Properties of the Transformation Semigroup of the Solitaire Stream Cipher

Boris Pogorelov[1] Marina Pudovkina[2]
[1]Institute of Cryptography Communication and Information,
Moscow, Russia,
[2]Moscow Engineering Physics Institute (State University),
Moscow, Russia

ABSTRACT Stream ciphers are often used in applications where high speed and low delay are a requirement. The Solitaire stream cipher was developed by B. Schneier as a paper-and-pencil cipher. Solitaire gets its security from the inherent randomness in a shuffled deck of cards. In this paper we investigate semigroups and groups properties of the Solitaire stream cipher and its regular modifications.

1 Introduction

Stream ciphers are often used in applications where high speed and low delay are a requirement. The Solitaire stream cipher was developed by B. Schneier[1] as a paper-and-pencil cipher. Solitaire gets its security from the inherent randomness in a shuffled deck of cards. Solitaire is an output-feedback mode stream cipher. The next-state function F is the composition of four transformations $F = F_4F_3F_2F_1$ which permute of elements of a deck. In [2] is considered the cycle structure of Solitaire. It is proved that Solitaire is not reversible and described all irreversible states. In [3] are analyzed properties of the key scheduling algorithm which derives the initial state from a variable size key, and described weaknesses of this process. One of these weaknesses is the existence of large classes equivalent keys.

In this paper we consider the method analysis of a cipher based on investigation properties of the group generated the cipher. We apply this approach to studying properties of the Solitaire stream cipher. Methods based on investigation group or semigroup properties of stream ciphers were not published in open .literature

In this paper we describe groups $<F_3>$, $<F_4>$and $<F_3, F_4>$. We prove that the group $<F_3, F_4>$is an intransitive group and describe its orbits.

We get that $<F_1>$, $<F_2>$are cyclic isomorphic semigroups of order n and $|<\mathsf{F}_1, \mathsf{F}_2>| \geq (\mathsf{n}-1)\mathsf{n}^2$. Also we prove that semigroups $<F_1, F_2, F_3>$, $<F_1, F_3>$and $<F_2, F_3>$are isomorphic and groups generated regular modifications of Solitaire are embedded to the semigroup $<F_1, F_2, F_3>$.

Also we investigate group properties of regular modifications of the Solitaire stream cipher. We obtain that some properties of the semigroup properties of Solitaire and its regular modifications are the same.

Let $\mathsf{n} \geq 3$. By A denote $\mathsf{n}-2$ and by B denote $\mathsf{n}-1$. We will suppose that records of jokers as letters or numbers are identical, i.e. $\mathsf{n}-2 \equiv$'A', $\mathsf{n}-1 \equiv$'B'.

If we select $\mathsf{n}-2$, $\mathsf{n}-1$, or only $\mathsf{n}-2$, or only $\mathsf{n}-1$ in Z_n, then denote $Z_n^{AB}=\{\overline{0, n-3}$, A, B$\}$, $Z_n^{A}=\{\overline{0, n-3}, \mathsf{n}-1$, A$\}$, $Z_n^{B}=\{\overline{0, n-2}$, B$\}$ respectively. Since numbers $\mathsf{n}-2$, $\mathsf{n}-1$ and letters A, B are identical we could consider sets Z_n^{AB}, Z_n^{A}, Z_n^{B} as Z_n.

The following standard notation will be used throughout:

1. $|X|$ denotes the cardinality of the set X;
2. $\mathsf{N}=\{1, 2, 3, 4, ...\}$;
3. $<\mathsf{P}>$denotes a cyclic group generated by P;
4. $<\mathsf{P}_1, \mathsf{P}_2, ..., \mathsf{P}_n>$denotes a group generated by $\mathsf{P}_1, \mathsf{P}_2, ..., \mathsf{P}_n$;
5. $\mathsf{S}(X)$ denotes the symmetric group on X, $S_n = S(Z_n)$;
6. E denotes the identity permutation;
7. (s)$<P_1,P_2,...,P_n>=s<P_1,P_2,...,P_n>$denotes the orbit of s;
8. G_Δ denotes the stabilizer of Δ in G;
9. G^X (g^X) denotes a restriction the transformation group G (transformation g) to the set X;

11. α^G denotes the orbit of α;

10. $\Delta^g=\Delta g=\{\alpha g \mid \alpha \in \Delta\}$, where g is an element of the transformation group(semigroup) G;

12. $\Delta^G=\Delta G=\bigcup_{g_i \in G} \Delta^{g_i}$, where G is a transformation group (semigroup);
13. $\mathsf{G} \cong \mathsf{H}$ denotes that groups (semigroups) G, H are isomorphic;
14. $< s[0], s[1]...s[n-1] >$denotes the permutation $\mathsf{s} \in \mathsf{S}_n$.

For convenience we shall simultaneously use two records for the permutation $<s[0]...s[k_1-1]$ A $s[k_1+1]...s[k_2-1]$ B $s[k_2+1]...s[n-1]> \equiv$ $<\delta[0]...\delta[k_1-1]$ A $\delta[k_1]...\delta[k_2-2]$ B $\delta[k_2-1]...\delta[n-3]>_{AB}$, where

$$\delta\left[j\right]=\begin{cases} s\left[j\right] & for \quad j=\overline{0, k_1-1}, \\ s\left[j+1\right] & for \quad j=\overline{k_1, k_2-2}, \\ s\left[j+2\right] & for \quad j=\overline{k_2-1, n-3}, \end{cases}$$

and $<\delta[0]...\delta[n-3]> \in S_{n-2}$.

We also suppose that $< s[0]...s[r-1]$ A $s[r+1]...s[n-1] >\equiv< \delta[0]...\delta[r-1]$ A $\delta[r]...\delta[n-2] >_A$,where

$$\delta[j] = \begin{cases} s[j] & for \quad j = \overline{0, r-1}, \\ s[j+1] & for \quad j = \overline{r+1, n-2}, \end{cases}$$

and $< \delta[0]...\delta[n-2] >\in S_{n-1}(Z_n^A \backslash A)$; $< s[0]...s[r-1]$ B $s[r+1]...s[n-1] >\equiv$ $< \delta[0]...\delta[r-1]$ B $\delta[r]...\delta[n-2] >_B$, where

$$\delta[j] = \begin{cases} s[j] & for \quad j = \overline{0, r-1}, \\ s[j+1] & for \quad j = \overline{r+1, n-2}, \end{cases}$$

and $< \delta[0]...\delta[n-2] >\in S_{n-1}$.

