Journal of Algebraic Systems
Vol. 3, No. 1, (2015), pp 83-95

COMPUTING THE PRODUCTS OF CONJUGACY CLASSES FOR SPECIFIC FINITE GROUPS

MARYAM JALALI-RAD AND ALI REZA ASHRAFI*

ABSTRACT. Suppose G is a finite group, A and B are conjugacy classes of G, and $\eta(AB)$ denotes the number of conjugacy classes contained in AB. The set of all $\eta(AB)$, such that A, B run over conjugacy classes of G, is denoted by $\eta(G)$. The aim of this paper is to compute $\eta(G)$, for $G \in \{D_{2n}, T_{4n}, U_{6n}, V_{8n}, SD_{8n}\}$ or G is a decomposable group of order $2pq$, a group of order $4p$ or p^3, where p and q are primes.

1. Introduction

Throughout this paper, all groups are assumed to be finite. If G is such a group, and A and B are conjugacy classes of G, then it is an elementary fact that AB is a $G-$invariant subset. Thus, AB can be written as a union of conjugacy classes of G. The number of distinct conjugacy classes of G contained in AB is denoted by $\eta(AB)$. The set of all $\eta(AB)$, such that A, B run over conjugacy classes of G, is denoted by $\eta(G)$.

The most important works on the problem of computing the number of $G-$conjugacy classes in the product of conjugacy classes were carried out by Adan−Bante. Here, we report some of her interesting results in this topic. Suppose $SL(2, q)$ is the group of 2×2 matrices, with determinant one over a finite field of order q. Adan−Bante and Harris [3] proved that if q is even, then the product of any two noncentral conjugacy classes of $SL(2, q)$ is a union of at least $q - 1$ distinct

MSC(2010): Primary: 20E45; Secondary: 20C15
Keywords: Conjugacy class, $G-$invariant subset, $p-$group.
Received: 30 November 2014, Revised: 27 April 2015.
*Corresponding author .

conjugacy classes of $SL(2,q)$; and if $q>3$ is odd, then the product of any two non-central conjugacy classes of $SL(2,q)$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes of $SL(2,q)$. Adan−Bante [1] proved that, for any finite supersolvable group G, and any conjugacy class A of G, $dl(\frac{G}{C_G(A)}) \leq 2\eta(AA^{-1})-1$, where $C_G(A)$ denotes the centralizer of A in G, and $dl(H)$ is the derived length of a group H. In [2], she also proved that if p is an odd prime number, G is a finite $p-$group, and a^G and b^G are the conjugacy classes of G of size p; then either $a^Gb^G=(ab)^G$ or a^Gb^G is a union of at least $\frac{p+1}{2}$ distinct conjugacy classes. If G is nilpotent, and a^G is again a conjugacy class of G of size p, then either $a^Ga^G=(a^2)^G$ or a^Ga^G is a union of exactly $\frac{p+1}{2}$ distinct conjugacy classes of G of size p.

Darafsheh and Robati [6] continued the works of Adan−Bante and proved that if $[a,G]=\{[a,x] \mid x\in G\}$, and $[a,G]$ be a subset of $Z(G)$, then we have:

i. $\eta(a^Gb^G)=|a^G||b^G|/|[a,G]\cap(b^{-1})^Gb^G||(ab)^G|$;
ii. If $a^Gb^G\cap Z(G)\neq\emptyset$, then $\eta(a^Gb^G)=|a^G|$;
iii. If $|a^G|$ is an odd number, then $\eta(a^Ga^G)=1$;
iv. If $|a^G|$ is an even number, then $\eta(a^Ga^G)=2^n$, where n is the number of cyclic direct factors in the decomposition of the Sylow $2-$subgroup of $[a,G]$.

We encourage the interested readers to consult also the papers by Arad and his co-authors [4, 5], and references therein for more information on this topic. Our notation is standard, and can be taken from [9, 10].

2. Main results

The aim of this section is to compute $\eta(G)$, where

$$G\in\{D_{2n},V_{8n},T_{4n},U_{6n},SD_{8n}\}$$

or G is a group of orders $2pq, 4p, p^3$, such that p and q are prime numbers. The case of $|G|=2pq$ and G that is indecomposable, is retained as an open question. The semi-dihedral group SD_{8n}, dicyclic group T_{4n}, and the groups U_{6n} and V_{8n} have the following presentations, respectively:

$$\begin{aligned}
SD_{8n} &= \langle a,b \mid a^{4n}=b^2=e,\ bab=a^{2n-1}\rangle,\\
T_{4n} &= \langle a,b \mid a^{2n}=1, a^n=b^2, b^{-1}ab=a^{-1}\rangle,\\
U_{6n} &= \langle a,b \mid a^{2n}=b^3=e,\ bab=a\rangle,\\
V_{8n} &= \langle a,b \mid a^{2n}=b^4=e,\ aba=b^{-1},\ ab^{-1}a=b\rangle.
\end{aligned}$$

It is easy to see the dicyclic group T_{4n} has the order $4n$, and the cyclic subgroup $\langle a\rangle$ of T_{4n} has the index 2 [10]. The conjugacy classes of U_{6n} and V_{8n} (n is odd), computed in the famous book of James and Liebeck [10]. The groups V_{8n} (n is even), and SD_{8n} have the order $8n$, and their conjugacy classes have been computed in [7, 8], respectively.

