ts$ and $ts = s$. Then

$$ss' = tss' = t(t'tss') = (tss't')t$$

and so $t \in (ss')\omega$. If $rs \in Ss$ then there exists $r' \in W(r)$ such that $s = r'rs$ and so $rs\mathcal{L}s$ and $Ss \subseteq L_s$.

If $(ss')\omega \subseteq S_s$ then in particular $ss' \in S_s$ and so $s' \in D^s$. Hence there exists $s'^* \in W(s')$ such that $s = s'^*s's$ and so $s = s'^* \in W(s')$ which means that s is regular and $s' \in V(s)$. Conversely, if s is regular then there exists $s' \in V(s)$ and so $ss' \in S_s$. Hence $(ss')\omega \subseteq S_s$ since S_s is closed. In this case, since $\mathcal{L}$ is a right congruence, then for any $s' \in V(s)$

$$ts \in Ss \iff t \in D^s \iff t \in D^{ss'} \iff tss' \in Sss' \iff tss'\mathcal{L}ss' \iff ts\mathcal{L}s$$

Hence $Ss = L_s$.

3. This follows from part (2) since se is regular.

4. Since s' is regular then from part(2) there exists $s'^* \in V(s')$ such that $S_{s'} = (s's'^*)\omega$ and $Ss' = L_{s'}$. But from Lemma 1.4, $s'^* = ss's$ and the result follows.

■

Let $x \in X$ and set $E^x = E \cap D^x$. In analogy with group theory, and following [6], we shall say that an $E-$dense $S-$act X is *locally free* if for all $x \in X, S_x = (E^x)\omega$.

Theorem 2.5 *Let S be an $E-$dense semigroup with semilattice of idempotents E and let X be an $E-$dense $S-$act. Then X is locally free if and only if for all $x \in X, s, t \in D^x$, whenever $sx = tx$ there exists $e \in S_x$ such that $se = te$.*

Proof. Suppose that S acts locally freely on X and that $sx = tx$ for some $x \in X, s, t \in D^x$. Then there exists $s' \in W(s)$ with $s't \in S_x$ and so there exist $f, g \in E, e \in E^x$ with $(s't)g = f(s't) = e$. Since $e \in W(e)$ then there exist $t' \in W(t), s'^* \in W(s'), f' \in W(f)$ with $e = t's'^*f'$. Hence since $ge = eg = e$, $t'te = e$ and $ss's'^* = s'^*$ then

$$se = sfs'tt's'^*f' = tt'sfs'tt's'^*f' = tt'ss'tgt's'^*f' = tt'tgt's'^*f' = tt'tge = te.$$

Conversely, suppose that $s \in S_x$ so that $sx = x$. Then there exists $s' \in W(s)$ such that $sx = s'sx$. By assumption there exists $e \in E^x$ such that $se = s'se = es's$. But $ses' = es'ss' = es'$ and so $se = (ses')s \in E^x$ and hence $s \in (E^x)\omega$ and X is locally free. ■

2.1 Graded actions

Let S be an $E-$dense semigroup with semilattice of idempotents E. We can consider E as an $E-$dense $S-$act with action given by the *Munn representation* on E. In more detail, let $e \in E$ and let $[e]$ denote the *order ideal* generated by e. This is the set

$$[e] = \{s \in S | s \leq e\} = \{s \in E | s = es = se\} = eE.$$

The second equality is easy to establish on observing that $[e] \subseteq E$ (see [14, Lemma 2.1]).

Lemma 2.6 *Let S be an ($E-$dense) semigroup with semilattice of idempotents E. Then for all $e \in E$, $[e] = W(e)$.*

Proof. If $s \in [e]$ then $s = es = se$ and so $ses = s^2 = s$. Hence $[e] \subseteq W(e)$. Conversely, if $s \in W(e)$ then $ses = s$ and so $es, se \in E$. Hence $s = ses = sees \in E$. Consequently, $s = se = es \in [e]$ and so $[e] = W(e)$. ∎

The action of S on E is given as follows. For each $s \in S$ define $D_s = \bigcup_{s' \in W(s)} [s's]$ and for each $x \in D_s \subseteq E$ define an action $s * x = sxs'$ where $x \in [s's]$ with $s' \in W(s)$. Notice that if $x \in [s^*s] \cap [s's]$ and $s', s^* \in W(s)$ then $x = s'sx = xs's$ and $x = s^*sx = xs^*s$. Consequently,

$$sxs' = sxs^*ss' = ss'sxs^* = sxs^*.$$

So the action is well-defined. Notice then that if $x \in D_{st}$ then $x \leq (st)'(st)$ for some $(st)' \in W(st)$. Since, by Lemma 1.1, $W(st) = W(t)W(s)$ then there exists $s' \in W(s), t' \in W(t)$ such that $x = t's'stx = xt's'st$. Hence $xt't = t'tx = t'tt's'stx = t's'sx = x$ and so $x \in D_t$. In addition $s's(txt') = (txt')s's = txt's'stt' = txt'$ and so $t * x \in D_s$.

Conversely, suppose that $x \in D_t$ and $t * x \in D_s$ so that $x = t'tx = xt't$ for some $t' \in W(t)$ and that $txt' = s'stxt' = txt's's$ for some $s' \in W(s)$. Then

$$xt's'st = t's'stx = t's'stxt't = t'txt't = x$$

and so $x \in D_{st}$.

Now, if $x \in D_{st}$ then for some $(st)' \in W(st), s' \in W(s), t' \in W(t)$ we have

$$(st) * x = (st)x(st)' = stxt's' = s * (txt') = s * (t * x).$$

If $s*x = s*y$ then $x = s'sx = xs's, y = s^*sy = ys^*s$ and $sxs' = sys^*$ for some $s', s^* \in W(s)$. Hence $x = s'sxs's = s'sys^*s$ and so $x \leq y$. Dually $y \leq x$ and so $x = y$.
Finally, if $x \in D_s$ then there exists $s' \in W(s)$ such that $x = s'sx = xs's$. Since $s's \in W(s's)$ then it easily follows that $x \in D_{s's}$. Consequently we have established that E is an $E-$dense $S-$act with action given as above.

Let X be an $E-$dense $S-$act. Following [18] we say that the action is *graded* if there exists a function $p : X \to E$ such that for all $e \in E, D_e = p^{-1}([e])$, and refer to p as the *grading*.

Lemma 2.7 *Let S be an $E-$dense semigroup with semilattice of idempotents E, and X a graded $E-$dense $S-$act. Then X is effective and for all $x \in X, p(x)$ is the minimum idempotent in S_x.*

Proof. Suppose that X is graded with grading $p : X \to E$ and let $x \in X$. Then as $x \in p^{-1}([p(x)]) = D_{p(x)}$ for all $x \in X$ it follows that X is effective. Notice also that $p(x) \in S_x \cap E$. Suppose that there exists $e \in S_x \cap E$. Then $x \in D_e = p^{-1}([e])$ and so $p(x) \in [e]$. Hence $p(x) \leq e$ as required. ∎

The following is fairly clear.

Proposition 2.8 *Let S be an $E-$dense semigroup with semilattice of idempotents E, and X a graded $E-$dense $S-$act with grading $p : X \to E$. Then X is locally free if and only if for all $x \in X, S_x = p(x)\omega$.*

Conversely, if X is an $E-$dense $S-$act with the property that for all $x \in X$ there exists $e_x \in E$ with $S_x = e_x\omega$, then X is locally free and graded with grading $p : X \to E$ given by $p(x) = e_x$.

Proof. Suppose that X is locally free. If $s \in (E^x)\omega$ then there exists $e \in E^x$ such that $e \leq s$. Then since $e \in S_x$ it follows that $p(x) \leq e \leq s$. On the other hand, it is clear that $p(x)\omega \subseteq (E^x)\omega \subseteq S_x$ and so $S_x = p(x)\omega$.

If $S_x = p(x)\omega$ then clearly $S_x \subseteq (E^x)\omega$. But $(E^x)\omega \subseteq S_x$ and so X is locally free.

The converse follows easily from Lemma 2.7. ∎

Notice that it follows from Lemma 2.7 that the grading function p is unique. Notice also that if $p(x)' \in W(p(x)) \cap D^{p(x)x}$ then $p(x)'p(x) \in S_x$ and so $p(x)' \in S_x$. Consequently $p(x)p(x)' \in S_x$. Moreover $p(x) \leq p(x)'p(x), p(x)p(x)'$ from which we easily deduce that $p(x) = p(x)'p(x) = p(x)p(x)'$. But then $p(x)' = p(x)'p(x)p(x)' = p(x)p(x)' = p(x)$.