2 Description of Solitaire

The Solitaire stream cipher is modeled by the autonomous automaton $A_g = (\mathsf{S}_n, \mathsf{Z}_{m\cup}\{\alpha\}, \mathsf{F}, \mathsf{f})$, where functions $\mathsf{F} : \mathsf{S}_n \to \mathsf{S}_n$, $\mathsf{f} : \mathsf{S}_n \to \mathsf{Z}_{m\cup}\{\alpha\}$ and α is an additional symbol. The cipher depends on $\mathsf{m}, \mathsf{n} \in \mathsf{N}$, for practice $\mathsf{m} = 26$, $\mathsf{n} =54$. The state of Solitaire at time $\mathsf{t}(\mathsf{t} = 0, 1, ...)$ is a permutation $s_t =< s_t[0]...s_t[\mathsf{n}-1] >\in \mathsf{S}_n$ and s_0 is an initial state.

The next-state function F is the composition of four transformations $\mathsf{F} =$

$\mathsf{F}_1\mathsf{F}_2\ \mathsf{F}_3\mathsf{F}_4$, which are given below. The transformation $\mathsf{F}_1 : S(Z_n^A) \to S(Z_n^A)$,

F_1:$<s[0]...s[r]$ A $s[r+1]...s[n-2]>_A \to<s[0]...s[r+1]$ A $s[r+2]...s[n-2]>_A$ for $r \neq n-2$,

$\mathsf{F}_1 :< s[0]\ s[1]...s[n-2]$ A$>_A \to<s[0]$ A $s[1]\ s[2]...s[n-2]>_A$.

The transformation $\mathsf{F}_2 : S(Z_n^B) \to S(Z_n^B)$,

$\mathsf{F}_2 :< s[0]...s[r]$B $s[r+1]s[r+2]s[r+3]...s[n-2] >_B\to<s[0]...s[r]\ s[r+1]$ $s[r+2]$B $s[r+3]...s[n-2]>_B$ where $r \notin \{n-3, n-2\}$

$\mathsf{F}_2 :< s[0]\ s[1]...s[n-3]$ B $s[n-2] >_B\to<s[0]$ B $s[1]...s[n-2] >_B$,

$\mathsf{F}_2 :< s[0]\ s[1]...s[n-2]B >_B\to<s[0]$ B $s[1]...s[n-2]>_B$.

The transformation $\mathsf{F}_3 : S(Z_n^{AB}) \to S(Z_n^{AB})$,

$\mathsf{F}_3 :< s[0]...s[k_1-1]$ A $s[k_1]...$B $s[k_2]...s[n-3] >_{AB}\to<s[k_2]...s[n-3]$ A $s[k_1]...$B $s[0]...s[k_1-1]>_{AB}$,

F_3: <s[0]...s[k$_1$-1] B s[k$_1$]...A $_{AB} \to< s[k_2]...s[n{-}3]$ B $s[k_1]...$A $s[0]...s[k_1-1]>_{AB}$.

The transformation $\mathsf{F}_4 : S(Z_n^{AB}) \to S(Z_n^{AB})$. Let $\mathsf{s}[n-1] = \mathsf{r}$. Then

$\mathsf{F}_4 :< s[0]...s[\mathsf{r}-1]\ s[\mathsf{r}]s[\mathsf{r}+1]...s[n-2]\ s[n-1] >\to< s[\mathsf{r}+1]...s[n-2]$ $s[0]...s[\mathsf{r}]s[n-1]>$for $\mathsf{s}[n-1] \notin \{A,B\}$,

$\mathsf{F}_4 :< s[0]...s[\mathsf{r}-1]\ s[\mathsf{r}]s[\mathsf{r}+1]...s[n-2]\ s[n-1] >\to< s[0]...s[n-2]$ $s[n-1] >$ for $\mathsf{s}[n-1] \in \{$A, B$\}$.

Consider the next-state and output functions of Solitaire at time t ($t = 1, 2....$).

The next-state function F

$\mathsf{x}_t = (\mathsf{s}_t)\mathsf{F}_1$;

$\mathsf{y}_t = (\mathsf{x}_t)\mathsf{F}_2$;

$\mathsf{v}_t = (\mathsf{y}_t)\mathsf{F}_3$;

$\mathsf{s}_{t+1} = (\mathsf{v}_t)\mathsf{F}_4$,

?i.e. $\mathsf{s}_{t+1} = (\mathsf{s}_t)\mathsf{F}_1\mathsf{F}_2\mathsf{F}_3\mathsf{F}_4$.

The output function f

Let $s_{t+1}[0] = \mathsf{r}_t$.

a) If $s_{t+1}[\mathsf{r}_t] \in$ {A, B}, then $z_t = \alpha$;

b) If $s_{t+1}[\mathsf{r}_t] \notin$ {A, B}, then $z_t = s_{t+1}[\mathsf{r}_t]$(mod m),

i.e.$z_t = (\mathsf{s}_{t+1})$ f.

The map ρ: $Z^*_m \times S_n \to S_n$ is generated an initial state s_0, which is a key of Solitaire, from a passphrase $k \in Z^*_m$. The map ρ is modeled by the automaton $A_\rho = (Z_m, \mathsf{S}_n, \mathsf{P})$ without an output with the next-state function P: $Z_m \times S_n \to S_n$.

The partial next-state function $\mathsf{P}_{(r)} = \mathsf{F}_1\mathsf{F}_2\mathsf{F}_3\mathsf{P}_r$, $\mathsf{r} \in Z_m$, where map P_r : $\mathsf{S}_n \to \mathsf{S}_n$,

$(< s[0]...s[r]s[r+1]...s[n-1] >)\mathsf{P}_r = < s[r+1]...s[n-1]s[0]...s[r] >$.

Let $\mathsf{k} = k_1...k_L$ be a passphrase of length $L \geq 1$, $\mathsf{k}_j \in Z_m$, $\mathsf{j} = \overline{1, L}$. $\mathsf{b}_0 = < 0\ 1...n-1 >$ is an initial state of the automaton A_ρ.

The map ρ

I. For $\mathsf{t} = \overline{1, L}$ do:

1. $\mathsf{x}_t = (\mathsf{b}_t)\mathsf{F}_1$;

2. $\mathsf{y}_t = (\mathsf{x}_t)\mathsf{F}_2$;

3. $\mathsf{v}_t = (\mathsf{y}_t)\mathsf{F}_3$;

4. $\mathsf{b}_{t+1} = (\mathsf{v}_t)P_{k_t}$.

II. Take $s_0 = b_{L+1}$.

The directed set $\Lambda_{\overline{z}} = \{t | z_t \neq \alpha, t = 1, 2...\}$ corresponds to the keystream $\overline{z}$. Let the sequence $r_{\overline{z}} = r_1...r_{|\Lambda_{\overline{z}}|}$, where $r_1 = \min(\Lambda_{\overline{z}})$, $r_j = \min(\Lambda_{\overline{z}} \backslash \{r_1, ..., r_{j-1}\})$, $j = \overline{2, |\Lambda_{\overline{z}}|}$,

Let the map g : $Z^*_m \to Z^*_m$, $(\overline{z})g = \overline{z}$', $z'_t = z_{r_t}$, $\mathsf{t} = \overline{1, |\Lambda_{\overline{z}}|}$. It is clear that the map g decimations the keystream $\overline{z}$.

