Publ. Math. Debrecen
72/3-4 (2008), 335–346

Normal $\widetilde{\mathcal{H}}$-abundant cryptographs

By XIANGZHI KONG (Wuxi) and K. P. SHUM (Hong Kong)

Abstract. Properties of the Green $\sim$-relations in $\widetilde{\mathcal{H}}$-abundant cryptographs are investigated and the semilattice decomposition of an $\widetilde{\mathcal{H}}$-abundant cryptograph is considered. By using the semilattice decomposition, we will show that a normal $\widetilde{\mathcal{H}}$-abundant cryptograph can be expressed by a strong semilattice of $\widetilde{\mathcal{J}}$-simple cryptogroups. This result not only generalizes the well known theorem of normal cryptogroups given by Petrich in 1974 and also the theorem of super abundant semigroups given by Fountain in 1982. In addition,our theorem extends some of the recent results obtained by Ren–Shum on superabundant semigroups which are orthodox.

1. Introduction

It is well known that Green's relations play an important role in the theory of regular semigroups [1]–[2]. The celebrated theorem of CLIFFORD [2] states that a semigroup is a union of groups if and only if it is a semilattice of completely simple semigroups, where a union of groups is in fact a semigroup in which every $\mathcal{H}$-class contains an idempotent. By using the strong semilattice decomposition, PETRICH [11] showed that a completely regular semigroup is a normal cryptogroup if and only if it is a strong semilattice of completely simple semigroups. By a normal cryptogroup, we mean a completely regular semigroup whose Green relation $\mathcal{H}$ is

Mathematics Subject Classification: 20M10.
Key words and phrases: Green $\sim$-relations, strong semilattice decomposition of semigroups, $\widetilde{\mathcal{J}}$-simple cryptogroups, normal $\widetilde{\mathcal{H}}$-abundant cryptographs, normal bands.
The research of the first author is supported by a NSF of Shandong Province, P. R. China (Y2005A11).
The research of the second author is partially supported by a RGC direct grant (CUHK, Hong Kong), 2005–06.

a normal band congruence. The theorem of Petrich was generalized by FOUNTAIN [4] in 1982 and in fact,he proved that an abundant semigroup S is a superabundant semigroup (that is, an abundant semigroup in which every $\mathcal{H}^*$-class of S contains an idempotent) if and only if S can be expressed by a semilattice of completely $\mathcal{J}^*$-simple semigroups. Thus, the theorem of FOUNTAIN [4] has been further modified by REN–SHUM to superabundant semigroups in [13] and [14].

The following Green*-relations were first introduced by PASTIJN [9] and used by FOUNTAIN [4] to study the structure of abundant semigroups:

$$\mathcal{L}^* = \{(a,b) \in S \times S : (\forall x, y \in S^1)ax = ay \Leftrightarrow bx = by\},$$
$$\mathcal{R}^* = \{(a,b) \in S \times S : (\forall x, y \in S^1)xa = ya \Leftrightarrow xb = yb\},$$
$$\mathcal{H}^* = \mathcal{L}^* \cap \mathcal{R}^*,\ \mathcal{D}^* = \mathcal{L}^* \vee \mathcal{R}^*.$$

Later on, in studying the adequate semigroups, EL-QALLALI [3] generalized the Green*-relations to the *Green*$\sim$-relations on a semigroup S as following:

$$\widetilde{\mathcal{L}} = \{(a,b) \in S \times S : (\forall e \in E(S))ae = a \Leftrightarrow be = b\},$$
$$\widetilde{\mathcal{R}} = \{(a,b) \in S \times S : (\forall f \in E(S))a = fa \Leftrightarrow b = fb\},$$
$$\widetilde{\mathcal{H}} = \widetilde{\mathcal{L}} \cap \widetilde{\mathcal{R}},\ \widetilde{\mathcal{D}} = \widetilde{\mathcal{L}} \vee \widetilde{\mathcal{R}}.$$

It can be easily seen that $\widetilde{\mathcal{L}}$ and $\widetilde{\mathcal{R}}$ are equivalences on a semigroup S , but $\widetilde{\mathcal{L}}$ need not to be right compatible with the semigroup multiplication and $\widetilde{\mathcal{R}}$ need not to be left compatible with the semigroup multiplication , same as the $\mathcal{L}$, $\mathcal{L}^*$, $\mathcal{R}$ and $\mathcal{R}^*$-relations respectively. The $\widetilde{\mathcal{L}}$-class containing the element a of the semigroup S will be denoted by $\widetilde{L}_a$ or by $\widetilde{L}_a(S)$ if no ambiguity arises. We can easily see that $\mathcal{L} \subseteq \mathcal{L}^* \subseteq \widetilde{\mathcal{L}}$. Among the usual Green relations or the above generalized Green relations, the relation $\mathcal{L}$ or the generalized $\mathcal{L}$-relations, say $\mathcal{L}^*$ or $\widetilde{\mathcal{L}}$, are the dual of the corresponding $\mathcal{R}$-relations. Hence, in what follows, we only discuss the properties related to the $\mathcal{L}$ relation or to the generalized $\mathcal{L}$-relations. One can easily see that there is at most one idempotent contained in each $\widetilde{\mathcal{H}}$-class [4]. If $e \in \widetilde{\mathcal{H}}_a \cap E(S)$, for some $a \in S$, then we write e as x^0, for any $x \in \widetilde{\mathcal{H}}_a$. Clearly, for any $x \in \widetilde{\mathcal{H}}_a$ with $a \in S$, we have $x = xx^0 = x^0x$.