The following simple lemma is crucial throughout this paper:

Lemma 2.1. *Suppose G is a finite group, and A and B are conjugacy classes of G. Then,*

(1) $\eta(AB) = \eta(BA)$,
(2) *If A is central, then* $\eta(AB) = 1$,
(3) *If* $|A| = |B| = 2$, *then* $\eta(AB) = 1, 2$ [2, Proposition 2.7],
(4) $\eta(AB) \leq |A|$ [6, Lemma 3.1].

Proposition 2.2.

$$\eta(D_{2n}) = \begin{cases} \{1, 2, \frac{n+1}{2}\} & 2 \nmid n \\ \{1, 2, \frac{n}{4}, \frac{n}{4}+1\} & n \equiv 0 \pmod 4 \\ \{1, 2, \frac{n+2}{4}\} & n \equiv 2 \pmod 4 \end{cases}.$$

Proof. The dihedral group D_{2n} can be presented by

$$D_{2n} = \langle a, b \mid a^n = b^2 = e,\ b^{-1}ab = a^{-1}\rangle.$$

We first assume that n is odd. Then the conjugacy classes of D_{2n} are $\{e\}, \{a^r, a^{-r}\}, 1 \leq r \leq \frac{n-1}{2}$ or $\{a^s b; 0 \leq s \leq n-1\}$. Thus the products of non$-$identity conjugacy classes are:

- $\{a^r, a^{-r}\} \cdot \{a^s, a^{-s}\} = \{a^{r+s}, a^{-(r+s)}\} \cup \{a^{r-s}, a^{-(r-s)}\}$,
- $\{a^r, a^{-r}\} \cdot \{a^s b; 0 \leq s \leq n-1\} = \{a^{r+s}b, a^{s-r}b; 0 \leq s \leq n-1\} = \{a^s b; 0 \leq s \leq n-1\}$,
- $\{a^s b; 0 \leq s \leq n-1\} \cdot \{a^r b; 0 \leq r \leq n-1\} = \{a^s b a^r b; 0 \leq r, s \leq n-1\} = \bigcup_{r=0}^{\frac{n-1}{2}} \{a^r, a^{-r}\}$.

Hence, $\eta(D_{2n}) = \{1, 2, \frac{n+1}{2}\}$. Next, assume that $n = 2m$. The conjugacy classes of D_{2n} are $\{e\}, \{a^m\}\{a^r, a^{-r}\}, 1 \leq r \leq m-1, \{a^s b; 0 \leq s \leq 2(n-1), 2 \mid s\}, \{a^s b; 0 \leq s \leq 2(n-1), 2 \nmid s\}$. Suppose $0 \leq r, l \leq m-1$, $F_1 = \{0 \leq s \leq 2(n-1), 2 \mid s\}$, and $F_2 = \{0 \leq s \leq 2(n-1), 2 \nmid s\}$. The products of non$-$identity conjugacy classes are as follows:

$$\begin{aligned}
\{a^r, a^{-r}\} \cdot \{a^l, a^{-l}\} &= \{a^{r-l}, a^{l-r}\} \cup \{a^{r+l}, a^{-(l+r)}\},\\
\{a^r, a^{-r}\} \cdot \{a^s b; s \in F_1\} &= \begin{cases} \{a^s b; s \in F_1\} & 2 \mid r \\ \{a^s b; s \in F_2\} & 2 \nmid r \end{cases},\\
\{a^r, a^{-r}\} \cdot \{a^s b; s \in F_2\} &= \begin{cases} \{a^s b; s \in F_1\} & 2 \nmid r \\ \{a^s b; s \in F_2\} & 2 \mid r \end{cases},\\
\{a^s b; s \in F_1\} \cdot \{a^r b; r \in F_1\} &= \{e\} \cup \begin{cases} \bigcup_{r=1}^{\frac{n-2}{4}} \{a^{2r}, a^{-2r}\} & n \equiv 2 \pmod 4 \\ \bigcup_{r=1}^{\frac{n}{4}} \{a^{2r}, a^{-2r}\} & n \equiv 0 \pmod 4 \end{cases},\\
\{a^s b; s \in F_1\} \cdot \{a^r b; r \in F_2\} &= \{e\} \cup \begin{cases} \bigcup_{r=1}^{\frac{n-2}{4}} \{a^{2r}, a^{-2r}\} & n \equiv 0 \pmod 4 \\ \bigcup_{r=1}^{\frac{n}{4}} \{a^{2r}, a^{-2r}\} & n \equiv 2 \pmod 4 \end{cases},\\
\{a^s b; s \in F_2\} \cdot \{a^r b; s \in F_2\} &= \{e\} \cup \begin{cases} \bigcup_{r=0}^{\frac{n-6}{4}} (a^{2r+1})^{D_{2n}} & n \equiv 2 \pmod 4 \\ \bigcup_{r=0}^{\frac{n}{4}} (a^{2r+1})^{D_{2n}} & n \equiv 0 \pmod 4 \end{cases}.
\end{aligned}$$