Let$p_1...p_N$ be a plaintext, $c_1...c_N$ be a corresponding ciphertext and $(\overline{z})g = \overline{z}\prime$.

Decryption: $c_t = p_t + z'_t$ (mod m), $t = \overline{1, N}$.

Encryption: $p_t = p_t - z'_t$ (mod m), $t = \overline{1, N}$.

3 Properties of the transformation group <F_3, F_4>

In this section we describe some properties of the transformation group $< F_3, F_4>$. We will suppose that $n \geq 3$ throughout.

First we consider the transformation group $< F_3 >$ of S_n. Let $G \in <F_3, F_4>$ and $I(G) = \{s \in S(Z_n^{AB}) | sG = s\}$.

Proposition 1 *Let $\{A_1, A_2\} = \{A, B\}$ Then*

1. F_3 *is involution;*
2. $I(F_3) = \{ <A_1 s[1]...s[n-2]\ A_2> | <s[1]...s[n-2]> \in S_{n-2}\}$ *and* $|I(F_3)| = 2(n-2)!$;
3. $<F_3>$ *has* $\frac{n!}{2} - (n-2)!$ *orbits of length 2;*

Proof. For proof note that for any k_1, k_2, $0 < k_1 < k_2 < n-1$. the following equalities are true.

$(<s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1]>)F_3 = (<s[k_2+1]...s[n-1]\ A_1\ s[k_1+1]...\ s[k_2-1] A_2\ s[0]...s[k_1-1]>)$,

$(<A_1 s[1]...s[n-2]\ A_2>)F_3 = <A_1\ s[1]...s[n-2]\ A_2>$. ■

Now let us prove some properties of the transformation group $<F_4>$. Let Θ be a set, $|\Theta| = n, n \geq 1$. $\eta : S(\Theta) \to S(\Theta)$ denotes left circular shift, i.e.

$$< s[0]...s[n-1] > \eta =< s[1]...s[n-1]\ s[0] >.$$

For any $r \in Z_n$ we have , $< s[0]...s[n-1] > \eta^r =< s[r]...s[n-1]\ s[0]...s[r-1] >$.

It is clear that

$$I(F_4) = \{< s[0]...s[n-2]\ A> | <s[0]...s[n-2]> \in S_{n-1}(Z_n^A \backslash A)\} \cup \{<s[0]...s[n-2]\ B> | <s[0]...s[n-2]> \in S_{n-2}\}. |.$$

and $|I(F_4)| = 2(n-1)!$.

In the following propositions we consider properties of $< F_4>$.

Proposition 2 *Let $\{A_1, A_2\} = \{A, B\}$ and $s = <s[0]...s[n-2]\ r>$, $r \in Z_{n-2}$, then* $|(s)<F_4>| = \frac{n-1}{gcd(r, n-1)}$.

Proof. Note that $(s)F_4 =< s[r+1]...s[n-2]s[0]...s[r]s[n-1] >= (s)\eta^r$ and $L_s = |(s)\eta^r|$ is the length of the orbit $(s)\eta^r$. Therefore, L_s is the number of decisions of the equation $L_s r = 0 \pmod{n-1}$. It follows that $L_s = \frac{n-1}{gcd(r, n-1)}$. ■

In the following propositions we describe properties of $< F_3, F_4 >$. Note that $F_3 F_4^r\ F_3 = (F_3F_4F_3)^r$ for any $r \in \mathsf{N}$.

Proposition 3 *Let* $\{A_2, A_1\}=\{A, B\}$, $\Delta=\{<A_1 s[1]...s[n-2]\ A_2>|<s[1] ... .s[n-2]>\in S_{n-2}\}$, *then* $<F_3, F_4>_\Delta = < F_3, F_4>$ *and* $|\Delta| = 2(n-2)!$.

Proof. The proof is by direct calculation. ■

Corollary 4 *Let* $\{A_2, A_1\}=\{A, B\}$ *and* $s=<A_1 s[1]...s[n-1]>\in S_n(Z_n^{AB})$, *where* $s[n-1] \neq A_2$, *then* $(s)F_3 \in I(F_4)$.

The proof follows from propositions 2 and 3.

Let $\{A_2, A_1\}=\{A, B\}$, $s =< s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1]>$, $k_2 > k_1$. Denote by $dist_{AB}(s)=k_2-k_1-1$ the number of elements between jokers A and B.

Proposition 5 *Let* $\{A_2, A_1\}=\{A, B\}$ *and* $s =< s[0]...s[k_1-1]\ A_1 s[k_1+1]... s[k_2-1]\ A_2\ s[k_2+1]...\ s[n-1] >\in S_n(Z_n^{AB})$. *If* $s\prime \in (s) < F_3, F_4>$, *then* $dist_{AB}(s)=dist_{AB}(s\prime)$ *or* $dist_{AB}(s\prime) = n-3-dist_{AB}(s)$.

Proof. Note that $<s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1] > F_3 = <s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1]>$, i.e. $dist_{AB}(s) = dist_{AB}(sF_3)$.

Since F_4 is a cyclic shift s, we consider the following three cases.

In the first case $s_1 =< s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1]>\eta^r = <s[r]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-2]\ s[0]...s[r]\ s[n-1]>$. Thus $dist_{AB}(s)=dist_{AB}(s_1)$.

In the second case $s_1 =< s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1]\ A_2\ s[k_2+1]...s[n-1]>\eta^r =< s[k_1+t]...s[k_2-1] A_2\ s[k_2+1]...s[n-2]\ s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_1+t-1]\ s[n-1]>$, where $r = k_1+t$. Thus $dist_{AB}(s_1) = n-3-dist_{AB}(s)$.

In the third case: $s_1 = (s)\eta^r = <s[k_2+t]...s[n-2]\ s[0]...s[k_1-1]\ A_1\ s[k_1+1]...s[k_2-1] A_2\ s[k_2+1]...s[k_2+t-1]\ s[n-1]>$for $r = k_2+t$. Therefore, $dist_{s_1}(A_1, A_2) = dist_s(A_1, A_2)$.

Since $s\prime = (s)F_3F_4^{t_1}...F_3F_4^{t_L}$ for some $t_1,...t_L \in Z_n$, it follows that $dist_{AB}(s) = dist_{AB}(s\prime)$ or $dist_{AB}(s\prime) = n-3-dist_{AB}(s)$ ■

Proposition 6 *Let* $\{A_2, A_1\}=\{A, B\}$ *and* $s=<s[0]...s[k_1-1]\ A_1 s[k_1+1]... s[k_2-1]\ A_2 s[k_2+1]...\ s[n-1]>$. *If* $s\prime \in (s) <F_3, F_4>$, *then* $s\prime[n-1] \in \{s[k_1-1], s[n-1], s[k_2-1]\}$.