If a semigroup S is regular, then every $\mathcal{L}$-class of S contains at least one idempotent, and so does every $\mathcal{R}$-class of S. If S is a completely regular semigroup, then every $\mathcal{H}$-class of S contains an idempotent. A semigroup S is called *abundant* [4] if every $\mathcal{L}^*$- and $\mathcal{R}^*$-class of S contains an idempotent. One can also see that $\mathcal{L}^* = \mathcal{L}$ on the regular elements of the semigroup S. Thus, abundant semigroups

are generalized regular semigroups. We call a semigroup S *superabundant* if each of its $\mathcal{H}^*$-classes contains an idempotent. Clearly, superabundant semigroups are generalization of completely regular semigroup in the class of abundant semigroups. Accordingly, we call a semigroup S *semiabundant* if both its $\widetilde{\mathcal{L}}$-class and $\widetilde{\mathcal{R}}$-class of S contains at least one idempotent. In particular, we call a semigroup S $\widetilde{\mathcal{H}}$*-abundant* if each of its $\widetilde{\mathcal{H}}$-classes contains an idempotent. Thus, an $\widetilde{\mathcal{H}}$-abundant semigroup is just a special semiabundant semigroups. The structure of semiabundant semigroup has been recently investigated by Guo–Shum [5] and some analogous cryptogroups and $\widetilde{\mathcal{H}}$ cryptogroups and cryptographs have been studied by Kong, Yuen and Shum (see [7] and [8]).One can easily see that $\widetilde{\mathcal{L}} = \mathcal{L}$ always holds on the regular elements in any $\widetilde{\mathcal{H}}$-abundant semigroup.

Recall that a *normal band* is a band satisfying the identity $axya = ayxa$ (see 5]) and a semigroup S is called *cryptic* if its Green $\sim$-relation $\widetilde{\mathcal{H}}$ is a congruence on S [10]. For completely regular semigroups, Petrich–Reilly [10] called these kind of semigroups the cryptogroups if their Green $\sim$-relation $\widetilde{\mathcal{H}}$ is a regular band congruence. In other words, a completely regular semigroup S is a regular cryptogroup if the set of all idempotents of S forms a regular band. Since abundant semigroups are generalization of completely regular semigroups, we naturally call a $\widetilde{\mathcal{H}}$-abundant semigroup a *normal* $\widetilde{\mathcal{H}}$*-abundant cryptograph* if the *Green*$\sim$-relation $\widetilde{\mathcal{H}}$ is a normal band congruence. Consequently, we call a $\widetilde{\mathcal{H}}$-abundant semigroup whose set of idempotents forms a normal band a normal $\widetilde{\mathcal{H}}$-abundant cryptograph. It is noteworthy that if S is an $\widetilde{\mathcal{H}}$-abundant semigroup,then the relation $\widetilde{\mathcal{H}}$ is always a congruence of S.Thus, we remark here that the $\widetilde{\mathcal{H}}$-classes in a $\widetilde{\mathcal{H}}$-abundant cryptograph S are submonoids of S. For notations and terminologies not mentioned in this paper, the reader is referred to [6] and [12].

In this paper, we concentrate to study the structure of normal $\widetilde{\mathcal{H}}$-abundant cryptographs. Our result not only generalizes the result of Petrich [11] on normal cryptogroups in 1974 and also the results of Fountain [4] in 1982. Also, we extend some recent results of Ren–Shum on superabundant semigroups which are orthodox to $\widetilde{\mathcal{H}}$-abundant cryptographs (see [13] and [14]).

For the sake of convenience, we first restate the definition of strong semilattice of semigroups. (see [7], for example).

Definition 1.1. Let the semigroup $S = (Y; S_\alpha)$ be the semilattice Y of semigroups $S_\alpha (\alpha \in Y)$. Suppose that for any $\alpha \geqslant \beta$ on Y, there is a homomorphism $\phi_{\alpha,\beta}$ from S_α into S_β such that

(i) $(\forall \alpha \in Y)\ \phi_{\alpha,\alpha} = 1_{S_\alpha}$ is the identity automorphism of S_α;

(ii) $(\forall \alpha, \beta, \gamma \in Y, \alpha \geqslant \beta \geqslant \gamma)\ \phi_{\alpha,\beta}\phi_{\beta,\gamma} = \phi_{\alpha,\gamma}$;

(iii) $(\forall a \in S_\alpha, b \in S_\beta)\ ab = (a\phi_{\alpha,\alpha\beta})(b\phi_{\beta,\alpha\beta})$.

Then we call S the strong semilattice of semigroups S_α and denote it by $S = [Y; S_\alpha, \phi_{\alpha,\beta}]$. The homomorphism $\phi_{\alpha,\beta}$ is called the *structural homomorphism*.

2. Preliminaries

We have already defined the *Green*$\sim$-relations $\widetilde{\mathcal{L}}$, $\widetilde{\mathcal{R}}$ and $\widetilde{\mathcal{H}}$ $\widetilde{\mathcal{D}}$. In order to define $\widetilde{\mathcal{J}}$, we first introduce the *left (right)* $\widetilde{ideal}$ of a semigroup S to be a left(right) ideal I of S such that $\widetilde{L}_a \subseteq I$ ($\widetilde{R}_a \subseteq I$,) for all $a \in I$. A subset I of S is now called a $\widetilde{ideal}$ *of* S if it is both a left $\widetilde{ideal}$ and a right $\widetilde{ideal}$ of S. By the fact that S is a $\widetilde{ideal}$ of S, we denote the smallest $\widetilde{ideal}$ containing the element a of S by $\widetilde{J}(a)$ and define $\widetilde{\mathcal{J}} = \{(a,b) \in S \times S : \widetilde{J}(a) = \widetilde{J}(b)\}$. We note that if S is regular, then every left(right, two-sided) ideal of S is a left(right, two-sided) $\widetilde{ideal}$ of S. We also observe that for an idempotent e in any semigroup S the left (right) ideal $Se(eS)$ is a left (right) $\widetilde{ideal}$. For if $a \in Se$, then $a = ae$, and hence for any element b in $\widetilde{L}_a$ we have $b = be \in Se$. If an $\widetilde{\mathcal{H}}$-abundant cryptograph S does not contain any proper $\widetilde{ideal}$ of S, then we call S a *completely regular* $\widetilde{\mathcal{J}}$*-simple semigroup*. We note here that a *completely regular* $\widetilde{\mathcal{J}}$*-simple semigroup* S is already a cryptogroup under the terminology of Petrich–Reilly [10] because $\widetilde{\mathcal{H}}$ is a group congruence on S.