Lemma 2.9 *Let S be an $E-$dense semigroup with semilattice of idempotents E and X a graded $E-$dense $S-$act with grading p. Then for $x \in D_s$, if $s's = p(x)$ for $s' \in W(s)$ then $ss' = p(sx)$.*

Proof. Suppose that $s's = p(x)$. Then $x \in D_{s's}$ and so $x \in D_s$. In addition, $sx \in D_{s'}$ and so $ss' \in S_{sx}$ which means that $p(sx) \leq ss'$. Now $s's = s'ss's \geq s'p(sx)s$ (since E is a semilattice). But since $s'p(sx)s \in S_x \cap E$ then by Lemma 2.7, $p(x) = s's = s'p(sx)s$ and so $ss' = sp(x)s' = ss'p(sx)ss'$, or in other words $ss' \leq p(sx)$. But as $ss' \geq p(sx)$ then $p(sx) = ss'$ as required. ∎

Corollary 2.10 *Let S be an $E-$dense semigroup with semilattice of idempotents E and X a graded $E-$dense $S-$act with grading p. Let $s \in S$ and $x \in D_s$. Then for all $s' \in W(s) \cap D^{sx}$, $p(sx) = sp(x)s'$.*

Proof. Let $t = sp(x)$ and let $s' \in W(s) \cap D^{sx}$. Then $t' = p(x)s' \in W(sp(x)) = W(t)$. Hence $t't = p(x)s'sp(x) = s'sp(x) = p(x)$ as $s's \in S_x$. In addition, $tx = sp(x)x = sx$ and so by Lemma 2.9, $p(sx) = p(tx) = tt' = sp(x)p(x)s' = sp(x)s'$ as required. ∎

Proposition 2.11 (Cf. [18, Proposition 1.1]) *Let S be an $E-$dense semigroup with semilattice of idempotents E and X a graded $E-$dense $S-$act with grading p and let $s \in S$. Then $D_s = \bigcup_{s' \in W(s)} p^{-1}([s's])$ and $sX = \{sx | x \in D_s\} = \bigcup_{s' \in W(s)} p^{-1}([ss'])$.*

Proof. Let $s \in S, x \in D_s, s' \in W(s) \cap D^{sx}$. Then $x \in D_{s's} = p^{-1}([s's])$ and so $D_s = \bigcup_{s' \in W(s)} p^{-1}([s's])$. Since $p(sx) = sp(x)s' = (sp(x)s')(ss') = (ss')(sp(x)s') \leq ss'$ then $p(sx) \in [ss']$ and so $sx \in p^{-1}([ss'])$. Conversely, if $y \in p^{-1}([ss']) = D_{ss'}$ then $y = ss'y = sx$ where $x = s'y$. Hence $sX = \bigcup_{s' \in W(s)} p^{-1}([ss'])$. ∎

Theorem 2.12 *Let S be an $E-$dense semigroup with semilattice of idempotents E and X an $E-$dense $S-$act. The following are equivalent.*

1. *X is a graded $E-$dense $S-$act,*
2. *there exists an $E-$dense $S-$map $f : X \to E$,*
3. *X is an effective $E-$dense $S-$act and for all $x \in X$, S_x contains a minimum idempotent.*

Proof. (1) $\implies$ (2). If $x \in D_s^X$ then from Corollary 2.10, for all $s' \in W(s) \cap D^{sx}$, $p(sx) = sp(x)s' = s * p(x)$ and $p(x) \in \bigcup_{s' \in W(s)}[s's]$. Hence $p(x) \in D_s^E$. Conversely, if $p(x) \in D_s^E$ then $p(x) \in \bigcup_{s' \in W(s)}[s's]$ and so there exists $s' \in W(s)$ such that $x \in p^{-1}([s's]) \subseteq D_s^X$. In addition $s * p(x) = sp(x)s' = p(sx)$ and it follows that p is an $S-$map.
(2) $\implies$ (3). Suppose that X is an $S-$act with an $E-$dense $S-$map $f : X \to E$ and let $x \in X$. Then as $f(x) \in D_{f(x)}^E$, it follows that $x \in D_{f(x)}^X$ and X is effective. Notice also that $f(x) \in S_x \cap E$. Suppose then that there exists $e \in S_x \cap E$. Then $x \in D_e^X$ so $f(x) \in D_e^E = [e]$ and so $f(x) \leq e$ as required.
(3) $\implies$ (1). If X is an effective $E-$dense $S-$act and for all $x \in S, S_x$ contains a minimum idempotent, say e_x, then define a function $p : X \to E$ by $p(x) = e_x$. Suppose then that $e \in E$ and $x \in D_e^X$. Then $e \in S_x \cap E$ and so $p(x) \leq e$. Hence $p(x) \in [e]$ or in other words $x \in p^{-1}([e])$ and so $D_e^X \subseteq p^{-1}([e])$. On the other hand, if $x \in p^{-1}([e])$ then $p(x) \in [e]$ and so $p(x) = p(x)e$ and since $x \in D_{p(x)}$ then $x \in D_e$ as well. Hence $D_e = p^{-1}([e])$ and p is a grading. ∎

It is easy to check that E is a graded $E-$dense $S-$act with grading $1_E : E \to E$, the identity function. The following is clear.

Corollary 2.13 *If X is an $E-$dense $S-$act and E is finite then X is graded.*

Let (X, p) and (Y, q) be graded $E-$dense $S-$acts with grading functions p and q. A *graded morphism* is an $E-$dense $S-$map $f : X \to Y$ such that $qf = p$. It is clear that graded $E-$dense $S-$acts and graded morphisms form a category and that $(E, 1_E)$ is a terminal object in this category.

2.2 Transitive $S-$acts

An $E-$dense $S-$act is called *indecomposable* if it cannot be written as the coproduct (i.e. disjoint union) of two other $E-$dense $S-$acts. In particular, a transitive $S-$act is easily seen to be indecomposable. Conversely, if X is indecomposable, then suppose that $Y = X \setminus Sx \neq \emptyset$ for some $x \in X$. Then Y cannot be a subact of X as X is indecomposable, so there exists $y \in Y, s \in S$ with $sy \in Sx$ and hence $y \in Sx$, a contradiction. Therefore $X = Sx$ is transitive. The transitive $S-$acts are therefore the 'building blocks' of $E-$dense $S-$acts. In this section, we restrict our attention, in the main, to those $E-$dense semigroups where E is a semilattice.

Suppose that S is an $E-$dense semigroup and that H is a subsemigroup of S. If for all $h \in H, W(h) \cap H \neq \emptyset$ then we will refer to H as an *$E-$dense subsemigroup of S*. For example, if E is a band then E is an $E-$dense subsemigroup of S.

Lemma 2.14 *Let S be an $E-$dense semigroup with semilattice of idempotents E and let H be an $E-$dense subsemigroup of S. Then $H\omega$ is an $E-$dense subsemigroup of S.*

Proof. Suppose that $x, y \in H\omega$ so that there exist $a, b \in H$ such that $a \leq x, b \leq y$. In addition, there exists $a' \in W(a) \cap H, b' \in W(b) \cap H$. Hence there exists $e, f, g, h \in E$ such that $a = xe = fx, b = yg = hy$. Let $x' \in W(x), f' \in W(f), y' \in W(y), h' \in W(h)$ be such that $a' = x'f' \in W(a), b' = y'h' \in W(b)$. Then

$$(xy)(y'h'hx'f'fxy) = (xyy'h'hx'f'f)(xy) = (f'f)(xhyy'h'x')(xhy) =$$
$$(f'f)(fxhyy'h'x')(xhy) = (fxhyy'h'x')(f'fxhy) = abb'a'ab \in H$$

and so $xy \in H\omega$ and $H\omega$ is a subsemigroup of S. Now suppose that $x \in H\omega$ so that there exists $h \in H$ and $e, f \in E$ such that $h = ex = xf$. Suppose also that $h' \in W(h) \cap H$ so that there exists $x' \in W(x), f' \in W(f)$ such that $h' = f'x'$. Then

$$x'(xff'x') = (x'xff')x' = ff'x'xff'x' = f'x'xfff'x' = h'hh' = h' \in H$$

and so $x' \in H\omega$ and $H\omega$ is an $E-$dense subsemigroup of S. ■

Lemma 2.15 *Let S be an $E-$dense semigroup with semilattice of idempotents E and let H be an $E-$dense subsemigroup of S. Let $x, y \in S, x' \in W(x), y' \in W(y), e \in E$. Then*

1. *if $x'ex \in H\omega$ then $x'x \in H\omega$;*
2. *if $x'ey, y'y \in H\omega$ then $x'y \in H\omega$.*

Proof. Let $x, y \in S, x' \in W(x), y' \in W(y), e \in E$. Notice that by Lemma 2.14, $H\omega$ is an $E-$dense subsemigroup of S.

1. By assumption there exists $f, g \in E, a \in H$ such that $a = (x'ex)f = g(x'ex)$. Consequently
$$a = x'exf = (x'x)(x'exf) = (x'exf)(x'x)$$
and so $a \leq x'x$ and $x'x \in H\omega$.
2. By assumption there exists $f, g \in E, a \in H$ such that $a = (x'ey)f = g(x'ey)$. Consequently
$$ay'y = x'eyfy'y = x'eyy'yf = (x'y)(y'eyf) = x'xx'eyfy'y = (x'eyfy'x)(x'y)$$
and so $ay'y \leq x'y$ and $x'y \in H\omega$ as required.

■

Proposition 2.16 *Let S be an $E-$dense semigroup with semilattice of idempotents E and let H be an $E-$dense subsemigroup of S. Then the following are equivalent*

1. *H is $\omega-$closed in S;*
2. *H is unitary in S;*
3. *H is $\omega_{\mathcal{M}}-$closed in S.*

Proof. (1) $\implies$ (2). Suppose that H is $\omega-$closed in S and suppose that $hs = h_1$ for some $s \in S, h, h_1 \in H$. Then there exists $h' \in W(h) \cap H, h'_1 \in W(h_1) \cap H$ and so there exist $s' \in W(s), h^* \in W(h)$ such that $h'_1 = s'h^* \in W(hs)$. Then

$$s(s'h'hh^*hs) = (ss'h'hh^*h)s = h'hss'h^*h_1 = h'h_1h'_1h_1 \in H$$

and so $s \in H\omega = H$. Consequently H is left unitary in S. The right unitary property follows in a similar way.
(2) $\implies$ (3). Suppose H is unitary in S and that $s \geq_{\mathcal{M}} h$ for $h \in H$. Then there exist $x, y \in S$ with $h = xs = sy, xh = hy = h$. Let $h' \in W(h) \cap H$ and notice that $h'hyh'h = h'hh'h = h'h \in H$. Therefore $y \in H$ and so $s \in H$ and H is $\omega_{\mathcal{M}}-$closed in S.
(3) $\implies$ (1). As $H \subseteq H\omega \subseteq H\omega_{\mathcal{M}}$ then this is clear. ■

In view of the above result, we shall simply say that a set A is *closed* if it is $\omega-$closed.