The proof is straightforward.

Corollary 7 *Let* $\Lambda_n = S(Z_n^{AB}) \setminus \{<A\ s[1]...s[n-2]\ B>, <B\ s[1]...s[n-2]\ A>|\ \ <s[1]...s[n-2]>\in S_{n-2}\}$. *Then the group* $<F_3, F_4>^{\Lambda_n}$ *is intransitive.*

The proof follows from proposition 6.

4 Properties of the semigroup transformation <F_1, F_2, F_3, F_4>

In this section we describe properties of the semigroup transformation <F_1, F_2, F_3, F_4>and the group that is generated regular versions of Solitaire. We begin with definitions.

Let Θ be a set, $|\Theta|=d$, $d>1$, and a map α: $\Theta \rightarrow \Theta$. Let G be a transformation semigroup of Θ. Recall [5] that $rg(\alpha, \Theta)=|\Theta\alpha|$is the rank of α and $def(\alpha, \Theta)=\mathsf{d}- rg(\alpha, \Theta)$ is the defect of α. $def(G, \Theta)=\mathsf{d}- |\Theta^G|$is the defect of G.

Let G=<a>=$\{a,a^2,...,a^{q+r-1}\}$ be a cyclic semigroup. The $r \in \mathsf{N}$, denoted ind(G), is called the index of G if the set $\{a^r,...,a^{q+r-1}\}$ is a cyclic group of order q.

Let $S(Z_n^A, \mathsf{r}) = \{s \in Z_n^A | s[r] =\text{A}\}$, $S(Z_n^B, \mathsf{r}) = \{s \in Z_n^B | s[r] =\text{B}\}$,$\mathsf{r} = \overline{0, n-1}$, $S(Z_n^{AB}, \mathsf{r}_1, \mathsf{r}_2) = \{s \in Z_n^{AB} \ | s[r_1] =\text{A}, s[r_2] =\text{B}\}$, $0<r_1,r_2 < n-1$, $r_1 \neq r_2$.

It is clear that

$$S(Z_n^A) = \bigcup_{r=0}^{n-1} S(Z_n^A, \mathsf{r}),\ S(Z_n^B) = \bigcup_{r=0}^{n-1} S(Z_n^B, \mathsf{r}),$$
$$S(Z_n^{AB}) = \bigcup_{r_1 \neq r_2} S(Z_n^{AB}, \mathsf{r}_1, \mathsf{r}_2).$$

Let maps σ_A: $\mathsf{S}(Z_n^A) \rightarrow \mathsf{S}(Z_{n-1})$, σ_B: $\mathsf{S}(Z_n^B) \rightarrow \mathsf{S}(Z_{n-1})$

$$<s[0]...s[k-1] \text{ A } s[k]...s[n-2]>_A \ \ \sigma_A=<s[0]...s[k-1]\ s[k]...s[n-2]>,$$
$$<s[0]...s[k-1] \text{ B } s[k]...s[n-2]>_B \ \sigma_B= <s[0]...s[k-1]\ s[k]...s[n-2]\ >,$$

where $\mathsf{k}=\overline{0, n-1}$, $<s[0]...s[n-2]\ >\in \mathsf{S}_{n-1}(Z_n^A \backslash A)$.

Let the map σ_{AB}: $\mathsf{S}(Z_n^{AB}) \rightarrow \mathsf{S}(Z_{n-2})$

$<s[0]...s[k_1-1] \text{ A } s[k_1]...B\ s[k_2]...s[n-3]>_{AB}\ \sigma_{AB}=<s[0]...s[k_1-1]$ $s[k_1]...\ \ s[k_2-1]\ s[k_2]...s[n-3]>$,
where $\mathsf{k}_1 \neq \mathsf{k}_2$,$\mathsf{k}_1=\overline{0, n-1}$, $\mathsf{k}_2=\overline{0, n-1}$, $<s[0]...s[n-3]>\in \mathsf{S}_{n-2}$.

$$<s[0]...s[k-1] \text{ A}_1 \text{ A}_2\ s[k]...s[n-3]>\sigma_{AB}=<s[0]...s[k-1]\ s[k]...s[n-3]>,$$

where $\{\text{A}_1, \text{A}_2\}=\{\text{A}, \text{B}\}$, $\mathsf{k}=\overline{0, n-1}$, $<s[0]...s[n-3]>\in S_{n-2}$.

Permutations $s, s\prime \in \mathsf{S}(Z_n^A)$ are called A- equivalent if $(s)\sigma_A = (s\prime)\sigma_A$. Permutations $s, s\prime \in \mathsf{S}(Z_n^B)$ are called B- equivalent if $(s)\sigma_B = (s\prime)\sigma_B$. Permutations $s, s\prime \in \mathsf{S}(Z_n^{AB})$ are AB- equivalent if $(s)\sigma_{AB} = (s\prime)\sigma_{AB}$.

By $s \sim_A s\prime$, $s \sim_B s\prime$, $s \sim_{AB} s\prime$ denote A-equivalent, B-equivalent, AB-equivalent permutations s, s$\prime$ respectively. Let $\Delta_s^A=\{s\prime |\ s\prime \in S(Z_n^A),\ s \sim_A s\prime\}$, $\Delta_s^B=\{s\prime | s\prime \in \mathsf{S}(Z_n^B),\ s \sim_B s\prime\}$, $\Delta_s^{AB} =\{s\prime\ | s\prime \in \mathsf{S}(Z_n^{AB}),\ s \sim_{AB} s\prime\}$.

First we consider properties of semigroups $<\mathsf{F}_1>$, $<\mathsf{F}_2>$ and $<\mathsf{F}_1, \mathsf{F}_2>$.

Proposition 8 *Let the sets* $\Omega_A = \mathsf{S}(\mathsf{Z}_n^A) \backslash \mathsf{S}(\mathsf{Z}_n^A, 0)$, $\Omega_B = \mathsf{S}(\mathsf{Z}_n^B) \backslash \mathsf{S}(\mathsf{Z}_n^B, 0)$. *Then*

1. $S(Z_n^A, 0)F_1^{-1} = \emptyset$, $def(F_1, Z_n^A) = (n-1)!$.
2. $S(Z_n^B, 0)F_2^{-1} = \emptyset$, $def(F_2, Z_n^B) = (n-1)!$.
3. $< F_1 >, < F_2 >$ *are cyclic semigroups of order n and* $ind(F_1) = ind(F_2) = 1$.
4. $< F_1 >^{\Omega_A}, < F_2 >^{\Omega_B}$ *are cyclic groups of order* $n-1$; $s\prime \in (s) < F_1 >^{\Omega_A}$ *iff* $s \sim_A s\prime$ *and* $|(s) < F_1 >^{\Omega_A}| = n-1$. $s\prime \in (s) < F_2 >^{\Omega_B}$; *iff* $s \sim_B s\prime$ *and* $|(s) < F_2 >^{\Omega_B}| = n-1$.
5. $< F_1 >^{\Omega_A}$ *has* $(n-1)!$ *orbits and* $< F_2 >^{\Omega_B}$ *has* $(n-1)!$ *orbits.*
6. $< F_1 > \cong < F_2 >$.