We have the following lemmas for $\widetilde{\mathcal{H}}$-abundant semigroups and $\widetilde{\mathcal{H}}$-abundant cryptographs.

Lemma 2.1. *A semigroup S is a $\widetilde{\mathcal{H}}$-abundant semigroup if and only if $(ab)^0 = (a^0b^0)^0$, for all a and b in S.*

Proof. *Necessity.* For any $a, b \in S$, we have $a\widetilde{\mathcal{H}}a^0$ and $b\widetilde{\mathcal{H}}b^0$. Since $\widetilde{\mathcal{H}}$ is a congruence, $ab\widetilde{\mathcal{H}}a^0b^0$. But $ab\widetilde{\mathcal{H}}(ab)^0$, and so $(ab)^0 = (a^0b^0)^0$ since every $\widetilde{\mathcal{H}}$-class contains a unique idempotent.

Sufficiency. Since $\widetilde{\mathcal{H}}$ is an equivalence, we only need to show that $\widetilde{\mathcal{H}}$ is compatible with semigroup multiplication. Let $(a,b) \in \widetilde{\mathcal{H}}$ and $c \in S$. Then $(ca)^0 = (c^0a^0)^0 = (c^0b^0)^0 = (cb)^0$ and so $\widetilde{\mathcal{H}}$ is left compatible with semigroup multiplication. Dually, $\widetilde{\mathcal{H}}$ is right compatible with semigroup multiplication and thus $\widetilde{\mathcal{H}}$ is indeed a congruence. □

Lemma 2.2. *If e, f are $\widetilde{\mathcal{D}}$-related idempotents of an $\widetilde{\mathcal{H}}$-abundant semigroup S, then $e\mathcal{D}f$.*

PROOF. Since $e\widetilde{\mathcal{D}}f$, there are elements $a_1, \ldots, a_k$ of S such that $e\widetilde{\mathcal{L}}a_1\widetilde{\mathcal{R}}a_2 \ldots a_k\widetilde{\mathcal{L}}f$. Since S is $\widetilde{\mathcal{H}}$-abundant, we have $e\widetilde{\mathcal{L}}a_1^0\widetilde{\mathcal{R}}a_2^0 \cdots a_k^0\widetilde{\mathcal{L}}f$. Thus $e\mathcal{D}f$. □

Corollary 2.3. *If S is an $\widetilde{\mathcal{H}}$-abundant semigroup, then*

$$\widetilde{\mathcal{D}} = \widetilde{\mathcal{L}} \circ \widetilde{\mathcal{R}} = \widetilde{\mathcal{R}} \circ \widetilde{\mathcal{L}}.$$

PROOF. If $a, b \in S$ and $a\widetilde{\mathcal{D}}b$, then by Lemma 2.2, $a^0\mathcal{D}b^0$. Thus there are elements c, d in S with $a^0\mathcal{L}c\mathcal{R}b^0$ and $a^0\mathcal{R}d\mathcal{L}b^0$. These lead to $a\widetilde{\mathcal{L}}c\widetilde{\mathcal{R}}b$ and $a\widetilde{\mathcal{R}}d\widetilde{\mathcal{L}}b$ and hence the result follows. □

Lemma 2.4. *Let e, f be idempotents in an $\widetilde{\mathcal{H}}$-abundant semigroup S. If $e\mathcal{J}f$ then $e\mathcal{D}f$.*

PROOF. Since $SeS = SfS$, there exist elements x, y, s, t in S such that $f = set, e = xfy$. Let $h = (fy)^0$ and $k = (se)^0$. Then $fy = ffy$ so that $h^2 = h = fh$ and $se = see$. Thus, $k^2 = k = ke$ and hence it follows that hf, ek are idempotents such that $hf\mathcal{R}h$ and $ek\mathcal{L}k$. These imply that $ehf\mathcal{R}eh$ and $ekf\mathcal{L}kf$. Now $eh = xfyh = xfy = e$ and $kf = kset = set = f$ so that $e\mathcal{R}ef\mathcal{L}f$, that is, $e\mathcal{D}f$. □

Proposition 2.5. *If a is an element of an $\widetilde{\mathcal{H}}$-abundant cryptograph S, then $\widetilde{J}(a) = Sa^0S$.*

PROOF. Certainly $a^0 \in \widetilde{J}(a)$ so that $Sa^0S \subseteq \widetilde{J}(a)$. We now see that the ideal Sa^0S of the semigroup S is an $\widetilde{ideal}$ of S and since $a = aa^0 \in Sa^0S$, the result follows. Let $b = xa^0y \in Sa^0S (x, y \in S)$ and $k = (a^0y)^0$. Then $a^0a^0y = a^0y$ so that $a^0k = k = k^2$. Also since $\widetilde{\mathcal{H}}$ is a congruence, $xa^0y\widetilde{\mathcal{H}}xk$. Now let $h = (xk)^0 = (xa^0y)^0$. Then $xk = xkk$ so that $h^2 = h = hk = ha^0k \in Sa^0S$. Hence if $c \in \widetilde{L}_b, d \in \widetilde{R}_b$, then $c = ch$ and $d = hd \in Sa^0S$ so that Sa^0S is an $\widetilde{ideal}$ of S, as required. □