We briefly review Schein's theory of partial congruences when applied to $E-$dense semigroups which have a semilattice of idempotents (see [1, Chapter 7] or [7, Chapter 5] for more details of the case for inverse semigroups).

Let $T \subseteq S$ be sets and suppose that ρ is an equivalence on T. Then we say that ρ is a *partial equivalence* on S with domain T. It is easy to establish that ρ is a partial equivalence on S if and only if it is symmetric and transitive. If now T is an $E-$dense subsemigroup of an $E-$dense semigroup S and if ρ is left compatible with the multiplication on S (in the sense that for all $s \in S, (u,v) \in \rho$ either $su, sv \in T$ or $su, sv \in S \setminus T$ and $(su, sv) \in \rho$ in the former case) then ρ is called a *left congruence* on S and the set T/ρ of $\rho-$classes will often be denoted by S/ρ.

Theorem 2.17 *Let H be a closed $E-$dense subsemigroup of an $E-$dense semigroup S and suppose that E is a semilattice. Define*

$$\pi_H = \{(s,t) \in S \times S | \exists s' \in W(s), s't \in H\}.$$

Then π_H is a left partial congruence on S and the domain of π_H is the set $D_H = \{s \in S | \exists s' \in W(s), s's \in H\}$.

The (partial) equivalence classes are the sets $(sH)\omega$ for $s \in D_H$. The set $(sH)\omega$ is the equivalence class that contains s and in particular H is one of the π_H-classes.

Proof. It is clear that π_H is reflexive on D_H. Notice first that if there exists $s' \in W(s)$ such that $s't \in H$ then $s'ss't \in H$ and so since H is unitary, $s's \in H$. Suppose then that $(s,t) \in \pi_H$. Then there exists $s' \in W(s), t' \in W(t)$ such that $s's, t't, s't \in H$. Let $t^* \in W(t), s'^* \in W(s')$ be such that $t^*s'^* \in W(s't) \cap H$. Then let $x = t's$ and $x' = (s't)(t't) \in W(x)$ so that $x'^* = (t't)(t^*s'^*) \in W(x') \cap H$. By Lemma 1.4 $x'^* = (t't)x'^* \leq x$ and so $t's = x \in H$ and hence π_H is symmetric.
Now suppose that $(s,t), (t,r) \in \pi_H$. Then there exists $s' \in W(s), t' \in W(t), r' \in W(r)$ such that $s's, s't, t't, t'r, r'r \in H$. Consequently

$$(s'r)(r'tt'ss'r) = (s'rr'tt's)(s'r) = s'tt'rr'ss'r = s'tt'rr'r \in H$$

and so $s'r \in H\omega = H$ and π_H is transitive.

Suppose that $(s,t) \in \pi_H$ and that $r \in S$ and suppose further that $rs, rt \in D_H$. Then there exists $s' \in W(s), t' \in W(t)$ such that $s's, t't, s't \in H$. Further, there exists $s^* \in W(s), t^* \in W(t), r', r^* \in W(r)$ such that $s^*r'rs, t^*r^*rt \in H$. From Lemma 1.4, $s^*ss' \in W(s)$ and so $(rs)'(rt) = s^*ss'r'rt = s^*r'rss't \in H$. Hence $(rs, rt) \in \pi_H$ and π_H is a left partial congruence on S.

Now suppose that $s \in (tH)\omega$ where $t't \in H$. Then there exists $h \in H$ such that $th \leq s$ and so there exists $e, f \in E$ such that $th = se = fs$. Hence $t'th = t'se = t'fs = t'tt'fs = (t'ft)t's$ and so $t'th \leq t's$ and $t's \in H\omega = H$. Consequently $s \in [t]_{\pi_H}$. On the other hand, if $s \in [t]_{\pi_H}$ then there exists $s' \in W(s), t' \in W(t)$ such that $s's, t't, s't \in H$. Hence there exists $t^* \in W(t), s'^* \in W(s')$ such that $t^*s'^* \in W(s't) \cap H$. Now by Lemma 1.4, $tt^*s'^* \leq s$ and hence $s \in (tH)\omega$.

Finally, if $s \in D_H$ then there exists $s' \in W(s)$ such that $s's \in H$ and so $s(s's) = (ss')s \in sH$ and hence $s \in (sH)\omega$. In particular, for all $h_1, h_2 \in H$ we see that $h_1 \pi_H h_2$ and so $H = H\omega = (hH)\omega$ for all $h \in H$ is an equivalence class. ∎

The sets $(sH)\omega$, for $s \in D_H$, are called the *left $\omega-$cosets* of H in S. The set of all left $\omega-$cosets is denoted by S/H. Notice that $(sH)\omega$ is a left $\omega-$coset if and only if there exists $s' \in W(s)$ such that $s's \in H$. The following is then immediate.

Proposition 2.18 *Let H be a closed $E-$dense subsemigroup of an $E-$dense semigroup S in which E is a semilattice, and let $(aH)\omega, (bH)\omega$ be left $\omega-$cosets of H. Then the following statements are equivalent:*

1. $(aH)\omega = (bH)\omega$;
2. $a\pi_H b$ *that is, there exists* $b' \in W(b)$, $b'a \in H$;
3. $a \in (bH)\omega$;
4. $b \in (aH)\omega$.

Lemma 2.19 *With H and S as in Theorem 2.17,*

1. *precisely one left $\omega-$coset, namely H, contains idempotents,*
2. *each left $\omega-$coset is closed,*
3. *π_H is left cancellative i.e. $xa\pi_H xb$ implies that $a\pi_H b$,*
4. *$((st)H)\omega$ is an $\omega-$coset if and only if $(tH)\omega$ and $(s((tH)\omega))\omega$ are $\omega-$cosets and then $(s((tH)\omega))\omega = ((st)H)\omega$.*

Proof. 1. If e is an idempotent contained in an $\omega-$coset then there exists $e' \in W(e)$ with $e'e \in H$. As $e'e \leq e$ then $e \in H\omega = H$. As H is an $E-$dense subsemigroup of S then for each $h \in H$ there exists $h' \in W(h) \cap H$ and so $h'h \in H$ and hence $E(H) \neq \emptyset$.

2. This is clear.

3. Suppose that $(xa, xb) \in \pi_H$ so that there exists $(xa)' \in W(xa), (xb)' \in W(xb)$ such that $(xa)'(xa), (xa)'(xb) \in H$. Then there exists $x' \in W(x), a' \in W(a)$ such that $a'x'xb \in H$ and $a'x'xa \in H$. It follows from Lemma 2.15 that $a'a, a'b \in H$. Hence $a\pi_H b$.

4. Suppose that $((st)H)\omega$ is an $\omega-$coset, so that there exists $(st)' \in W(st)$ such that $(st)'st) \in H$. Then there exist $s' \in W(s), t' \in W(t)$ such that $t's' = (st)'$. Since $t's'st \in H$ and H is closed then it follows from Lemma 2.15 that $t't \in H$ and so $(tH)\omega$ is an $\omega-$coset. If $x \in (s((tH)\omega))\omega$ then there exists $y \in (tH)\omega$ such that $sy \leq x$ and so there exists $h \in H$ such that $th \leq y$. Hence there exist idempotents e_1, e_2, f_1, f_2 such that $sy = e_1 x = xf_1$ and $th = e_2 y = yf_2$. Now let $h' \in W(h)$ then $h't' \in W(th) = W(yf_2)$ and so there exists $f_2' \in W(f_2)$ and $y' \in W(y)$ such that $h't' = f_2'y'$. But $y's' \in W(sy) = W(xf_1)$ and so there exist $f_1' \in W(f_1)$ and $x' \in W(x)$ such that $y's' = f_1'x'$. Hence

$$\begin{aligned} x(f_1f_2f_2'f_1'f_1f_2x'x) &= (xf_1f_2f_2'f_1'f_1f_2x')x \\ &= sthf_2'f_1'x'xf_1f_2 = sthh't's'sth \in (st)H \end{aligned}$$

and so $x \in ((st)H)\omega$.

On the other hand, suppose that $x \in ((st)H)\omega$ so that there exists $e, f \in E, h \in H$ such that $ex = xf = sth$. Then $s(th) \leq x$ and $th \in tH \subseteq (tH)\omega$ and hence $x \in (s((tH)\omega))\omega$.

Conversely, if $(tH)\omega$ and $(s((tH)\omega))\omega$ are $\omega-$cosets then as $t \in (tH)\omega$ it follows that $st \in s((tH)\omega) \subseteq (s((tH)\omega))\omega$. Which means that $(s((tH)\omega))\omega$ is the $\omega-$coset containing st and so equals $((st)H)\omega$.

■

Notice that S_x is a closed $E-$dense subsemigroup of S for every $x \in X$.