Proof. The domain of the transformation F_1 is $S(Z_n^A) = \bigcup_{r=0}^{n-1} S(Z_n^A, r)$, where $S(Z_n^A, r_1) \cap S(Z_n^A, r_2) = \emptyset$, $r_1 \neq r_2$. Consider $s = < s[0]...s[n-2]\text{A} >_A \in S(Z_n^A, n-1)$. Then

F_1: $<s[0]...s[n-2]\ \text{A}>_A \to <s[0]\ \text{A}\ s[1]...s[n-2]>_A$,

F_1^j: $<s[0]...s[n-2]\ \text{A}>_A \to <s[0]...s[j-1]\ \text{A}\ s[j]...s[n-2]>_A \in S(Z_n^A, j)$ for $j = \overline{1, n-1}$. (1)

Therefore, $F_1 : S(Z_n^A, j) \to S(Z_n^A, j+1)$ for $j = \overline{0, n-2}$, $F_1 : S(Z_n^A, n-1) \to S(Z_n^A, 1)$.

Obviously, $S(Z_n^A, n-1)F_1 = S(Z_n^A, 0)F_1 = S(Z_n^A, 1)$ Thus, $S(Z_n^A, 0)F_1^{-1} = \emptyset$.

Similarly. The domain of the transformation F_2 is $S(Z_n^B) = \bigcup_{r=0}^{n-1} S(Z_n^B, r)$ for $S(Z_n^B, r_1) \cap S(Z_n^B, r_2) = \emptyset$, $r_1 \neq r_2$. Let $s = < s[0]...s[n-2]B >_B \in S(Z_n^B, n-1)$. Then

F_2: $<s[0]...s[n-2]\ \text{B}>_B \to <s[0]\ s[1]\ \text{B}\ s[2]...s[n-2]>_B$,

F_2^j: $<s[0]...s[n-2]\ \text{B}>_B \to <s[0]...s[j-1]\ s[j]\ \text{B}...s[n-2]>_B \in S(Z_n^B, j)$ for $j = \overline{1, n-1}$. (2)

Thus,

$F_2 : S(Z_n^B, j) \to S(Z_n^B, j+2)$ for $j = \overline{0, n-3}$,

$F_2 : S(Z_n^B, n-2) \to S(Z_n^B, 1)$,

$F_2 : S(Z_n^B, n-1) \to S(Z_n^B, 2)$.

Hence, $S(Z_n^B, n-1)F_2 = S(Z_n^B, 0)F_2 = S(Z_n^B, 2)$ This implies that $S(Z_n^B, 0)$ $F_2^{-1} = \emptyset$. Items (3)-(6) follow from (1) and (2). ■

We consider regular transformations ψ_A: $S(Z_n^A) \to S(Z_n^A)$, ψ_B: $S(Z_n^B) \to S(Z_n^B)$, ϑ_A: $S(Z_n^A) \to S(Z_n^A)$, ϑ_B: $S(Z_n^B) \to S(Z_n^B)$, where

$$\psi_A: <s[0]...s[n-2]\ \text{A}>_A \to <\text{A}\ s[0]...s[n-2]>_A,$$

ψ_A: $<s[0]...s[k]\ \text{A}\ s[k+1]...s[n-1]>_A \to <s[0]...s[k]\ s[k+1]\ \text{A}...s[n-2]>_A$ for $k = \overline{0, n-2}$

$$\psi_B: <s[0]...s[n-2]\ \text{B}>_B \to <\text{B}\ s[0]...s[n-2]>_B,$$

ψ_B:<s[0]...s[k] B s[k+1]...s[$n-1$]>$_B$ →<s[0]...s[k] s[k+1] B...s[$n-2$]>$_B$ for $k=\overline{0, n-2}$.

$$\vartheta_A: <s[0]...s[n-2]\ \mathrm{A}>_A \rightarrow <\mathrm{A}\ s[1]\ s[2]...s[n-2]\ s[0]>_A,$$

ϑ_A:<s[0]...s[k] A s[k+1]...s[$n-1$]>$_A$ →<s[0]...s[k] s[k+1] A...s[$n-2$]>$_A$ for $k=\overline{0, n-2}$

$$\vartheta_B: <s[0]...s[n-2]\ \mathrm{B}>_B \rightarrow <\mathrm{B}\ s[1]s[2]...s[n-2]\ s[0]>_B,$$

ϑ_B:<s[0]...s[k] B s[k+1]...s[$n-1$]>$_B$ →<s[0]...s[k] s[k+1] B...s[$n-2$]>$_B$ for $k=\overline{0, n-2}$.

It is clear that $<\psi_A>$, $<\vartheta_A>$ and $<\psi_B>$, $<\vartheta_B>$ are cyclic groups.

Note that ψ_A, ϑ_A are two regular modifications of F_1 and $<\psi_B>$, $<\vartheta_B>$ are two regular modifications of F_2. It is not hard to prove that $<\psi_A>$ is a cyclic group of order n. $s\prime \in (s) <\psi_A>$ iff $s \sim_A s\prime$. The group $<\psi_A>$ has $(n-1)!$ orbits and $|(s) <\psi_A>| = n$. $<\vartheta_A>$ is a cyclic group of order $n(n-1)$and $(s) <\vartheta_A> = \bigcup_{k=1}^{n-1} (s)\ \eta^k <\psi_A>$. There exist the following isomorphism of groups $<\psi_A>\cong<\psi_B>$, $<\vartheta_A>\cong<\vartheta_B>$, $<\eta,\psi_A>\cong<\vartheta_A>$, $<\eta,\psi_B>\cong<\vartheta_B>$.