We now call a completely $\widetilde{\mathcal{J}}$-simple semigroup S a $\widetilde{\mathcal{J}}$-simple cryptogroup because the Green $\sim$-relation $\widetilde{\mathcal{H}}$ on S is a congruence on S and S itself is completely regular.Thus, as an analogous concept of cryptogroup introduced in the monograph of PETRICH–REILLY [10], we naturally call the above semigroup the $\widetilde{\mathcal{J}}$-simple cryptogroup. For $\widetilde{\mathcal{J}}$-simple cryptogroups, we have the following properties:

Proposition 2.6. *If S is a $\widetilde{\mathcal{J}}$-simple cryptogroup, then $\widetilde{\mathcal{J}} = \widetilde{\mathcal{D}}$.*

PROOF. Let $a, b \in S$ such that $a\widetilde{\mathcal{J}}b$. Then,by Proposition 2.5, $Sa^0S = Sb^0S$. By Lemma 2.4, $a^0\mathcal{D}b^0$ and hence $a\widetilde{\mathcal{H}}a^0\mathcal{D}b^0\widetilde{\mathcal{H}}b$. This implies that $a\widetilde{\mathcal{D}}b$ and

therefore $\widetilde{\mathcal{J}} \subseteq \widetilde{\mathcal{D}}$. Conversely, let $a, b \in S$ with $a\widetilde{\mathcal{D}}b$. Then, by Corollary 2.3, there exists $c \in S$ such that $a\widetilde{\mathcal{L}}c\widetilde{\mathcal{R}}b$. Thus $a^0\mathcal{L}c^0\mathcal{R}b^0$ and so $Sa^0S = Sc^0S = Sb^0S$. By Proposition 2.5, $(a, b) \in \widetilde{\mathcal{J}}$ and hence $\widetilde{\mathcal{D}} \subseteq \widetilde{\mathcal{J}}$. Now we have $\widetilde{\mathcal{J}} = \widetilde{\mathcal{D}}$. □

Proposition 2.7. *A $\widetilde{\mathcal{J}}$-simple cryptogroup S is primitive for idempotents.*

Proof. Let e, f be idempotents in S with $e \leqslant f$. Since S is in fact a completely regular $\widetilde{\mathcal{J}}$-simple semigroup, it follows from Proposition 2.5 that $f \in SeS$. Now by the first part of Exercise 3 of [1, §8.4], there exists an idempotent g of S such that $f\mathcal{D}g$ and $g \leqslant e$. Let $a \in S$ be such that $f\mathcal{L}a\mathcal{R}g$. Then $f\mathcal{L}a^0\mathcal{R}g$ and since $g \leqslant f$, we have

$$a^0 = ga^0(gf)a^0 = g(fa^0) = gf = g.$$

Now $g \leqslant f$ and $g\mathcal{L}f$ so that $f = fg = g$. But $g \leqslant e$ so that $e = f$ and all idempotent of S are hence primitive. □

Lemma 2.8. *In a $\widetilde{\mathcal{J}}$-simple cryptogroup S, the regular elements of S generate a regular subsemigroup.*

Proof. Let a, b be regular elements of S. Since S consists of a single $\widetilde{\mathcal{D}}$-class (by Proposition 2.6), it follows from Corollary 2.3 that there is an element $c \in S$ with $a\widetilde{\mathcal{L}}c\widetilde{\mathcal{R}}b$. Hence, $a\widetilde{\mathcal{L}}c^0\widetilde{\mathcal{R}}b$. Thus $c^0b = b$ and $a\mathcal{L}c^0$ since a is regular. Now we have $ab\mathcal{L}b$ and the regularity of ab follows from the regularity of b. □

Theorem 2.9. *Let S be a $\widetilde{\mathcal{H}}$-abundant cryptograph. Then S can be expressed by a semilattice Y of $\widetilde{\mathcal{J}}$-simple cryptogroups $S_\alpha(\alpha \in Y)$ such that for $\alpha \in Y$ and $a \in S_\alpha$, $\widetilde{L}_a(S) = \widetilde{L}_a(S_\alpha)$, $\widetilde{R}_a(S) = \widetilde{L}_a(S_\alpha)$.*

Proof. If $a \in S$, then $a\widetilde{\mathcal{H}}a^2$ so that by Proposition 2.5 $\widetilde{J}(a) = \widetilde{J}(a^2)$. Now for $a, b \in S$, $(ab)^2 \in SbaS$, and so

$$\widetilde{J}(ab) = \widetilde{J}((ab)^2) \subseteq \widetilde{J}(ba)$$

and by symmetry, we have $\widetilde{J}(ab) = \widetilde{J}(ba)$. By invoking Proposition 2.5, we have $\widetilde{J}(a) = Sa^0S$ and $\widetilde{J}(b) = Sb^0S$ so that if $c \in \widetilde{J}(a) \cap \widetilde{J}(b)$, then $c = xa^0y = zb^0t$ for some $x, y, z, t \in S$. Now $c^2 = zb^0txa^0y \in Sb^0txa^0S \subseteq \widetilde{J}(b^0txa^0)$ and $\widetilde{J}(b^0txa^0) = \widetilde{J}(a^0b^0tx)$ by the preceding paragraph. Hence $c^2 \in \widetilde{J}(a^0b^0)$ and since $c\widetilde{\mathcal{H}}c^2$, we have $c \in \widetilde{J}(a^0b^0)$. Since $a\widetilde{\mathcal{H}}a^0$, $b\widetilde{\mathcal{H}}b^0$ and $\widetilde{\mathcal{H}}$ is a congruence so that $ab\widetilde{\mathcal{H}}a^0b^0$. Hence $c \in \widetilde{J}(ab)$. Thus $\widetilde{J}(a) \cap \widetilde{J}(b) \subseteq \widetilde{J}(ab)$ and since the converse inclusion is clear, $\widetilde{J}(a) \cap \widetilde{J}(b) = \widetilde{J}(ab)$.

