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

Jim Renshaw

January 25, 2018

UNIVERSITY OF Southampton
School of Mathematics

Outline

1. Background
   - Discrete Log Cipher
   - $E-$dense semigroups
2. $E-$dense acts
   - Transitive acts
   - Graded acts
3. Applications to cryptography
   - Semigroup Actions
   - Completely Regular Semigroups

Discrete Log

- Choose a large prime p and a residue n coprime to $p - 1$.
- Encode data using integers in $\mathbb{Z}_p$.
- Encrypt data using the function $x \mapsto x^n \mod p$.
- Decrypt using the function $x \mapsto x^m \mod p$ where $nm \equiv 1 \mod (p-1)$.

Discrete Log

- More algebraically, 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 $\mathbb{Z}_p$.
- For $n \in S, x \in X$ define an action of S on X by $n \cdot x = x^n$.
- 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 $x^{mn} \equiv x \mod p$.
- The usefulness of this system lies in the fact that we know of no efficient, non-quantum algorithms, to solve this particular *discrete log problem* - given x, x^n and p, calculate n.

Discrete Log

- Let S be a semigroup acting on a set X.
- Call $x \in X$ the *plaintext*, $s \in S$ the *key*, and $sx \in X$ the *ciphertext*.
- Given $x \neq y$ we clearly require $sx \neq sy$ - different plaintexts give rise to different ciphertexts.
- For each $x \in X$, $s \in S$ we also require that there exists $s' \in S$ with $s'(sx) = x$ - each ‘encrypt’ key has a corresponding ‘decrypt’ key.

Discrete Log

- Notice this means that if $e = e^2$ then $x = ex$ ...
- ... and for each $s \in S$ there exists $s' \in S$ with $s's \in S_x = \{t \in S | tx = x\}$ - the *stabilizer* of x in S.
- 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.
- So we require that the stabilizers be left dense in S.

Discrete Log

- When $T = E$ 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 and subsequently by a large number of authors.
- 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.

Discrete Log

Example (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.

Discrete Log

Example (Massey-Omura)

We can in fact remove the need for S to be commutative if we assume that X is an $(S, S)-$biact.

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.

Discrete Log

Example (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.

$E-$dense semigroups

Let S be an $E-$dense semigroup, let $L(s) = \{s' \in S | s's \in E\}$ and let

$$W(s) = \{s' \in S | s'ss' = s'\}$$

be the set of *weak inverses* of s.

Notice that if $s's \in E$ then $s'ss' \in W(s)$ and $(s'ss')s = s's$.

Conversely, if $s' \in W(s)$ then $s's \in E$.

$E-$dense semigroups

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

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

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 $A \subseteq A\omega$. It is also clear that $(A\omega)\omega = A\omega$.

We say that A is *closed* in S if $A\omega = A$.

$E-$dense semigroups

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 (Reither (94))

Let S be an $E-$dense semigroup. Then S is $E-$unitary if and only if E is a band and $E\omega = E$.

$E-$dense acts

Let S be an $E-$dense semigroup, let X be a non-empty set and let $S \times X \to X$ be a ‘partial’ action with the property that $(st)x$ exists if and only if tx and $s(tx)$ exists and then $(st)x = s(tx)$.

We say that the action 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.

$E-$dense acts

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

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

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 $s' \in W(s)$.

$E-$dense acts

Example (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) - in other words the action on X is a total action. For each $s \in S$ define

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

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

$E-$dense acts

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

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

- 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 $x = sz, y = tz$.

Transitive acts

Lemma

An $E-$dense $S-$act is effective and transitive if and only if it has only one $S-$orbit.

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

The transitive acts are precisely the *indecomposable* $E-$dense acts.

Transitive acts

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.

Proposition

Let S be an $E-$dense semigroup with semilattice of idempotents E and let H be an $E-$dense subsemigroup of S. Then H is closed in S if and only if H is unitary in S.

Transitive acts

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.

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 then ρ is called a *left partial congruence* on S and the set T/ρ of $\rho-$classes will be denoted by S/ρ.

Transitive acts

Theorem

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 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.

Transitive acts

Theorem

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 $X, sX \in S/H$.

Theorem

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.

Locally Free acts

In analogy with group theory, and following Funk (2010), 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

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 $se = te$.

Graded acts

Let S be an $E-$dense semigroup, let $e \in E$ and let $[e]$ denote the *order ideal* generated by e. This is the set

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

Let X be an $E-$dense $S-$act. Following Steinberg (2001) 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*.

Graded acts

Proposition

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 $p(x) = e_x$.

Locally free, transitive and graded

Theorem

Let S be an $E-$dense semigroup with a semilattice of idempotents E. Then X is a locally free, transitive, graded $E-$dense $S-$act if and only if there exists $e \in E$ such that $X \cong Se \cong L_e$.

Graded acts

It is easy to check that E is a graded $E-$dense $S-$act with action given by $s * e = ses'$ for $s' \in W(s)$, and with grading $1_E : E \to E$, the identity function.