Let $s \in S(Z_n^{AB})$ such that $s[k_1]$ =A, $s[k_2]$ =B. Denote

$$dist_A(s) = \begin{cases} k_2-k_1-1 & \text{for } k_2>k_1, \\ n-1+k_2-k_1 & \text{for } k_2<k_1, \end{cases}$$

$$dist_B(s) = \begin{cases} k_1-k_2-1 & \text{for } k_2<k_1, \\ n-1+k_1-k_2 & \text{for } k_2>k_1. \end{cases}$$

Let the transformation τ: $S(Z_n^{AB}) \rightarrow S(Z_n^{AB})$ be given by

τ: <s[0]...s[k_1-1] A s[k_1+1]...s[k_2-1] B s[k_2+1]...s[$n-3$]>→<s[0]...s[k_1+1] A... s[k_2+1] B...s[$n-3$]>for$|k_1-k_2|>1$.

$$\tau: <s[0]...\mathrm{A\ B}\ s[k]\ s[k+1]...s[n-3]> \rightarrow <s[0]...s[k]\ \mathrm{A\ B}\ s[k+1]...s[n-3]>,$$
$$\tau: <s[0]...\mathrm{B\ A}\ s[k]\ s[k+1]...s[n-3]> \rightarrow <s[0]...s[k]\ \mathrm{B\ A}\ s[k+1]...s[n-3]>.$$

It is easy to prove that the transformation group $<\tau>$is an 1/2-transitive cyclic group of order n. For any $s \in S(Z_n^{AB})$ the orbit $(s) <\tau>$ of s is the set $\{s\prime | dist_A(s\prime) = dist_A(s), s\prime \in \Delta_s^{AB}\}$, $|(s) <\tau>| = n$. For any $s \in S(Z_n^{AB})$the stabilizer $<\tau>_s = E$.

Proposition 9 *Let* $<\psi_A, \psi_B>$*be a transformation group of* S_n*. Then*

1. $<\psi_A, \psi_B>$*is an 1/2-transitive group.*$(s)<\psi_A,\psi_B>=\Delta_s^{AB}$ *and* $|\Delta_s^{AB}| = n(n-1)$.

2. $<\psi_A,\ \psi_B>$*has* $(n-2)!$ *orbits.*

3. *the sets* $\Omega_k = \{s\prime | dist_A(s\prime) = k, s\prime \in \Delta_s^{AB}\}$, *where* $k=\overline{0, n-2}$, $|\Omega_k|=n$ *are imprimitive blocks of* $<\psi_A, \psi_B>^{\Delta_s^{AB}}$.

4. $<\psi_A, \psi_B>_{\Omega_k}^{\Delta_s^{AB}} = <\psi_A^j \psi_B^j | j = \overline{0, n-2}>$ *for any* $k=\overline{0, n-1}$.

5. *the group acting on imprimitive blocks is isomorphic to* Z_{n-1}.

6. $|<\psi_A, \psi_B>| = (n-1)n^2$.

The proof is omitted.

Proposition 10 *Let* $\Omega_{AB}=S(Z_n^{AB})\backslash(S(Z_n^A,0)\cup S(Z_n^B,0))$. *Then*

1. $\Omega_{AB}<F_1, F_2>=\Omega_{AB}$. $def(<F_1, F_2>, Z_n^{AB})=2(n-1)!$ *and* $def(F_1 F_2,\ Z_n^{AB}) = def(F_2 F_1,\ Z_n^{AB}) = 2(n-1)! - (n-2)!$.

2. $s\prime \in (s)<F_1,\ F_2>^{\Omega_{AB}}$ *iff* $s \sim_{AB} s\prime$ *and* $|(s)<F_1,\ F_2>^{\Omega_{AB}}|=(n-1)(n-2)$.

3. *the group* $<F_1, F_2>^{\Omega_{AB}}$ *has* $(n-2)!$ *orbits.*

4. *the group* $<F_1, F_2>^{\Omega_{AB}}$ *is isomorphic to the transformation group* $<\psi_A,\ \psi_B>^{S(Z_{n-1}^{AB})}$.

Proof. The domain of the transformations F_1F_2, F_2F_1 is

$$S(Z_n^{AB}) = \bigcup_{r_1 \neq r_2} S(Z_n^{AB}, r_1, r_2).$$

From proposition 8 and $S(Z_n^B, 0) \cap S(Z_n^A, 0) = \emptyset$ for F_1F_2 we have

$$S(Z_n^A, n-1)F_1 = S(Z_n^A, 0)F_1 = S(Z_n^A, 1),$$

$(S(Z_n^{AB})\backslash S(Z_n^A, 0))F_2 = ((S(Z_n^B, 0)\backslash S(Z_n^{AB}, 1, 0)) \cup S(Z_n^{AB}, 1, 0) \cup \Omega_{AB})F_2 = (S(Z_n^B, 2)\backslash S(Z_n^{AB}, 0, 2)) \cup S(Z_n^{AB}, 0, 2) \cup \Omega_{AB} = S(Z_n^{AB}, 0, 2) \cup \Omega_{AB}$.

Similarly, for F_2F_1 we get

$$S(Z_n^B, n-1)F_2 = S(Z_n^B, 0)F_2 = S(Z_n^B, 2),$$

$(S(Z_n^{AB})\backslash S(Z_n^B, 0))F_1 = ((S(Z_n^B, 0)\backslash S(Z_n^{AB}, 0, 1)) \cup S(Z_n^{AB}, 0, 1) \cup \Omega_{AB})F_1 = (S(Z_n^B, 1)\backslash S(Z_n^{AB}, 1, 0)) \cup S(Z_n^{AB}, 1, 0) \cup \Omega_{AB} = S(Z_n^{AB}, 1, 0) \cup \Omega_{AB}$.

Thus,

$S(Z_n^{AB})F_1F_2 = S(Z_n^{AB}, 0, 2) \cup \Omega_{AB}, S(Z_n^{AB})F_2F_1 = S(Z_n^{AB}, 1, 0) \cup \Omega_{AB}$.

This means that

$$def(F_1F_2, Z_n^{AB}) = def(F_2F_1, Z_n^{AB}) = 2(n-1)! - (n-2)!.$$

Note that $(S(Z_n^{AB}, 0, 2) \cup \Omega_{AB})F_1 = Z_{AB}, (S(Z_n^{AB}, 1, 0) \cup \Omega_{AB})F_2 = \Omega_{AB}$.

From $\Omega_{AB}\ F_1^{-1} = \Omega_{AB}$, $\Omega_{AB}\ F_2^{-1} = \Omega_{AB}$ we have $\Omega_{AB} < F_1, F_2 >= \Omega_{AB}$.

The proof of items (b)-(d) is straightforward. ■
From propositions 9 and 10 we obtain that $|<F_1, F_2>| \leq n^2(n-1)$.

Corollary 11 *If states of Solitaire are the following permutations:*

1. $s = <A\ s[1]\ s[2] \ldots s[\mathsf{n}-2]\ B> \in S(Z_n^{AB})$;
2. $s = <s[0]\ s[1]\ s[2] \ldots s[\mathsf{n}-3]\ A\ B> \in S(Z_n^{AB})$;
3. $s = <s[0] \ldots s[\mathsf{p}-1]\ B\ s[p+1] \ldots s[\mathsf{n}-2]\ A> \in S(Z_n^{AB})$, *where* $p \in \{\overline{0, n-2}\}$;
4. $s = <s[0] \ldots s[\mathsf{p}-1]\ A\ s[p+1] \ldots s[\mathsf{n}-2]\ B> \in S(Z_n^{AB})$, *where* $p \in \{\overline{0, n-4}\} \cup \{\mathsf{n}-2\}$

then $(\mathsf{s})\mathsf{F}^{-1} = \emptyset$.