It can be easily seen that the set Y of all $\widetilde{ideals}$ $\widetilde{J}(a)(a \in S)$ forms a semilattice under set intersection and that the map $a \mapsto \widetilde{J}(a)$ is a homomorphism

from S onto Y. The inverse image of $\widetilde{J}(a)$ is just the $\widetilde{\mathcal{J}}$-class $\widetilde{J}_a$ which forms a subsemigroup of S. Hence S is a semilattice Y of the semigroups $\widetilde{J}_a$.

Now let a, b be elements of the $\widetilde{\mathcal{J}}$-class $\widetilde{J}$ and suppose that $(a,b) \in \widetilde{\mathcal{L}}(\widetilde{J})$. Certainly $a^0, b^0 \in \widetilde{J}$ so that $(a^0, b^0) \in \widetilde{\mathcal{L}}(\widetilde{J})$, that is, $a^0b^0 = a^0, b^0a^0 = b^0$ and $(a^0, b^0) \in \widetilde{\mathcal{L}}(S)$. It follows that $(a,b) \in \widetilde{\mathcal{L}}(S)$ and since $\widetilde{L}_a(S) \subseteq \widetilde{J}$, $\widetilde{L}_a(S) = \widetilde{L}_a(\widetilde{J})$. By using a similar argument as above, we can show that $\widetilde{R}_a(S) = \widetilde{R}_a(\widetilde{J}_a)$.

From the above paragraph, we have $\widetilde{H}_a(\widetilde{J}) = \widetilde{H}_a(S)$ so that $\widetilde{J}$ is $\widetilde{\mathcal{H}}$-abundant. Furthermore, if $a, b \in \widetilde{J}$, then by Proposition 2.6, $(a,b) \in \widetilde{\mathcal{D}}(S)$ so that, by Corollary 2.3, there is an element c in $\widetilde{L}_a(S) \cap \widetilde{R}_b(S) = \widetilde{L}_a(\widetilde{J}) \cap \widetilde{R}_b(\widetilde{J})$. Thus a, b are $\widetilde{\mathcal{D}}$-related in $\widetilde{J}$ so that each $\widetilde{J}_a$ is a $\widetilde{\mathcal{J}}$-simple semigroup. This completes the proof. □

Lemma 2.10. *Let $S = (Y; S_\alpha)$ be an $\widetilde{\mathcal{H}}$-abundant cryptograph. Then the following statements hold:*

(i) *Let $a \in S_\alpha$ and $\alpha \geqslant \beta$. Then there exists $b \in S_\beta$ with $a \geqslant b$;*

(ii) *Let $a, b, c \in S$, $b\widetilde{\mathcal{H}}c$, and $a \geqslant b, c$. Then $b = c$;*

(iii) *Let $a \in E(S)$ and $b \in S$ be such that $a \geqslant b$. Then $b \in E(S)$.*

Proof. (i) Let $b \in S_\beta$. Then by Lemma 2.1, $a(aba)^0, (aba)^0a$ and $(aba)^0$ are in the same $\widetilde{\mathcal{H}}$-class and so $a(aba)^0 = (aba)^0a(aba)^0 = (aba)^0a$. If $b = a(aba)^0$, then $b \in S_\beta$ and $a \geqslant b$.

(ii) By the definition of "$\geqslant$", there exist $e, f, g, h \in E(S)$ such that $b = ea = af$, $c = ga = ah$. From $eb = b$ and $b\widetilde{\mathcal{H}}b^0$, we have $eb^0 = b^0$. Similarly, $c^0h = c^0$. Thus $ec = ec^0c = eb^0c = b^0c = c$. Similarly,we also have $bh = b$ and hence $b = bh = eah = ec = c$, as required.

(iii) We have $b = ea = af$ for some $e, f \in E(S)$ and whence,

$$b^2 = (ea)(af) = ea^2f = b.$$ □

Following Proposition 2.7 and Lemma 2.10 (ii), we can easily deduce the following corollary

Corollary 2.11. *A $\widetilde{\mathcal{J}}$-simple cryptogroup S is primitive, that is, all idempotents of S are primitive.*

3. Normal $\widetilde{\mathcal{H}}$-cryptographs

Following Proposition 2.7, we can easily prove the following lemma

Lemma 3.1. *Let ϕ be a homomorphism from a $\widetilde{\mathcal{J}}$-simple cryptogroup S into another $\widetilde{\mathcal{J}}$-simple cryptogroup T. Then $(a\phi)^0 = a^0\phi$.*

Remark. If ϕ be a homomorphism between two $\widetilde{\mathcal{J}}$-simple cryptogroups, then the $\widetilde{Green}$-relations $\widetilde{\mathcal{L}}$ and $\widetilde{\mathcal{R}}$ are preserved so that the relation $\widetilde{\mathcal{D}}$ is also preserved.