This completes the proof. □

Proposition 2.3.

$$\eta(V_{8n}) = \begin{cases} \{1, 2, \frac{n}{2}, \frac{n}{2}+1\} & n \textit{ is even} \\ \{1, 2, n, n+1\} & n \textit{ is odd} \end{cases}.$$

Proof. By Lemma 2.1 (1, 2), it is enough to compute $\eta(AB)$, where A and B are the non-central conjugacy classes of V_{8n}. Our main proof considers two separate cases, in which n is odd or even.

We first assume that n is odd. Then by [10], the conjugacy classes of V_{8n} are as follows:

$\{e\}$, $\{b^2\}$, $\{a^{2r+1}, a^{-(2r+1)}b^2\}$, $0 \le r \le \frac{n-1}{2}$, $\{a^{2s}, a^{-2s}\}$, $\{a^{2s}b^2, a^{-2s}b^2\}$, $1 \le s \le \frac{n-1}{2}$, $\{a^j b^k; k = 1, 3 \ \&\ 2 \mid j\}$ and $\{a^j b^k; k = 1, 3 \ \&\ 2 \nmid j\}$.

Before starting our calculations, we notice that if A and B are two conjugacy classes of length 2, then by Lemma 2.1 (3), $\eta(AB) = 2$. Thus, it is enough to consider the cases where $(|A|, |B|) \neq (2, 2)$.

- $(a^{2s}, a^{-2s}\} \cdot \{a^j b^k; k = 1, 3\} = \{a^{j+2s} b^k; k = 1, 3\} \cup \{a^{j-2s} b^k; k = 1, 3\}$,
- $\{a^{2r+1}, a^{-(2r+1)}b^2\} \cdot \{a^j b^k; k = 1, 3 \ \&\ 2 \nmid j\} = \{a^j b^k; k = 1, 3 \ \&\ 2 \mid j\} \cup \{a^j b^k; k = 1, 3 \ \&\ 2 \nmid j\}$,
- $\{a^{2r+1}, a^{-(2r+1)}b^2\} \cdot \{a^j b^k; k = 1, 3 \ \&\ 2 \mid j\} = \{a^j b^k; k = 1, 3 \ \&\ 2 \nmid j\}$,
- $\{a^{2s}b^2, a^{-2s}b^2\} \cdot \{a^j b^k; k = 1, 3 \ \&\ 2|j\} = \{a^j b^k; k = 1, 3 \ \&\ 2 \mid j\}$,
- $(b)^{V_{8n}} \cdot (b)^{V_{8n}} = \bigcup_{s=0}^{\frac{n-1}{2}} \{a^{2s}, a^{-2s}\} \bigcup_{s=0}^{\frac{n-1}{2}} \{a^{2s}b^2, a^{-2s}b^2\}$,
- $(ab)^{V_{8n}} \cdot (ab)^{V_{8n}} = \bigcup_{s=0}^{\frac{n-1}{2}} \{a^{2s}, a^{-2s}\} \bigcup_{s=0}^{\frac{n-1}{2}} \{a^{2s}b^2, a^{-2s}b^2\}$,
- $(b)^{V_{8n}} \cdot (ab)^{V_{8n}} = \bigcup_{r=0}^{\frac{n-1}{2}} \{a^{2r+1}, a^{-(2r+1)}b^2\}$.