Corollary 12 *Let* $\Omega_{AB} = S(Z_n^{AB}) \backslash (S(Z_n^A, 0) \cup S(Z_n^B, 0))$ *and a substitution* π: $\{3, 4\} \rightarrow \{3, 4\}$. *Then*

1. $(S(Z_n^{AB}, 0, 2) \cup \Omega_{AB})(F_{\pi(3)}\ F_{\pi(4)})\ (F_1 F_2 F_{\pi(3)} F_{\pi(4)})^{-1} = \emptyset$, $def(F_1 F_2 F_{\pi(3)} F_{\pi(4)}, Z_n^{AB}) = 2(\mathsf{n}-1)! - (\mathsf{n}-2)!$.
2. $(S(Z_n^{AB}, 0, 2) \cup \Omega_{AB})\ (F_{\pi(3)} F_{\pi(4)} F_1 F_2)^{-1} = \emptyset$, $def(F_{\pi(3)} F_{\pi(4)} F_1 F_2.\ Z_n^{AB}) = 2(\mathsf{n}-1)! - (\mathsf{n}-2)!$.
3. $(S(Z_n^{AB}, 1, 0) \cup \Omega_{AB})(F_{\pi(3)} F_{\pi(4)})(F_2 F_1 F_{\pi(3)} F_{\pi(4)})^{-1} = \emptyset$, $def(F_2 F_1 F_{\pi(3)} F_{\pi(4)}, Z_n^{AB}) = 2(\mathsf{n}-1)! - (\mathsf{n}-2)!$.
4. $(S(Z_n^{AB}, 1, 0) \cup \Omega_{AB})\ (F_{\pi(3)} F_{\pi(4)} F_2 F_1)^{-1} = \emptyset$, $def(F_{\pi(3)} F_{\pi(4)} F_2 F_1, Z_n^{AB}) = 2(\mathsf{n}-1)! - (\mathsf{n}-2)!$.

The proof follows from proposition 10.

Proposition 13 *In the following proposition we describe properties of the* $<F_1, F_2, F_3>$ *semigroup.*

1. *If* $s \in S(Z_n^{AB})$, *then* $(s)<F_1, F_2, F_3> = S(Z_n^{AB})$.
2. *Let* $\Lambda = \{ S(Z_n^{AB}, r_1, r_2) | r_1, r_2 = \overline{0, n-1}, r_1 \neq r_2\}$, $g \in <F_1, F_2, F_3>$ *and* $\Delta \in \Lambda$. *Then* $\Delta^g \cap \Delta = \Delta$ *or* $\Delta^g \cap \Delta = \emptyset$. $|\Lambda| = \mathsf{n}(\mathsf{n}-1)$.
3. *Let* $s \in S(Z_n^{AB})$, $\Delta_s = \{s\prime | s\prime \sim_{AB} s,\ s\prime \in S(Z_n^{AB})\}$. *Then the transformation semigroup* G *of* Λ *is isomorphic to the semigroup* $< \mathsf{F}_1, \mathsf{F}_2 >^{\Delta_\mathsf{s}}$.
4. *Let* $\Omega = \mathsf{S}(\mathsf{Z}_n^{AB}) \backslash (\mathsf{S}(\mathsf{Z}_n^A, 0) \cup \mathsf{S}(\mathsf{Z}_n^B, 0) \cup \mathsf{S}(\mathsf{Z}_n^B, \mathsf{n}-1) \cup \mathsf{S}(\mathsf{Z}_n^A, \mathsf{n}-1))$ *Then* $< \mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3 >^\Omega$ *is transitive and* $| < \mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3 >^\Omega | = (\mathsf{n}-2)!$. *The group* $< \mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3 >^\Omega$ *is isomorphic to* $<\psi_A, \psi_B, F_3>^{S(Z_{\mathsf{n}-2}^{\mathsf{AB}})}$.

Proof. Note that
F_3: S(Z_n^{AB}, r_1,r_2)→ S(Z_n^{AB}, $n-r_2-1, n-r_1-1$),
F_1: S(Z_n^{AB}, r_1,r_2)→ S(Z_n^{AB}, r_1+1,r_2) for $r_1+1 \neq r_2$ and $r_{1\neq} n-1$,
F_1: S(Z_n^{AB}, $n-1$,r_2)→ S(Z_n^{AB}, 1,r_2+1) for r_2 ≠0,
F_1: S(Z_n^{AB}, $n-1$,0)→ S(Z_n^{AB}, 1, 0) for r_2 ≠0,
F_1: S(Z_n^{AB}, r_1,r_2)→ S(Z_n^{AB}, r_2,r_1) for $r_1+1 = r_2$ and $r_{1\neq} n-1$,
F_2: S(Z_n^{AB}, r_1,r_2)→ S(Z_n^{AB}, r_1,r_2+2) for $r_1-r_2 \notin$\{1, 2\}and $r_2 \notin \{n-2, n-1\}$,
F_2: S(Z_n^{AB}, r_1,r_2)→ S(Z_n^{AB}, r_1-1,r_1+1) for $r_1-r_2 \in$\{1, 2\}, $r_2 \notin \{n-2, n-1\}$,
F_2: S(Z_n^B, r_1, $n-2$)→ S(Z_n^B, r_1+1,1) for $r_1 \in \{\overline{2, n-3}\}$,
F_2: S(Z_n^B, r_1, $n-1$)→ S(Z_n^B, r_1+1, 2) for $r_1 \in$\{0, 1\},
F_2: S(Z_n^B, r_1, $n-2$)→ S(Z_n^B, r_1,1) for $r_1 \in \{0, n-1\}$,

By the above it follows that for any $g \in < F_1, F_2, F_3 >$ and $\Delta \in \Lambda$ we have $\Delta^g \cap \Delta = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. Since $|S(Z_n^{AB})| = n!$ and $|S(Z_n^{AB}, r_1, r_2)| = (n-2)!$, $r_1,r_2 = \overline{0, n-1}$, $r_1 \neq r_2$, we get $|\Lambda| = |S(Z_n^{AB})| \backslash |S(Z_n^{AB}, r_1, r_2) = n(n-1)$.

It is obviously that $< F_1, F_2 >^{\Lambda} \cong < F_1, F_2 >^{S(Z_n^{AB})}$and $S(Z_n^{AB}, n-r_2-1, n-r_1-1) \in S(Z_n^{AB}, r_1, r_2) < F_1, F_2 >$. Therefore, the transformation semigroup G of Λ is isomorphic to the semigroup $< F_1, F_2 >^{\Delta_s}$.