Lemma 3.2. *Let $S = (Y; S_\alpha)$ be a normal $\widetilde{\mathcal{H}}$-cryptograph.Then the following statements hold:*

(i) *For any $\alpha \geqslant \beta$ on Y and $a \in S_\beta$, there exists a unique element $a_\beta \in S_\beta$ such that $a \geqslant a_\beta$.*

(ii) *For any $\alpha \geqslant \beta$ on Y and $a \in S_\alpha$, $x \in S_\beta$, if $a^0 \geqslant e$ for some idempotent $e \in S_\beta$ then $eax = ax, xae = xa$, $ea = ae$ and $(ea)^0 = e$.*

Proof. (i) By Lemma 2.10 (i), there exists $a_\beta = a(aca)^0 = (aca)^0a \in S_\beta$ for any $c \in S_\beta$ such that $a \geqslant a_\beta$. If there is another $b \in S_\beta$ such that $a \geqslant b$, then there are idempotents $g, h \in E(S)$ such that $b = ga = ah$. Hence $a_\beta\widetilde{\mathcal{H}} = (aca)^0\widetilde{\mathcal{H}}a\widetilde{\mathcal{H}} = a\widetilde{\mathcal{H}}(aca)^0\widetilde{\mathcal{H}}$ and $b\widetilde{\mathcal{H}} = g\widetilde{\mathcal{H}}a\widetilde{\mathcal{H}} = a\widetilde{\mathcal{H}}h\widetilde{\mathcal{H}}$, that is, $a_\beta\widetilde{\mathcal{H}} \leqslant a\widetilde{\mathcal{H}}$ and $b\widetilde{\mathcal{H}} \leqslant a\widetilde{\mathcal{H}}$. It can be easily seen that $S/\widetilde{\mathcal{H}} = (Y; S_\alpha/\widetilde{\mathcal{H}})$, and so $a_\beta\widetilde{\mathcal{H}} = b\widetilde{\mathcal{H}}$ since $S/\widetilde{\mathcal{H}}$ is still a normal band. By Lemma 2.10 (ii), $a_\beta = b$.

(ii) Since $(a^0(ax)^0a^0)a^0 = a^0(ax)^0a^0 = a^0(a^0(ax)^0a^0)$ and $a^0(ax)^0a^0\widetilde{\mathcal{H}}(a^0(ax)^0a^0)^0$, we have $(a^0(ax)^0a^0)^0a^0 = (a^0(ax)^0a^0)^0 = a^0(a^0(ax)^0a^0)^0$, that is, $a^0 \geqslant (a^0(ax)^0a^0)^0$. Also, since $a \in S_\alpha$ and $x \in S_\beta$, $ax \in S_\beta$ and so $e = (a^0(ax)^0a^0)^0$ by (i). Thereby, we have $eax = (a^0(ax)^0a^0)^0ax = (a^0(ax)^0a^0)^0a^0(ax)^0a^0ax = ax$. Similarly, we have $xae = xa$. Since x is an arbitrarily chosen element in S_β, we can particularly choose $x = e$. In this way, we obtain $ea = ae$ and consequently, by Lemma 2.1, $(ea)^0 = (ea^0)^0 = e$, as required. □

Theorem 3.3. *An $\widetilde{\mathcal{H}}$-abundant semigroup S is a normal $\widetilde{\mathcal{H}}$-abundant cryptograph if and only if it is a strong semilattice of $\widetilde{\mathcal{J}}$-simple cryptogroups.*

Proof. *Necessity.* Following Theorem 2.9, we can let $S = (Y; S_\alpha)$, where Y is a semilattice and each component $S_\alpha(\alpha \in Y)$ is a $\widetilde{\mathcal{J}}$-simple cryptogroup. For $\alpha \geqslant \beta$ on Y and $a \in S_\alpha$, by Lemma 3.2, we can define a map $\phi_{\alpha,\beta} : a \mapsto a_\beta$ from S_α into S_β, where a_β is the unique element in S_β such that $a_\beta \leqslant a$ and $a_\beta = (aca)^0a = a(aca)^0$ for any $c \in S_\beta$. Now we show that $S = [Y; S_\alpha, \phi_{\alpha,\beta}]$ is a strong semilattice of $\widetilde{\mathcal{J}}$-simple cryptogroups S_α. In order to show that $\phi_{\alpha,\beta}$ is a structure homomorphism, we let $b \in S_\beta$. Then $b\phi_{\alpha,\beta} = (bcb)^0b = b(bcb)^0$. Thus by Lemma 3.2,

$$a_\beta b_\beta = (aca)^0ab(bcb)^0 = (aca)^0ab = ab(bcb)^0,$$

and this implies that $a_\beta b_\beta \leqslant ab$ and so by Corollary 2.11,

$$a_\beta b_\beta = (a\phi_{\alpha,\beta})(b\phi_{\alpha,\beta}) = (ab)\phi_{\alpha,\beta}.$$

Hence $\phi_{\alpha,\beta}$ is indeed a structure homomorphism.

(i) For every $\alpha \in Y$, we easily see that $\phi_{\alpha,\alpha} = 1_{S_\alpha}$ is the identity automomorphism of S_α.

(ii) For $\alpha \geqslant \beta \geqslant \gamma$ on Y, by the transitivity of $\leqslant$, we have $\phi_{\alpha,\beta}\phi_{\beta,\gamma} = \phi_{\alpha,\gamma}$.