Theorem 2.20 *For all $x \in X$, S_x is either empty or a closed $E-$dense subsemigroup of S.*

Proof. Assume that $S_x \neq \emptyset$. If $s, t \in S_x$ then $x = sx = s(tx) = (st)x$ and so S_x is a subsemigroup. Also $sx = x$ implies that $x = s'x$ for any $s' \in W(s) \cap D^{sx}$ and so S_x is an $E-$dense subsemigroup of S. Let $s \leq h$ with $s \in S_x$. Then there exist $e, f \in E$ such that $s = he = fh$. Consequently $e \in D^x$ and $h \in D^{ex} = D^x$ and so $hx = hex = sx = x$ which means that $h \in S_x$. Hence S_x is $\omega-$closed and so closed. ∎

From Lemma 2.19 we can easily deduce the following important result.

Theorem 2.21 *If H is a closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E then S/H is a transitive $E-$dense $S-$act with action given by $s \cdot X = (sX)\omega$ whenever $X, sX \in S/H$. Moreover, it is easy to establish that $S_{H\omega} = H$.*

Proof. Let $X = (rH)\omega$ be an $\omega-$coset and suppose that $s, t \in S$ and that $X \in D_{st}$. Then by Lemma 2.19, $((st)X)\omega = (st(rH)\omega)\omega$ is an $\omega-$coset and

$$(st) \cdot X = ((st)X)\omega = ((str)H)\omega = s \cdot (t \cdot X).$$

In addition if $s \cdot X = s \cdot Y$ then $(sX)\omega = (sY)\omega$ and so Lemma 2.19 $X = Y$. Now suppose that $X \in D_s$. We are required to show that there exists $s' \in W(s) \cap D^{sX}$. Suppose then that $X = (tH)\omega$ so that $s \cdot X = ((st)H)\omega$. Then there exists $(st)' \in W(st)$ such that $(st)'(st) \in H$. Hence there exist $s' \in W(s), t' \in W(t)$ such that $t's'st \in H$. Consequently, $t's'(ss's)s'st \in H$ and since $t's'(ss's) \in W(s'st)$ then there exists $(s'st)' \in W(s'st)$ such that $(s'st)'(s'st) \in H$ and so $((s'st)H)\omega$ is an $\omega-$coset of H and $s' \in W(s) \cap D^{sX}$ as required.
If $(sH)\omega$ and $(tH)\omega$ are $\omega-$cosets then there exist $s' \in W(s), t' \in W(t)$ such that $s's, t't \in H$. Now as $s'(ss's)t' = s'st' \in W(ts's)$ and as $s'st'ts's = t'ts's \in H$ then $((ts's)H)\omega$ is an $\omega-$coset. Moreover, as $(ts's)t't = tt'(ts's) \in tH$ then $ts's \in (tH)\omega$ and so $(tH)\omega = ((ts's)H)\omega = (ts') \cdot ((sH)\omega)$ and S/H is transitive.
Finally $S_{H\omega} = \{s \in S | (sH)\omega = H\omega\}$. Hence $s\pi_H h$ for any $h \in H$ and so $s \in H$ as H is an $\omega-$coset. ∎

The converse of Theorem 2.21 is also true.

Theorem 2.22 *Let S be an $E-$dense semigroup with semilattice of idempotents E, let X be an effective, transitive $E-$dense $S-$act, let $x \in X$ and let $H = S_x$. Then X is isomorphic to S/H. If K is a closed $E-$dense subsemigroup of S and if X is isomorphic to S/K then there exists $x \in X$ such that $K = S_x$.*

Proof. Let $y \in X$ and notice that since X is transitive then there exists $s \in S$ such that $y = sx$. Notice then that there exists $s' \in W(s) \cap D^{sx}$ such that $s's \in S_x = H$. Moreover if $y = tx$ for some $t \in S$ then $sx = tx$ and so $s't \in H$ and hence $(sH)\omega = (tH)\omega$. Therefore we have a well-defined map $\phi : X \to S/H$ given by

$$\phi(y) = (sH)\omega.$$

Since $\phi(sx) = (sH)\omega$ for all $(sH)\omega \in S/H$ then ϕ is onto. If $(sH)\omega = (tH)\omega$ then $s't \in H = S_x$ and so $sx = tx$ and ϕ is a bijection. Finally, suppose $\phi(y) = (sH)\omega$ and $t \in S$. Then $y \in D_t$ if and only if $t \in D^y$ if and only if $ts \in D^x$ if and only if there exists $(ts)' \in W(ts)$ such that $(ts)'(ts) \in S_x = H$ if and only if $((ts)H)\omega$ is an $\omega-$coset if and only if $\phi(y) = (sH)\omega \in D_t$. In this case it is clear that $\phi(ty) = t\phi(y)$ and ϕ is an isomorphism.

By assumption there is an isomorphism $\theta : S/K \to X$. Let $x = \theta(K\omega)$ so that $sx = \theta((sK)\omega)$ for all $s \in D_K$. Notice also that since θ is an $S-$map then $s \in D^x$ if and only if $s \in D_K$. If $s \in S_x$ then $\theta(K\omega) = \theta((sK)\omega)$ and so $s \in K$ as θ is an isomorphism. On the other hand, if $s \in K$ then $sx = \theta((sK)\omega) = \theta(K\omega) = x$ and so $s \in S_x$ as required. ∎

Recall that L_e denotes the $\mathcal{L}-$class containing e.

Theorem 2.23 *Let S be an $E-$dense semigroup with a semilattice of idempotents E and let X be a locally free, transitive, graded $E-$dense $S-$act with grading p. Then there exists $e \in E$ such that $X \cong Se \cong L_e$. Conversely, if $e \in E$ then the orbit Se of e in the $E-$dense $S-$act S (with the Wagner-Preston action) is a locally free, transitive, graded $E-$dense $S-$act.*

Proof. If X is transitive then $X \cong Sx$ for some (any) $x \in X$. Using a combination of Theorem 2.21, Proposition 2.8 and Proposition 2.4, we deduce

$$X \cong S/S_x = S/p(x)\omega \cong S/S_{p(x)} = Sp(x) = L_{p(x)}.$$

Conversely, the orbit Se is clearly a transitive $E-$dense $S-$act. By Proposition 2.4, $S_{te} = (tet')\omega$ and so by Proposition 2.8 Se is locally free and graded with grading $p : Se \to E$ given by $p(te) = tet'$. ∎

Lest X be a graded $S-$act and let $x \in X$. If $p(x) \in D_s^S$ then there exists $s' \in W(s)$ such that $p(x) = s'sp(x)$ and so it follows that $x \in D_s^X$. Conversely, if $x \in D_s^X$ then there exists $s' \in W(s) \cap D^{sx}$ and so $p(x) \leq s's$. Consequently $p(x) = s'sp(x)$ and $p(x) \in D_s^S$. Hence the map $Sp(x) \to Sx$ given by $sp(x) \mapsto sx$ is an $S-$map which is clearly onto. We have therefore demonstrated

Proposition 2.24 *Let S be an $E-$dense semigroup with a semilattice of idempotents E and let X be a graded $E-$dense $S-$act. Then X is a quotient of a locally free graded $S-$act.*

The question now arises as to when two transitive $E-$dense $S-$acts are isomorphic.

Lemma 2.25 *Let H be a closed $E-$dense subsemigroup of an $E-$dense semigroup S with a semilattice of idempotents E. Let $(sH)\omega$ be a left $\omega-$coset of H so that there exists $s' \in W(s)$ such that $s's \in H$. Then $sHs' \subseteq S_{(sH)\omega}$.*

Proof. Let $h \in H$ and consider $(shs') \cdot ((sH))\omega$. First notice that $(shs')H\omega$ is an $\omega-$coset as for any $h' \in W(h) \cap H$, $s'sh's' \in W(shs')$ and $(s'sh's')(shs's) \in H$. So $(shs') \cdot ((sH))\omega = ((shs's)H)\omega = (sH)\omega$ and so $sHs' \subseteq S_{(sH)\omega}$. ∎

If H and K are two closed $E-$dense subsemigroups of an $E-$dense semigroup S with semilattice of idempotents E, then we say that H and K are *conjugate* if $S/H \cong S/K$ (as $E-$dense $S-$acts).

Theorem 2.26 *Let H and K be closed $E-$dense subsemigroups of an $E-$dense semigroup S with semilattice of idempotents E. Then H and K are conjugate if and only if there exist $s \in S, s' \in W(s)$ such that*

$$s'Hs \subseteq K \text{ and } sKs' \subseteq H.$$

Moreover, any such element s necessarily satisfies $ss' \in H, s's \in K$.