Theorem

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.*

Graded acts

Corollary

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

Decrypt Keys

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

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 closed,*
2. $(S_x W(s) S_{sx})\omega \subseteq K(s,x)$*,*
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* $K(s,x) = \left(S_x s^{-1}\right)\omega$*.*
5. *If S is a group then* $K(s,x) = S_x s^{-1}$*.*

Decrypt Keys

To minimise the size of $K(x,s)$ we may wish to restrict attention to locally fee acts where $S_x = E\omega$ and to $E-$unitary semigroups where $E\omega = E$ (when E is a band).

Such semigroups will be referred to as *$E-$unitary dense semigroups*.

In this case it turns out that

$$K(s,x) = \{t | ts \in S_x\} = \{t | ts \in E\} = L(s) = (W(s))\omega.$$

$E-$unitary dense semigroups

Let C be a small category with a set of objects, $\mathrm{Obj}\ C$ and a disjoint collection of sets, $\mathrm{Mor}(u, v)$ of morphisms, for each pair of objects $u, v \in \mathrm{Obj}\ C$.

The identity morphism on u is denoted by 0_u and composition of morphisms is denoted by $p + q$.

For each object $u \in \mathrm{Obj}\ C$ the set $\mathrm{Mor}(u, u)$ is a monoid under composition and is called the *local monoid* of C at u.

C is *locally idempotent* if each local monoid $\mathrm{Mor}(u, u)$ is a band, and C is *strongly connected* if for every $u, v \in \mathrm{Obj}\ C$, $\mathrm{Mor}(u, v) \neq \emptyset$.

$E-$unitary dense semigroups

Let G be a group. An *action* of the group G on a category C, is given by a group action on $\mathrm{Obj}\ C$ and $\mathrm{Mor}\ C$ 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 $g \in G, p, q \in \mathrm{Mor}\ C$, (whenever both sides are defined),
3. $g0_u = 0_{gu}$ for all $g \in G, u \in \mathrm{Obj}\ C$.

The action is said to be *transitive* if for all objects $u, v \in \mathrm{Obj}\ C$ 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 $u \in \mathrm{Obj}\ C$).

$E-$unitary dense semigroups

Now suppose that C is a strongly connected, locally idempotent category and that the group G acts transitively and freely on C. Let $u \in \mathrm{Obj}\ C$ and let

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

Then C_u is a monoid with multiplication defined by

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

$E-$unitary dense semigroups

Theorem (Almeida, Pin, Weil 1992)

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) $u \in \mathrm{Obj}\ C$.

$E-$unitary dense semigroups

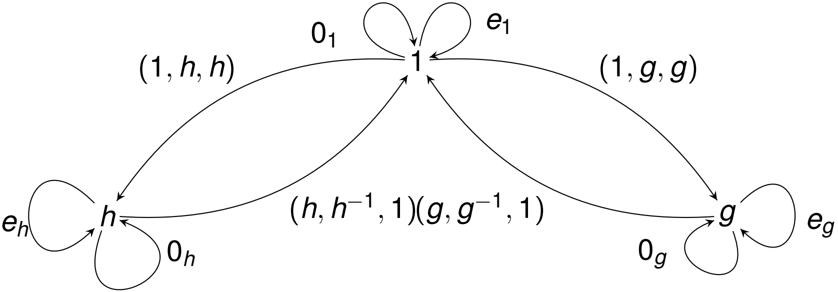
Let $\mathrm{Obj}\ C = G$, a group, and for $u, v \in \mathrm{Obj}\ C$ define $\mathrm{Mor}(u, v) = \{(u, g, v) | g \in G, v = gu\}$.

This is called the *derived category* of the group G. The underlying graph is often called the *left Cayley graph* of G.

The induced action of G on C is given by $g(u, s, v) = (gu, gsg^{-1}, gv)$.

Then C_u is an $E-$unitary dense monoid 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*.

$E-$unitary dense semigroups



$E-$unitary dense semigroups

Let S be finite (or at least E is finite) and E a semilattice so that every $E-$dense act is graded and so 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 by the Wagner-Preston action.

If X is a locally free total act 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.

$E-$unitary dense semigroups

Theorem

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 $x \in X, |K(s, x)| = 2$.

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.

We will in fact restrict our attention to completely regular semigroups where every element lies in a subgroup of S.

Completely Regular semigroups

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.

Completely Regular semigroups

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.

Completely Regular semigroups

Suppose now we know x, x^n and G. Can we compute n? f 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.

So P has to be kept secret.

Completely Regular semigroups

Computing n using trial multiplication attack would consists of computing $g^m q^{m-1}$ for $1 \leq m \leq n$ and $q \in G$ in order to find the relevant pair (n, p_i).

If $gcd(m-1, |G|) = 1$ then there exists k such that $k(m-1) \equiv 1 \mod |G|$ and so for any $q \in G, q^{k(m-1)} = q$. Consequently

$$g^n p_i^{n-1} = g^m \left(\left(g^{n-m} p_i^{n-1} \right)^k \right)^{m-1}$$

and so there is no unique pair (n, p_i) that can be computed by simple trial multiplication attack alone.