(iii) For $\alpha, \beta \in Y$ and $a \in S_\alpha$, $b \in S_\beta$. By using the proof of Lemma 2.10 (i), we can let $a\phi_{\alpha,\alpha\beta} = a_1 = a(aca)^0 = (aca)^0 a$ and $b\phi_{\beta,\alpha\beta} = b_1 = b(bcb)^0 = (bcb)^0 b$, for any $c \in S_{\alpha\beta}$. Thus by Lemma 2.10 (ii), $a_1 b_1 = (aca)^0 ab(bcb)^0 = (aca)^0 ab = ab(bcb)^0$ so that $a_1 b_1 \leqslant ab$. Now we have $ab = a_1 b_1 = (a\phi_{\alpha,\alpha\beta})(b\phi_{\beta,\alpha\beta})$ since $S_{\alpha\beta}$ is primitive.

Sufficiency. Let $S = [Y; S_\alpha, \phi_{\alpha,\beta}]$ be a strong semilattice $\widetilde{\mathcal{J}}$-simple cryptogroups $S'_\alpha s$. We still need to show that $\widetilde{\mathcal{H}}$ is a congruence on the semigroup S and $S/\widetilde{\mathcal{H}}$ is a normal band. For this purpose, we let $a \in S_\alpha, b \in S_\beta$. Then $ab = (a\phi_{\alpha,\alpha\beta})(b\phi_{\beta,\alpha\beta})$ and so $(ab)^0 = [(a^0\phi_{\alpha,\alpha\beta})(b^0\phi_{\beta,\alpha\beta})]^0 = (a^0 b^0)^0$. Thus by Lemma 2.1, S is a completely regular semigroup.

For $a \in S_\alpha$, $x \in S_\beta$ and $y \in S_\gamma$, we let $\delta = \alpha\beta\gamma$. Then by direct computation, we have $(axya)\widetilde{\mathcal{H}} = a\phi_{\alpha,\delta}\widetilde{\mathcal{H}} = (ayxa)\widetilde{\mathcal{H}}$. This shows that $S/\widetilde{\mathcal{H}}$ is indeed a normal band. In other words, S is a normal $\widetilde{\mathcal{H}}$-abundant cryptograph. The proof is completed. □

Corollary 3.4. *Let $S = [Y; S_\alpha, \phi_{\alpha,\beta}]$ be a normal $\widetilde{\mathcal{H}}$-abundant cryptograph. Let $a \in S_\alpha$ and $b \in S_\beta$. Then the followings conditions are equivalent:*

(i) $a \geqslant b$.

(ii) $\alpha \geqslant \beta$ *and* $a\phi_{\alpha,\beta} = b$.

(iii) $b = b^0 a = ab^0$.

Proof. (i) $\Longrightarrow$ (ii) By our hypothesis, $b = ea = af$ for some idempotents $e \in S_\gamma$ and $f \in S_\delta$. This implies that $\alpha \geqslant \beta$ and $\beta = \gamma\alpha$, $\beta = \delta\alpha$. Now, by the definition of strong semilattice of semigroups, $b = (e\phi_{\gamma,\beta})(a\phi_{\alpha,\beta}) = (a\phi_{\alpha,\beta})(f\phi_{\delta,\beta})$. Since $e\phi_{\gamma,\beta}$ and $f\phi_{\delta,\beta}$ are idempotents, $b \leqslant a\phi_{\alpha,\beta}$ in S_β and so $b = a\phi_{\alpha,\beta}$ since S_β is primitive.

(ii) $\Longrightarrow$ (iii) We have $b^0 a = b^0(a\phi_{\alpha,\beta}) = b^0 b = b$ and dually, $b = ab^0$.

(iii) $\Longrightarrow$ (i) This part is obvious. □

4. An example

In closing this paper, we provide here a non-trivial example which is an $\widetilde{\mathcal{H}}$-abundant cryptograph but it is not a cryptogroup.

Example 4.1. We consider the following example: We first start with the following elements:

$$a_{11} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad a_{12} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad a_{13} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$a_{21} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad a_{22} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad a_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then, we form the sets

$$S_{ij} = \{3^n a_{ij} \mid n \geqslant 0 \text{ and } n \in N\}, \quad \text{where } i = 1, 2;\ j = 1, 2, 3.$$

It can be easily verified that the set $S_\alpha = S_{11} \bigcup S_{12} \bigcup S_{13} \bigcup S_{21} \bigcup S_{22} \bigcup S_{23}$ is indeed a semigroup under the usual matrix multiplication in which the elements a_{11}, a_{12}, a_{13}, a_{21}, a_{22} and a_{23} are idempotents. Clearly, the sets S_{11}, S_{12}, S_{13}, S_{21}, S_{22} and S_{23} are subsemigroups of the semigroup S_α, and each of which is "generated" by the above idempotents a_{11}, a_{12}, a_{13}, a_{21}, a_{22} and a_{23}, respectively. Also, we can easily see that the set of all idempotents of S_α forms a rectangular band.

Let
$$S_\beta = \{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, a, b, c, d, e, f, g, h, s, t, u, v\}$$
with the following Cayley table. Then we can check that the semigroup S_β is a completely regular semigroup and the set of idempotents
$E(S_\beta) = \{e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}\}$ of the semigroup S_β forms a rectangular band in S_β under the semigroup multiplication so that S_β is a rectangular group.