Let $s =< s[0]\ s[1]...s[j-1]\ s[j]\ s[j+1]...s[n-3]$ A B>and $s^{(j)} =< s[j]$ $s[1]...s[j-1]$ s[0] $s[j+1]...s[n-3]$ A B>, $j=\overline{1, n-3}$.

We will prove that for any j=$\overline{1, n-3}$, $s^{(j)} \in (s) < F_1, F_2, F_3 >$. The following are true.

<$s[0]$A $s[1]...s[j-1]$ B $s[j]\ s[j+1]...s[n-3]$>∈<$s[0]\ s[1]...s[j-1]\ s[j]$ $s[j+1]...s[n-3]$ A B>$< F_1, F_2 >$,

<$s[0]$ A $s[1]...s[j-1]$B $s[j]s[j+1]...s[n-3]$>F_3 =<$s[j]\ s[j+1]...s[n-3]$ A $s[1]...s[j-1]$ B $s[0]$>,

<$s[j]$A $s[j+1]...s[n-3]\ s[1]...s[j-1]$B $s[0]$>∈<$s[j]\ s[j+1]...s[n-3]$ A $s[1]...s[j-1]$ B $s[0]$>$< F_1, F_2 >$,

<$s[j]$ A $s[j+1]...s[n-3]\ s[1]...s[j-1]$ B $s[0]$>F_3 =<$s[0]$ A $s[j+1]...s[n-3]$ $s[1]...s[j-1]$ B $s[j]$>,

<$s[0]\ s[j+1]...s[n-3]$ A $s[1]...s[j-1]$ B $s[j]$>∈<$s[0]$ A $s[j+1]...s[n-3]$ $s[1]...s[j-1]$ B $s[j]$ >$< F_1, F_2 >$,

<$s[0]\ s[j+1]...s[n-3]$ A $s[1]...s[j-1]$B $s[j]$>F_3 =<$s[j]$A $s[1]...s[j-1]$ B $s[0]s[j+1]...s[n-3]$>,

<$s[j]$ A $s[1]...s[j-1]$ B $s[0]\ s[j+1]...s[n-3]$>∈<$s[j]$A $s[1]...s[j-1]$ B $s[0]s[j+1]...s[n-3]$><F_1, F_2>.

Therefore, for any $j=\overline{1, n-3}$ we get $s^{(j)} \in (s) < F_1, F_2, F_3 >$.

Since, <$s[0]...s[n-3]$ A B>F_3= <A B $s[0]...s[n-3]$>, we have <A B $s[0]...s[n-3]$>∈ $(s) < F_1, F_2, F_3 >$.

Thus, transpositions (s, $s^{(j)}$) ∈<F_1, F_2, F_3>It is well known that the symmetric group S_n is generated by transpositions $(0, j)$, $j=\overline{1, n-1}$. Therefore, $S_n = (s) < F_1, F_2, F_3 >$.

Item 4 follows from proposition 10 and item 1. ■

Recall [5] that a semigroup G divides a semigroup H (denote $G|H$) if there exist a subsemigroup R of H such that G is isomorphic to R.

It is easily shown that $< F_2 > | < F_1, F_3 >, < F_1 > | < F_2, F_3 >$.

Theorem 14 $< F_1, F_2, F_3 > \cong < F_1, F_3 > \cong < F_2, F_3 >$.

Proof. The proof follows from proposition 9. ■

Theorem 15 *Let the set* $\Omega = \{S(Z_n^{AB}, r_1, r_2) | r_1, r_2 = \overline{0, n-1}, r_1 \neq r_2\}$ *and* $< \psi_A, F_3 >$ *be the transformation group of* $S(Z_n^{AB})$. *Then*

1. $< \psi_A, F_3 >$ *is imprimitive on* $S(Z_n^{AB})$.
2. *the sets* $S(Z_n^{AB}, r_1, r_2)$, *where* $r_1, r_2 = \overline{0, n-1}, r_1 \neq r_2$, *are imprimitive blocks of* $< \psi_A, F_3 >$ *and* $|S(Z_n^{AB}, r_1, r_2)| = (n-2)!$.
3. *the number of imprimitive blocks is* $n(n-1)$, *i.e.* $|\Omega| = n(n-1)$.
4. *the transformation group* G *of* Ω *is isomorphic to* $< \psi_A, \psi_B >$.
5. $< \psi_A, \psi_B, F_3 > \cong < \psi_A, F_3 > \cong < \psi_B, F_3 >$.

This proposition can be proved as proposition 13 for semigroups.

5 Conclusion

In this paper we began to investigate semigroups and groups properties of the Solitaire stream cipher and its regular modifications. We described the groups $< F_3 >$, $< F_4 >$, $< F_3, F_4 >$ and proved that the group $< F_3, F_4 >$ is an intransitive group.

Also we described properties of the semigroups $< F_1 >$ and $< F_2 >$. As particular, we proved that $< F_1 >$ and $< F_2 >$ are isomorphic

We proposed and investigated group properties of regular modifications of the Solitaire stream cipher It was considered group properties of $< \psi_A >$, $< \psi_B >$ which are regular modifications of $< F_1 >$, $< F_2 >$. We found that $< \psi_A >$ and $< \psi_B >$ are isomorphic; $| < \psi_A, \psi_B > | = n^2(n-1)$ and $| < F_1, F_2 > | \leq n^2(n-1)$.

We obtained that semigroups $< F_1, F_2, F_3 >$, $< F_1, F_3 >$ and $< F_2, F_3 >$ are isomorphic This property is the same as for proposed regular modifications of Solitaire, i.e.$< \psi_A, \psi_B, F_3 > \cong < \psi_A, F_3 > \cong < \psi_B, F_3 >$.

We proved that some properties of the semigroup properties of Solitaire and its regular modifications are the same. Therefore, we can use or investigate proposed regular modifications of Solitaire.

6 References

[1] Schneier B., "*The Solitaire Encryption Algorithm*", http://www.counterpane.com/ solitaire.html.

[2] Pudovkina M, Varfolomeev A.A. "*A Cycle Structure of the Solitaire Keystream Generator*". 3nd International Workshop on Computer Science and Information Technologies CSIT'2001, YFA, 2001

[3] Varfolomeev A.A., Zhukov A.E., Pudovkina M.A., "*Analysis of Stream Ciphers* ', Moscow, MEPhI, 2000

[4] Wielandt H. *Finite permutation groups*. -New York and London: Academic Press, 1964.

[5] Clifford A. H., Preston G. B., *The algebraic theory of semigroups*, Vol 1. Am. Math., Soc., Providence, Rhode Island, 1964.