Proof. Suppose that H and K are conjugate. Then by Theorem 2.21 there is an $\omega-$coset, $(sK)\omega$ say, such that $S_{(sK)\omega} = H$. So by Lemma 2.25 there exists $s' \in W(s)$ such that $s's \in K$ and $sKs' \subseteq H$. Hence $ss' \in H$. In addition, for each $h \in H, (hsK)\omega = (sK)\omega$ and so $hs\pi_K s$. Consequently $s'hs \in K$ and so $s'Hs \subseteq K$ as required.
Conversely suppose there exist $s \in S, s' \in W(s)$ such that $s'Hs \subseteq K$ and $sKs' \subseteq H$. Then $ss'Hss' \subseteq sKs' \subseteq H$. If $e \in E(H)$ then $ss'ess' = ess' = ss'e \in H$ and since H is unitary in S then $ss' \in H$ from which we deduce that $s's \in K$. Therefore $(sK)\omega$ is an $\omega-$coset of K in S. Now suppose that $t \in S_{(sK)\omega}$. Then $((ts)K)\omega = (sK)\omega$ and so $ts\pi_K s$. Therefore $s'ts \in K$ and so $ss'tss' \in H$ and since H is unitary in S we deduce that $t \in H$. Conversely if $t \in H$ then $s'ts \in K$ and so $s\pi_K ts$ or in other words $((ts)K)\omega = (sK)\omega$ and $t \in S_{(sK)\omega}$. Hence $H = S_{(sK)\omega}$. Define $\phi : S/H \to S/K$ by $\phi((tH)\omega) = (tsK)\omega$ and notice that ϕ is a well-defined morphism. To see this note that there exists $t' \in W(t)$ with $t't \in H$. It follows that $s'(t't)s \in K$ and since $s't' \in W(ts)$ then $((ts)K)\omega$ is an $\omega-$coset. If $(tH)\omega = (rH)\omega$ then there exists $r' \in W(r)$ such that $r'r, r't \in H = S_{(sK)\omega}$ and so $(rsK)\omega = (tsK)\omega$. Finally, as $H = S_{(sK)\omega}$ then ϕ is injective and as S/K is transitive then ϕ is onto and so an isomorphism as required. ∎

In fact we can go a bit further

Theorem 2.27 *Let H and K be closed $E-$dense subsemigroups of an $E-$dense semigroup S. Then H and K are conjugate if and only if there is exist $s \in S, s' \in W(s)$*

$$(s'Hs)\omega = K \text{ and } (sKs')\omega = H.$$

Moreover, any such element s necessarily satisfies $ss' \in H, s's \in K$.

Proof. From Theorem 2.26, if H and K are conjugate, then there exists $s \in S, s' \in W(s)$ such that

$$s'Hs \subseteq K \text{ and } sKs' \subseteq H.$$

Now it is clear that $(s'Hs)\omega \subseteq K$ so let $k \in K, k' \in W(k) \cap K$ and let $l = skk'ks' \in H$. Now put $m = s'ls = s'skk'ks's \in s'Hs$ and notice that $m \leq k$ and so $k \in (s'Hs)\omega$ as required. ∎

Notice that if $ss' \in H$ then $s'Hs$ is an $E-$dense subsemigroup of H. To see this note that it is clearly a subsemigroup and that $s'h'ss's \in W(s'hs) \cap s'Hs$ for any $h' \in W(h) \cap H$. In particular from Theorem 2.20 we immediately deduce

Proposition 2.28 *Let S be an $E-$dense semigroup with a semilattice of idempotents E and let X be an $E-$dense $S-$act. Let $s \in S$ and $x \in D_s$. Then $sS_x s'$ is an $E-$dense subsemigroup of S for any $s' \in W(s) \cap D^{sx}$.*

Theorem 2.29 *Let S be an $E-$dense semigroup with semilattice of idempotents E and let X be an $E-$dense $S-$act. Let $s \in S$ and $x \in D_s$. Then S_x and S_{sx} are conjugate.*

Proof. Since $Sx = Ssx$ the result follows from Theorem 2.22. In fact, we have that $(sS_x s')\omega = S_{sx}$ for any $s' \in W(s) \cap D^{sx}$. ∎

If H is a closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E, then we say that H is *self-conjugate* if H is only conjugate to itself.

Proposition 2.30 *Let H be a closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E. Then H is self-conjugate if and only if for all $s \in S$ and all $s' \in W(s)$ such that $s's \in H$ then $sHs' \subseteq H$.*

Proof. If $s \in S$ and $s' \in W(s)$ with $s's \in H$ then by Lemma 2.25, $sHs' \subseteq S_{(sH)\omega}$. By Theorem 2.22, $S_{(sH)\omega}$ is conjugate to H and so since H is self-conjugate, $sHs' \subseteq H$.

Conversely, suppose that K is a closed $E-$dense subsemigroup of S and that K is conjugate to H. Then by Theorem 2.21 there is an $\omega-$coset, $(sH)\omega$ say, such that $S_{(sH)\omega} = K$. Hence there exists $s' \in W(s)$ such that $s's \in H$. If $k \in K$ then $s\pi_H ks$ and so $s'ks \in H$ and in addition, since $s's \in H$ and $sHs' \subseteq H$ then $ss' = s(s's)s' \in H$. Hence $s(s'ks)s' \in sHs' \subseteq H$ and so $K \subseteq H$ as H is unitary in S. Since $ss' = (ss's)s'$ and since $ss's \in W(s')$ then $s'H(ss's) \subseteq H$ and so $s'Hs \subseteq H$ as H is unitary. Consequently, for all $h \in H, s\pi_H hs$ and so $H \subseteq S_{(sH)\omega} = K$. ∎

An alternative characterisation of self-conjugacy is given by

Proposition 2.31 *Let H be a closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E. Then H is self-conjugate if and only if for all $s, t \in S, st \in H$ implies $ts \in H$.*

Proof. If $st \in H$ then there exists $t' \in W(t), s' \in W(s)$ such that $t's' \in W(st)$ and $t's'st \in H$. Hence $(t't)(t's'st) \in H$ and so $t't \in H$. Since $tHt' \subseteq H$ then $tt' \in H$. But then $ts(tt') = tstt'tt' = t(stt't)t' \in tHt' \subseteq H$ and so $ts \in H$ as H is unitary in S.

Conversely, suppose that $s \in S, s' \in W(s)$ with $s's \in H$ and let $h \in H$. Then $s'(shs's) = (s's)h(s's) \in H$ and so $shs' = (shs's)s' \in H$ and H is self-conjugate. ∎

If H is self-conjugate then S/H has a richer structure. First notice that

Lemma 2.32 *Let H be a self-conjugate closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E. Then D_H is a closed $E-$dense subsemigroup of S.*

Proof. Let $s, t \in D_H$ and $s' \in W(s), t' \in W(t)$ with $s's, t't \in H$. By Proposition 2.31 $tt' \in H$ and since $tt't \in W(t')$ then $t'Htt't \subseteq H$. Then $t's' \in W(st)$ and $t's'st = t's'stt't \in t'Htt't \subseteq H$ so that $st \in D_H$. Further, as $ss' \in H$ and as $ss's \in W(s')$ then $s' \in D_H$. Hence D_H is an $E-$dense subsemigroup of S. Now suppose that $s \leq r$ with $r \in S$ so that there exist $e, f \in E$ such that $s = re = fr$. Hence there exists $f' \in W(f), r' \in W(r)$ such that $s' = r'f'$ Consequently, $r'rs's = r'rr'f'fr = r'f'fr = s's \in H$ and so $r'r \in H$ as H is unitary in S. Hence D_H is a closed $E-$dense subsemigroup of S. ∎

As a consequence we can deduce the following interesting result.

Theorem 2.33 *Let H be a self-conjugate closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E. Then S/H is a group under the multiplication*

$$((sH)\omega)((tH)\omega) = ((st)H)\omega.$$

Proof. The multiplication given is well defined as if $(s_1H)\omega = (s_2H)\omega$ and $(t_1H)\omega = (t_2H)\omega$ with $s_1, s_2, t_1, t_2 \in D_H$ then there exist $s_1' \in W(s_1), t_1' \in W(t_1)$ such that $s_1's_2, t_1't_2 \in H$ and so by Proposition 2.31 we have $t_2t_1' \in H$ and $s_1's_2t_2t_1' \in H$ and so $t_1's_1's_2t_2 \in H$. Hence $((s_1t_1)H)\omega = ((s_2t_2)H)\omega$ as required. Multiplication is clearly associative and it is easy to see that $H\omega$ is the identity. It is also clear that $(s'H)\omega \in W((sH)\omega)$ and so S/H is an $E-$dense monoid. Let $(sH)\omega \in E(S/H)$ so that $s's^2 \in H$. Since $s's \in H$ and H is unitary in S then $s \in H$ and so $|E(S/H)| = 1$. Hence by Lemma 1.6, S/H is a group. ∎

In particular, if H is self-conjugate and $D_H = S$ then π_H is a group congruence on S.

Proposition 2.34 *Let H be a self-conjugate closed $E-$dense subsemigroup of an $E-$dense semigroup S with semilattice of idempotents E. Then for each $s \in D_H$ $\rho_s : S/H \to S/H$ given by $\rho_s(X) = (sX)\omega$ is a bijection. The map $\rho : D_H \to \mathrm{Sym}(S/H)$ given by $\rho(s) = \rho_s$ is a semigroup homomorphism with $\ker(\rho) = \pi_H$.*

Proof. If $s, t \in D_H$ then it is clear that $\rho_{st} = \rho_s\rho_t$ and so ρ is a homomorphism. Let $X \in S/H$ so that $X = (tH)\omega$ for some $t \in D_H$. If $s \in D_H$ then $st \in D_H$ and so $\rho_s(X) = (sX)\omega = ((st)H)\omega \in S/H$. In addition there exists $s' \in D_H \cap W(s)$ and so $s's \in D_H$ and $\rho_{s's}(X) = ((s's)X)\omega = ((s'st)H)\omega = (tH)\omega = X$. In a similar way $\rho_{ss'}(X) = ((ss')X)\omega = X$ and so $\rho_{s'}$ is the inverse of ρ_s.
If $(s, t) \in \ker(\rho)$ then in particular $\rho_s(H\omega) = \rho_t(H\omega)$ and so $(s, t) \in \pi_H$. Conversely if $(s, t) \in \pi_H$ then $(sH)\omega = (tH)\omega$ and so since S/H is a group then for any $r \in D_H$, $(srH)\omega = (trH)\omega$ or in other words $(sX)\omega = (tX)\omega$ for any $X \in S/H$. Therefore $(s, t) \in \ker(\rho)$. ∎

3 Semigroup acts and the discrete log problem

Many modern cryptographic applications make implicit use of the inherent difficulty of solving the discrete log problem. In this section we consider the problem from an abstract perspective focussing on the (total) action of semigroups on sets (see [9] for more details of this approach).