The Cayley table of the semigroup S_β is shown below:

$*$	e_{11}	e_{12}	e_{13}	e_{21}	e_{22}	e_{23}	a	b	c	d	e	f	g	h	s	t	u	v
e_{11}	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c	g	h	s	g	h	s
e_{12}	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c	g	h	s	g	h	s
e_{13}	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c	g	h	s	g	h	s
e_{21}	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f	t	u	v	t	u	v
e_{22}	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f	t	u	v	t	u	v
e_{23}	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f	t	u	v	t	u	v
a	a	b	c	a	b	c	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}
b	a	b	c	a	b	c	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}
c	a	b	c	a	b	c	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}
d	d	e	f	d	e	f	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}
e	d	e	f	d	e	f	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}
f	d	e	f	d	e	f	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}
g	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c
h	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c
s	g	h	s	g	h	s	e_{11}	e_{12}	e_{13}	e_{11}	e_{12}	e_{13}	a	b	c	a	b	c
t	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f
u	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f
v	t	u	v	t	u	v	e_{21}	e_{22}	e_{23}	e_{21}	e_{22}	e_{23}	d	e	f	d	e	f

Now, we define a multiplication "$*$" on $S = S_\alpha \bigcup S_\beta$ by extending the matrix multiplication on S_α and S_β as follows: for any $a \in S_\alpha$ and any $b \in S_\beta$, we define $a * b = b * a = b$. Then, S equipped with the above multiplication "$*$" becomes a semigroup. We can also calculate that the $\widetilde{\mathcal{L}}$-classes of S are the sets

$$\{3^n a_{11}, 3^n a_{21}, \}\{3^n a_{12}, 3^n a_{22}\},\{3^n a_{13}, 3^n a_{23}\}, \tag{1}$$

$$\{e_{11}, e_{21}, a, d, g, t\}, \{e_{12}, e_{22}, b, e, h, u\}, \{e_{13}, e_{23}, c, f, s, v\}. \tag{2}$$

Also the $\widetilde{\mathcal{R}}$-classes of S are the sets

$$\{3^n a_{11}, 3^n a_{12}, 3^n a_{13}\}, \{3^n a_{21}, 3^n a_{22}, 3^n a_{23}\}, \tag{3}$$

$$\{e_{11}, e_{12}, e_{13}, a, b, c, g, h, s\}, \{e_{21}, e_{22}, e_{23}, d, e, f, t, u, v\}, \tag{4}$$

where $n \geqslant 0$ is an integer. Consequently, the $\widetilde{\mathcal{H}}$-classes of S are the sets

$$\{3^n a_{11}\}, \{3^n a_{12}\}, \{3^n a_{13}\}, \{3^n a_{21}\}, \{3^n a_{22}\}, \{3^n a_{23}\}, \tag{5}$$

$$\{e_{11}, a, g\}, \{e_{12}, b, h\}, \{e_{13}, c, s\}, \{e_{21}, d, t\}, \{e_{22}, e, u\}, \{e_{23}, f, v\}, \tag{6}$$

where $n \geqslant 0$ is an integer.

This shows that the semigroup S is semiabundant and every $\widetilde{\mathcal{H}}$-class of S contains an idempotent and so in particular S is an $\widetilde{\mathcal{H}}$-abundant cryptograph. Because every element of $S \setminus \{S_\beta \cup \{a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}\}$ is non-regular, S itself is not a cryptogroup.

The above example illustrates that the class of cryptogroups is a proper subclass of the class of $\widetilde{\mathcal{H}}$-cryptographs.

References

[1] A. H. Clifford and G. B. Preston, The Algebraic Theory of Semigroups, Mathematical Surveys 7, Vols 1 and 2, *American Mathematical Society*, *Providence, R. I.*, 1967.

[2] A. H. Clifford, Semigroups admitting relative inverses, *Ann. of Math.* **42** (1941), 1037–1049.

[3] A. El-Qallali, Structure Theory for Abundant and Related Semigroups, PhD thesis, *York University*, *England*, 1980.

[4] J. B. Fountain, Abundant semigroups, *Proc. London Math. Soc.* **43**(3) **yr 1982**, 103–129.

[5] X. J. Guo and K. P. Shum, On left cyber groups, *Int. Math. J.* **5**, no. 8 (2004), 705–717.

[6] J. M. Howie, Fundamental of Semigroup Theory, *Clarendon Press*, *Oxford*, 1995.

[7] X. Z. Kong, Z. L. Yuan and K. P. Shum, $\mathcal{H}^\sharp$-abundant Semigroups and $\mathcal{H}^\sharp$-cryptographs, (to appear in Algebra Colloqium, 2007).

[8] X. Z. Kong and K. P. Shum, On the structure of regular crypto semigroups, *Comm. Algebra* **29**, no. 6 (2001), 2461–2479.

[9] F. J. Pastijn, A representation of a semigroup by a semigroup of matrices over a group with zero, *Semigroup Forum* **10** (1975), 238–249.

[10] M. Petrich and N. R. Reilly, Completely Regular Semigroups, *John Wiley & Sons*, 1999.

[11] M. Petrich, The structure of completely regular semigroups, *Trans. Amer. Math. Soc.* **189** (1974), 211–236.

[12] M. Petrich, Lectures in Semigroups, *Wiley & Sons Inc.*, *London*, 1976.

[13] X. M. Ren and K. P. Shum, The strucurue of superabundant semigroups, *Science in China ,A* **47**, no. 5 (2004), 755–771.

[14] X. M. Ren and K. P. Shum, Superabundant semigroups whose set of idempotents forms a subsemigroup, *Algebra Colloqium* **14**, no. 2 (2007), 215–228.

XIANGZHI KONG
SCHOOL OF SCIENCE
SOUTHERN YANGTZE UNIVERSITY, (JIANGNAN UNIVERSITY)
WUXI, JIANGSU, 214122
CHINA

E-mail: xiangzhikong@163.com

K. P. SHUM
FACULTY OF SCIENCE
THE CHINESE UNIVERSITY OF HONG KONG SHATIN, HONG KONG (SAR)
CHINA

E-mail: kpshum@@math.cuhk.edu.hk

(Received October 31, 2006; revised April 24, 2007)