Let S be a semigroup and X a (total) left $S-$act. Suppose also that the action on X is *cancellative* in the sense that for all $s \in S$ and all $x, y \in X$ if $sx = sy$ then $x = y$. For each $s \in S$ we shall call the pair (X, s) an *$S-$cryptosystem* with encryption (function) $x \mapsto sx$. We refer to x as the *plaintext*, sx as the *ciphertext* and s as the *cipher key*. Our problem is then to find a *decrypt key* t such that $(ts)x = x$.
If for $s \in S, x, y \in X$ we have $y = sx$ then we shall refer to s as the *discrete log* of y *to the base* x. The discrete log problem is then to compute s given sx and x. In general of course, the discrete log of sx may not be unique.

As an example, let $S = U_{p-1}$ be the group of units of the ring $\mathbb{Z}_{p-1}$ and $X = U_p$ the group of units of $\mathbb{Z}_p$ with p a prime. For $n \in S, x \in X$ define $n \cdot x = x^n \mod p$. By Fermat's little theorem, if x is a unit modulo p, then $x^{p-1} \equiv 1 \mod p$ and since n is coprime to $p-1$ then there is a positive integer m such that $mn \equiv 1 \mod p-1$ and hence $x^{mn} \equiv x \mod p$. Consequently m is a decrypt key for n. The usefulness of this system lie in the fact that we know of no efficient, non-quantum algorithms, to solve this particular discrete log problem.

More generally, we can let X be a finite group of order r and let S be the group of units of the ring $\mathbb{Z}_r$. Then the action $S \times X \to X$ given by $(n, x) \mapsto x^n$ is the basis of an $S-$cryptosystem, in which the inverse of any key $n \in S$ can easily be computed using the Euclidean algorithm. The case when $r = pq$ with p and q being distinct primes, forms the basis of the RSA public-key encryption system.

There are in fact a number of well-know algorithms or protocols for public key encryption which depend on the difficulty of solving the discrete log problem. For example

Example 3.1 *Massey-Omura*

Let S be a commutative semigroup that acts on a set X and suppose that for each $s \in S$ there is an *inverse element* s^{-1} with the property that $s^{-1}sx = x$ for all $x \in X$. Suppose now that Alice wants to send Bob a secure message x. She chooses a secret random element of the semigroup s, say and sends Bob the value sx. Bob also chooses a secret random element of the semigroup t, say and sends Alice the value $t(sx)$. Alice then computes

$tx = (s^{-1}s)(tx) = s^{-1}(t(sx))$ and sends this to Bob. Bob then computes $x = t^{-1}(tx)$ as required.

We can in fact remove the need for S to be commutative if we assume that X is an $(S,S)-$biact. In this case, Alice sends Bob the value sx and Bob sends Alice the value $(sx)t = s(xt)$. Alice then computes $xt = (s^{-1}s)(xt) = s^{-1}(s(xt))$ and Bob then proceeds as normal.

The beauty of such a scheme is that the values of s and t are chosen at random, do not need to be exchanged in advance and do not need to be re-used.

Example 3.2 *Generalised ElGamal encryption.*

In this system, we again assume that S is a (not necessarily commutative) semigroup that acts on a set X and that a shared secret key, $s \in S$, has previously (or concurrently) been exchanged. Alice chooses a secret random value $c \in S$, while Bob chooses a secret random value $d \in S$ and publishes sd as his public key. Alice then sends the pair of values $((c(sd))x, cs)$ to Bob, who computes $(cs)d = c(sd)$ and hence $(c(sd))^{-1}$ and so recovers x. Again the values c and d do not have to be re-used.

It is clear that if S is a group, the *inverse* element s^{-1} will always exist, namely the group inverse. For semigroups in general however this may not always be the case. We require that the stabilizers S_x be left dense in S in order to guarantee that the inverse key will exist for all $s \in S$.

Proposition 3.3 *Let S be a semigroup and X an $S-$act. The following are equivalent;*

1. *for all $x \in X$, S_x is left dense in S,*
2. *for all $x \in X$, Sx is a transitive $S-$act and $x \in Sx$,*
3. *every locally cyclic $S-$subact of X is transitive and for all $x \in X$, $x \in Sx$.*

Proof. (1) $\implies$ (2). For all $s, r \in S$ there exists $t \in S$ such that $tsx = x$ and so $(rt)sx = rx$. Hence Sx is transitive and $x \in Sx$.
(2) $\implies$ (3). Let Y be a locally cyclic $S-$subact of X and let $x, y \in Y$. Then there exists $z \in Y$ such that $x, y \in Sz$ and so since Sz is transitive then there exists $s \in S$ such that $y = sx$ as required.
(3) $\implies$ (1). Let $x \in X$ so that by assumption $x \in Sx$. It is clear that Sx is locally cyclic and so transitive. Consequently, for all $s \in S$ there exists $t \in S$ such that $t(sx) = x$ and S_x is left dense in S. ∎

We also require that X is a cancellative $S-$act. The following result is straightforward to prove, but note that we only require S to be $E-$dense in order to justify (4) $\implies$ (1).

Lemma 3.4 *Let S be an $E-$dense semigroup and X an $S-$act. The following are equivalent*

1. *X is cancellative,*
2. *for all $x \in X$, $E \subseteq S_x$,*
3. *for all $x \in X$, $E\omega \subseteq S_x$,*
4. *for all $s \in S, s' \in L(s), x \in X$ then $s's \in S_x$.*

Notice from property (4) that if X is a cancellative $S-$act then for all $x \in X, S_x$ is left dense in S. So if S is an $E-$dense semigroup then all cancellative cyclic acts are automatically transitive. So the question arises as to how we can construct a cancellative $S-$act over an $E-$dense semigroup. We do know the structure of $E-$dense transitive acts over $E-$dense semigroups and these are automatically cancellative. In fact it is then clear that if S is $E-$dense, then a total $S-$act X is cancellative if and only if it is an $E-$dense $S-$act in which for each $s \in S, D_s = X$.

Let S be an $E-$dense semigroup, let (X, s) be an $S-$cryptosystem and let $s', s'' \in L(s)$. Then for any $x \in X$ we see that

$$s'x = (s''s)(s'x) = s''(ss'x) = s''x.$$

As with $E-$dense $S-$acts we have

Lemma 3.5 *Let S be an $E-$dense semigroup and let X be a cancellative $S-$act. Then for all $x \in X, S_x$ is $\omega-$closed.*

If $K(s,x) = \{t \in S | ts \in S_x\}$, *the decrypt key space*, then we know that $W(s) \subseteq L(s) \subseteq K(s,x)$.

Theorem 3.6 *Let S be an $E-$dense semigroup, let (X, s) be an $S-$cryptosystem and let $x \in X$. Then*

1. *$K(s,x)$ is $\omega_{\mathcal{M}}-$closed,*
2. *$(S_x W(s) S_{sx})\,\omega_{\mathcal{M}} \subseteq K(s,x)$,*
3. *If E is a band then $(S_x W(s) S_{sx})\,\omega = K(s,x)$,*
4. *If S is an inverse semigroup then $K(s,x) = \left(S_x s^{-1}\right)\omega$.*

Proof. Let S, s and x be as in the statement of the theorem.

1. If $t \in K(s,x)$ and if $t \leq_{\mathcal{M}} r$ then there exist $a, b \in S$ such that $t = ar = rb, at = tb = t$. Hence if $b' \in W(b)$ then $rsx = r(bb'sx) = tb'sx = tbb'sx = tsx = x$ and so $r \in K(s,x)$.
2. Let $t \in S_x$, $s' \in W(s)$ and let $r \in S_{sx}$. Then $(ts'r)(sx) = ts'sx = tx = x$ and so $ts'r \in K(s,x)$ and the result then follows by part (1).
3. Let $t \in K(s,x)$ and notice that for any $s' \in W(s)$ and any $t' \in W(t)$ it follows that $tss't't \in S_x W(s) S_{sx}$. But $ss't't \in E$ since E is a band and $tss't' \in E$ since S is weakly self-conjugate. Hence $tss't't \leq t$ and so $K(s,x) \subseteq (S_x W(s) S_{sx})\omega$.
4. If $t \in S_x$ then $ts^{-1} = ts^{-1}ss^{-1} \in S_x L(s) S_{sx}$ and so $(S_x s^{-1})\omega \subseteq K(s,x)$. Conversely, let $t \in K(s,x)$ so that $tsx = x$. Then $tss^{-1} \in S_x s^{-1}$ and since $tss^{-1} \leq t$ the result follows.

■

In particular, if S is a group then $K(s,x) = S_x s^{-1}$ and so $|K(s,x)| = |S_x|$. A group S is said to act *freely* on a set X if for all $x \in X, S_x = \{1\}$. Clearly in this case, for each key s there is then a unique decrypt key s^{-1}. However if the action is not free then there will be more than one decrypt key for at least one $s \in S$. Notice that for the classic discrete log cipher $U_{p-1} \times U_p \to U_p$, $(n, x) \mapsto x^n$, the action is indeed a free action. Notice also that for any $E-$dense semigroup S and for all $x \in X$, $E\omega \subseteq S_x$. As with $E-$dense acts, we shall say that a cancellative $S-$act X is *locally free* if for all $x \in X, S_x = E\omega$. This is a different definition from the usual concept of freeness in $S-$acts (see [8]).

Example 3.7 *Let S be an $E-$dense semigroup with a band of idempotents E and let I be a left ideal of S. Then I is a locally free $S-$act.*

To see this suppose that $s \in S, x \in I$ and that $sx = x$. Then for $x' \in W(x), s' \in W(s)$ it follows that $sxx's's = xx's's \in E$ since E is a band. However, $sxx's's = s(xx's's) = (sxx's')s$ and since $xx's's, sxx's' \in E$ it follows that $s \geq sxx's's$ so that $S_x \subseteq E\omega$.

From the point of view of decryption, ideally we need a group acting freely on a set. However, the point of the discrete log problem is not that it is impossible to solve, but rather that it is hard to solve. Perhaps if finding one needle in a haystack is hard, then finding two, or at least a relatively small number, is equally hard. Having said that, we probably wish to minimise the size of $K(s,x)$ and so if S is an $E-$dense semigroup then we may wish to consider those semigroups for which $E\omega = E$, which in the case of those $E-$dense semigroups with a band of idempotents is, by Lemma 1.7, an $E-$unitary semigroup. We shall refer to such semigroups as $E-$*unitary dense* semigroups. Notice that in this case, if X is locally free, $K(s,x) = \{t|ts \in S_x\} = \{t|ts \in E\} = L(s)$. Notice also that by Lemma 1.5, if $|L(s)| = 1$ then S is a group.

Proposition 3.8 *Suppose that S is an $E-$unitary dense semigroup with a semilattice of idempotents E and suppose that X is a locally free cancellative $S-$act. Then for all $s \in S, x \in X, K(s,x) = (W(s))\omega$.*

Proof. By Theorem 3.6, $K(s,x) = (EW(s)E)\omega$ and by Lemma 1.4, $EW(s)E \subseteq W(s)$. Hence $K(s,x) \subseteq (W(s))\omega$. But if $s' \leq t$ for some $s' \in W(s), t \in S$ then there exist $e, f \in E$ such that $s' = et = ft$. Consequently $fts = s's \in E$ and so $ts \in E$ as S is $E-$unitary. Hence $(W(s))\omega \subseteq L(s) = K(x,s)$ and the result follows. ∎

There have been many results concerning the structure of $E-$unitary dense semigroups based on the celebrated results of McAlister ([10], [11]) and we present here a version of the one first given in [3]. First notice that if S is a semigroup and if ${}^1S$ is the monoid obtained from S by adjoining an identity element 1 (regardless of whether S already has an identity), then S is an $E-$unitary dense semigroup if and only if ${}^1S$ is an ${}^1E-$unitary dense monoid. This observation allows us to present the construction for $E-$unitary dense monoids, without much loss of generality. We use, for the most part, the terminology of [5]. Let C be a small category, considered as an algebraic object, with a set of objects, Obj C and a disjoint collection of sets, $\mathrm{Mor}(u,v)$ of morphisms, for each pair of objects $u, v \in$ Obj C. The collection of all morphisms of C is denoted by Mor C, for each object $u \in$ Obj C the identity morphism is denoted by 0_u and composition of morphisms, denoted by $p + q$ for $p, q \in$ Mor C, is considered as a partial operation on Mor C. Notice that, despite the notation, we do not assume that $+$ is commutative. For each object $u \in$ Obj C the set $\mathrm{Mor}(u,u)$ is a monoid under composition and is called the *local monoid* of C at u. We shall say that C is *locally idempotent* if each local monoid $\mathrm{Mor}(u,u)$ is a band, and that C is *strongly connected* if for every $u, v \in$ Obj $C, \mathrm{Mor}(u,v) \neq \emptyset$.
Let G be a group. An *action* of the group G on a category C, is given by a group action on Obj C and Mor C such that

1. if $p \in \mathrm{Mor}(u,v)$ then $gp \in \mathrm{Mor}(gu, gv)$,
2. $g(p+q) = gp + gq$ for all $g \in G, p, q \in$ Mor C, (whenever both sides are defined),
3. $g0_u = 0_{gu}$ for all $g \in G, u \in$ Obj C.

The action is said to be *transitive* if for all objects $u, v \in \text{Obj } C$ there exists $g \in G, gu = v$, and *free* if the action on the objects if a free action (i.e. $S_u = \{1\}$ for all $u \in \text{Obj } C$). Notice that if the action is both transitive and free then for each pair $u, v \in \text{Obj } C$ there exists a unique $g \in G$ with $gu = v$.
Now suppose that C is a strongly connected, locally idempotent category and that the group G acts transitively and freely on C. Let $u \in \text{Obj } C$ and let

$$C_u = \{(p, g) | g \in G, p \in \text{Mor}(u, gu)\}.$$

Then C_u is a monoid with multiplication defined by

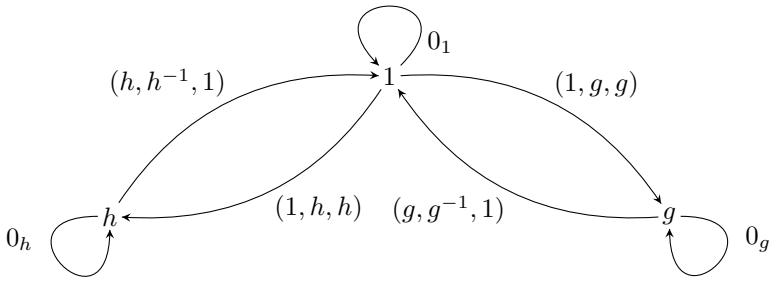
$$(p, g)(q, h) = (p + gq, gh).$$

Theorem 3.9 ([3, Proposition 3.2, Theorem 3.4]) *Let S be a monoid with band of idempotents E. Then S is $E-$unitary dense if and only if there exists a strongly connected, locally idempotent category C and a group G that acts transitively and freely on C and S is isomorphic to C_u for some (any) $u \in \text{Obj } C$.*

Notice that the idempotents of S correspond to the elements of the form $(p, 1)$. Also, as $K(s, x) = L(s)$, we see that $K((p, g), x) = \{(q, g^{-1}) \in S\}$ and so $|K((p, g), x)| = |\text{Mor}(u, g^{-1}u)|$. Consequently we see by Lemma 1.5 that S is a group if and only if for all $g \in G, |\text{Mor}(u, gu)| = 1$. In fact we see from Lemma 1.6 that in order for G not to be a group we require $|E| > 1$ (this would not be true if S is not a monoid).

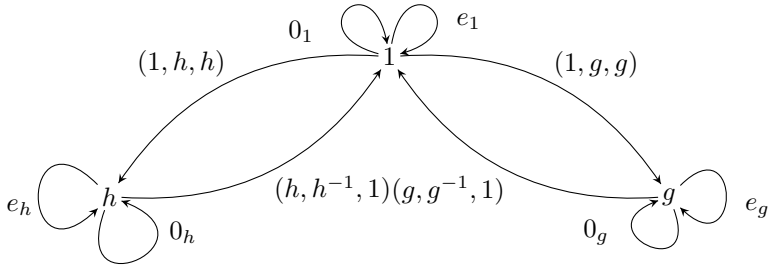
Define the *support* of the category C to be the underlying graph of C. Now consider the following category. Let $\text{Obj } C = S$ and for $u, v \in \text{Obj } C$ define $\text{Mor}(u, v) = \{(u, s, v) | s \in S, v = su\}$. This is called the *derived category* of the monoid S. The support of C is often called the *left Cayley graph* of S.

For a specific example of the above construction of an $E-$unitary dense monoid, let G be a group and let C be the derived category of G with the induced action of G on C. That is to say $g(u, s, v) = (gu, gsg^{-1}, gv)$. Then C_u is an $E-$unitary dense monoid, C is a locally idempotent category on which G acts transitively and freely and $C_u \cong C_1 \cong G$. Notice that in this case every morphism in C is an isomorphism and so C is a *groupoid*.



If we wish to work with $E-$unitary dense semigroups rather than monoids, we can simply remove the need for an identity element in $\text{Mor}(u, u)$ (see [3] for more details).

A simple modification of the previous example can provide us with an $E-$unitary dense semigroup that is not a group. Let G be a group and in the derived category of G, replace $\text{Mor}(u, u) = \{0_u\}$ with the 2-element band $\{0_u, e_u\}$. Now extend the composition of maps so that we form a category. In other words for each $u \in \text{Obj } C, g \in G$ add in the maps $e_u + (u, g, gu), (u, g, gu) + e_{gu}, e_u + (u, g, gu) + e_{gu}$. In addition we can extend the action of G accordingly so that $ge_u = e_{gu}$.



Notice then that $(u,g,gu)+e_{gu}+(gu,g^{-1},u) \in \mathrm{Mor}(u,u)$ and so must be either equal to 0_u or e_u. If it were equal to 0_u then we can add (gu,g^{-1},u) to the left and (u,g,gu) to the right to deduce that $e_u = 0_u$ which is obviously a contradiction. Hence $(u,g,gu)+e_{gu}+(gu,g^{-1},u) = e_u$ and so for all $u \in \mathrm{Obj}\ C, g \in G$ we have

$$(u,g,gu) + e_{gu} = e_u + (u,g,gu).$$

It then follows that $\mathrm{Mor}(u,gu) = \{(u,g,gu), e_u + (u,g,gu)\}$ and C_1 is an $E-$unitary dense monoid with 2 idempotents and $|K(s,x)| = 2$ for all $s \in S$ and $x \in X$. Notice that we can view this monoid in the following way. Let G be a group and e a symbol not in G and let $eG = \{eg | g \in G\}$ be a set in 1-1 correspondence with G. Let $S = G \dot\cup eG$ and extend the multiplication on G to S by setting $e^2 = e$, $eg = ge$ for all $g \in G$ and all other products defined by associativity or the multiplication in G. Then $S \cong C_1$ and the isomorphism is given by $g \mapsto ((1,g,g),g), eg \mapsto (e_1 + (1,g,g),g) = (e_1,1)((1,g,g),g)$. The element e corresponds to $(e_1,1) \in C_1$.

By replacing $\mathrm{Mor}(u,u)$ by a band of any given size, we should be able to construct an $E-$unitary dense monoid with any finite number of idempotents.

The above construction gives us a mechanism to build a suitable $E-$unitary dense semigroup S. However we need X to be a locally free cancellative $S-$act, so let us revisit the theory of $E-$dense $S-$acts. If S is finite (or at least E is finite) and E is a semilattice, then every $E-$dense act is graded and so by Theorem 2.23, X is a locally free $E-$dense $S-$act if and only if $X \cong \dot\bigcup Se_i$ for some idempotents e_i, where the action is that given in Example 2.2. As previously observed, if X is a cancellative total act then it is automatically reflexive and hence an $E-$dense act. Consequently, if X is locally free then as every idempotent acts on e_i, we can deduce that for each $i, e_i = f$, the minimum idempotent in S. Conversely if f is the minimum idempotent in S then $Sf \cong S/f\omega$ is a locally free transitive cancellative total $S-$act. We have therefore shown

Theorem 3.10 *Let S be a finite $E-$dense semigroup with semilattice of idempotents E, let $s \in S$ and let f be the minimum idempotent in S. Then (X,s) is a locally free $S-$cryptosystem if and only if $X \cong \dot\bigcup Sf$. In addition, if S is $E-$unitary then for each $x \in X, |K(s,x)| = |(W(s))\omega|$.*

In the above example where $S = G \dot\cup eG$, the minimum idempotent is e and $X = eG = Ge$ is a locally free cancellative $S-$act and for each $x \in X, |K(s,x)| = 2$. In the classic discrete log cipher, U_{p-1} acts freely on U_p by exponentiation, the minimm idempotent is $1 \in U_{p-1}$ and in fact $U_p \cong \dot\bigcup_{|U_p|} U_{p-1}$.

3.1 Completely Regular Semigroups

In the classic discrete log cipher, a group acts freely on a group by exponentiation. We now briefly consider a group acting freely on a semigroup by exponentiation. It is clear that the semigroup needs to be periodic as every element will need to have finite order.

A semigroup S is called *completely regular* if every element of S belongs to a subgroup of S. A particular example of such a semigroup is a *completely simple* semigroup, which by Rees' Theorem ([7, Theorem 3.2.3]), can be shown to be isomorphic to a Rees Matrix Semigroup. Indeed a semigroup is completely regular if and only if it is isomorphic to a semilattice of completely simple semigoups ([7, Theorem 4.1.3]). A semigroup $S = \mathcal{M}[G; I, \Lambda; P]$ is a called a *Rees Matrix Semigroup* if

$$S = I \times G \times \Lambda$$

and $P = (p_{\lambda i})$ is a $\Lambda \times I$ matrix with entries in the group G, and where multiplication is given by

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu).$$

If follows that for $n \in \mathbb{N}, (i, g, \lambda)^n = (i, (gp_{\lambda i})^{n-1}g, \lambda)$. Notice that S is not in general commutative, even if G is abelian.

Suppose now that S is a completely simple semigroup, considered as a Rees matrix semigroup $\mathcal{M}[G; I, \Lambda; P]$ and suppose also that G is finite, of order r so that $g^r = 1$ for all $g \in G$. Define an action of U_r, the group of units in $\mathbb{Z}_r$, on S by $n \cdot x = x^n$, so that if $x = (i, g, \lambda)$ then $n \cdot x = (i, (gp_{\lambda i})^{n-1}g, \lambda)$. This action is clearly a free action and group actions are always cancellative.

Suppose now that n is coprime to r and that $mn \equiv 1 \mod r$. Then

$$x^{mn} = (i, (gp_{\lambda i})^{mn-1}g, \lambda) = (i, (gp_{\lambda i})^{mn}p_{\lambda i}^{-1}, \lambda) = (i, (gp_{\lambda i})p_{\lambda i}^{-1}, \lambda) = (i, g, \lambda) = x.$$

Consequently if we know n, x^n and P, then we can compute x^{mn} and so recover x. We can in fact compute x^{mn} in an efficient manner, as we can deduce the values of i and λ from x^n and so we can compute $p_{\lambda i}$. Then

$$(gp_{\lambda i})^{mn-1}g = (gp_{\lambda i})^{mn}p_{\lambda i}^{-1} = \left(\left((gp_{\lambda i})^{n-1}g\right)p_{\lambda i}\right)^m p_{\lambda i}^{-1}.$$

Suppose now we know x, x^n and G. Can we compute n? If we also know P then we know $p_{\lambda i}$ and so $(gp_{\lambda i})^n$. Consequently, the discrete log problem in this case is equivalent to that in the classic discrete log problem. Suppose however that P is secret. We know $(gp_{\lambda i})^{n-1}g$ and we know g and so we can compute $(gp_{\lambda i})^{n-1}$ but we don't know $p_{\lambda i}$ and so can't obviously recover the classic discrete log problem from this. However, according to [4], the discrete log problem here, can be reduced, in polynomial time, to the classic discrete log problem in a subgroup of S, namely the kernel of the element x.

An alternative strategy might be to utilise the matrix P to form a kind of "Vigenère" version of the discrete log cipher. Here, the data to be enciphered would be encoded using the group G alone as with the classic discrete log cipher, and an additional keyword would be used to generate a large sequence of values $(i, \lambda)_j$ with the j^{th} such pair used to encipher the j^{th} plaintext block using the scheme above. In principle different data blocks, even if containing the same value, would produce different ciphertext blocks, thereby potentially increasing the diffusion.

References

[1] A.H. Clifford and G.B. Preston, *The Algebraic Theory of Semigroups II, American Mathematical Society, Mathematical Surveys 7*, AMS, 1967.

[2] Ahsan, Javed and Liu Zhongkui, *A Homological Approach to the Theory of Monoids*, Science Press, Beijing, (2008).

[3] J. Almeida, J.E. Pin and P. Weil, Semigroups whose idempotents form a subsemigroup, *Math. Proc. Camb. Phil. Soc.* (1992), 111241–253.

[4] Matan Banin, Boaz Tsaban, A reduction of Semigroup DLP to Classic DLP, *Designs, Codes and Cryptography*, (2016), Volume 81, Issue 1, 75–82.

[5] John Fountain, Jean-Eric Pin, Pascal Weil, *Covers for monoids*, Journal of Algebra, 271 (2004) 529–586.

[6] Jonathon Funk and Pieter Hofstra, Topos theoretic aspects of semigroup actions, *Theory and applications of Categories*, Vol 24, No. 6, 2010, pp. 117–147.

[7] J.M. Howie, *Fundamentals of Semigroup Theory*, London Mathematical Society Monographs, (OUP, 1995).

[8] Kilp, Mati, Knauer, Ulrich and Alexander V. Mikhalev, *Monoids, Acts and Categories*, De Gruyter Expositions in Mathematics **(29)**, (Walter de Gruyter, Berlin, New York, 2000).

[9] Maze, G., Monico, C., Rosenthal, J., Public key cryptography based on semigroup actions, *Adv. Math. Commun.*, **1**(4), 489–507 (1996).

[10] D. B. McAlister. Groups, semilattices and inverse semigroups. I. *Trans. Amer. Math. Soc.* 192 (1974) 227-244.

[11] D. B. McAlister. Groups, semilattices and inverse semigroups. II. *Trans. Amer. Math. Soc.* 196 (1974) 351-370.

[12] H. Mitsch, A Natural Partial Order for Semigroups, *Proceedings of the American Mathematical Society*, Vol. 97, No. 3 (Jul., 1986), pp. 384-388.

[13] H. Mitsch, Subdirect Products Of $E-$inversive Semigroups, *J. Austral. Math. Soc.* (Series A) 48 (1990), 66–78

[14] H. Mitsch, Semigroups and their natural order, *Mathematica Slovaca*, Vol 44 (1994), No 4, 445-462.

[15] H. Mitsch, *Introduction to $E-$inversive semigroups, in "Proceedings of the International Conference on Semigroups. Ed. Paula Smith, Emilia Giraldes, Paula Martins, World Scientific*, 1999, 114–135.

[16] J. Renshaw, *Inverse semigroups acting on graphs in "Proceedings of the Workshop Semigroups and Languages. Ed. Isabel M. Araújo, Mário J.J. Branco, Vitor H. Fernandes, Graconda M.S. Gomes, World Scientific*, 2004, 212–239.

[17] S. Reither, *Die nat urliche Ordnung auf Halbgruppen*, University of Vienna, PhD-Thesis (1994).

[18] Benjamin Steinberg, *A note on amalgams of inverse semigroups* Journal of the Australian Mathematical Society (2001), 70: 71-75.

[19] G. Thierrin, Demigroupes inversés et rectangularies, *Bull. Cl. Sci. Acad. Roy. Belgique*, (1955) **41**, 83–92.

[20] B. Weipoltshammer, On classes of $E-$inversive semigroups and semigroups whose idempotents form a subsemigroup, *Comunications in Algebra*, Vol 32, No 8, pp. 2929–2948 (2004).