Next, we assume that $n = 2l$ is even. Then, by [6], the conjugacy classes of V_{8n} are $\{e\}$, $\{b^2\}$, $\{a^n\}$, $\{a^n b^2\}$, $\{a^{2k+1} b^{(-1)^{k+1}};\ 0 \le k \le n-1\}$, $\{a^{2r+1}, a^{-(2r+1)}b^2\}$, $0 \le r \le n-1$, $\{a^{2s}, a^{-2s}\}$, $\{a^{2s}b^2, a^{-2s}b^2\}$,

$1 \leq s \leq \frac{n}{2}-1$, $\{a^{2k}b^{(-1)^k}; 0 \leq k \leq n-1\}$, $\{a^{2k}b^{(-1)^{k+1}}\ ;\ 0 \leq k \leq n-1\}$, $\{a^{2k+1}b^{(-1)^k}\ ;\ 0 \leq k \leq n-1\}$. Suppose $0 \leq k \leq n-1$, and $0 \leq r, s \leq \frac{n}{2}-1$. Then the product of non-central conjugacy classes are as follows:

- $\{a^{2s}, a^{-2s}\} \cdot \{a^{2r}, a^{-2r}\} = \{a^{2(r+s)}, a^{-2(r+s)}\} \cup \{a^{2(r-s)}, a^{-2(r-s)}\}$.
- Suppose:
  $F = \{b^2\} \cup \{a^n b^2\} \bigcup_{r=1, 2\nmid r}^{\frac{n}{2}-1} \{a^{2s}, a^{-2s}\} \bigcup_{r=1,2|r}^{\frac{n}{2}-1} \{a^{2s}b^2, a^{-2s}b^2\}$.
  Then $\{a^{2k}b^{(-1)^k}; 0 \leq k \leq n-1\} \cdot \{a^{2k}b^{(-1)^k}; 0 \leq k \leq n-1\}$ can be simplified as follows:
  $$F \cup \begin{cases} \{a^n b^2\} & n \equiv 0 \pmod 4 \\ \{a^n\} & n \equiv 2 \pmod 4 \end{cases}.$$
  Therefore, $\eta(b^{V_{8n}}.b^{V_{8n}}) = \frac{n}{2}+1$.
- In a similar argument as above, we have:
  $$\begin{aligned} \eta((b)^{V_{8n}}.(b^{-1})^{V_{8n}}) &= \eta((ab^{-1})^{V_{8n}}.(ab^{-1})^{V_{8n}}) \\ &= \eta((ab^{-1})^{V_{8n}}.(ab)^{V_{8n}}) \\ &= \eta((b^{-1})^{V_{8n}}.(b^{-1})^{V_{8n}}) \\ &= \eta((b^{-1})^{V_{8n}}.(ab)^{V_{8n}}) \\ &= \eta((ab)^{V_{8n}}.(ab)^{V_{8n}}) = \frac{n}{2}+1. \end{aligned}$$
- In the following case, it can be proved that $\eta((ab^{-1})^{V_{8n}}.b^{V_{8n}}) = \frac{n}{2}$.
  $$(ab^{-1})^{V_{8n}} \cdot (b^{-1})^{V_{8n}} = \bigcup_{r=1,2\nmid r}^{n-1} \{a^{2r+1}, a^{-(2r+1)}b^2\}.$$
- For the following product of conjugacy classes, we have:
  $$\eta((ab^{-1})^{V_{8n}}.(b)^{V_{8n}}) = \eta((b)^{V_{8n}}.(ab)^{V_{8n}}) = \frac{n}{2}.$$
- $$(a^{2r+1})^{V_{8n}} \cdot (b^{-1})^{V_{8n}} = \begin{cases} (ab^{-1})^{V_{8n}} & r \equiv 1 \pmod 4 \\ (b^{-1})^{V_{8n}} & r \equiv 3 \pmod 4 \end{cases}.$$
- $$(a^{2r+1})^{V_{8n}} \cdot (ab)^{V_{8n}} = \begin{cases} (b^{-1})^{V_{8n}} & r \equiv 1 \pmod 4 \\ (b)^{V_{8n}} & r \equiv 3 \pmod 4 \end{cases}.$$
- $$(a^{2r+1})^{V_{8n}} \cdot (ab^{-1})^{V_{8n}} = \begin{cases} (b)^{V_{8n}} & r \equiv 1 \pmod 4 \\ (ab)^{V_{8n}} & r \equiv 3 \pmod 4 \end{cases}.$$

- $$(a^{2r+1})^{V_{8n}} \cdot (b)^{V_{8n}} = \begin{cases} (ab)^{V_{8n}} & r \equiv 1 \pmod 4 \\ (ab^{-1})^{V_{8n}} & r \equiv 1 \pmod 4 \end{cases}.$$

The product of Conjugacy classes of length two by another conjugacy class of two given types is again a conjugacy class. This completes the proof. □

Proposition 2.4.

$$\eta(T_{4n}) = \begin{cases} \{1, 2, \frac{n}{2}, \frac{n}{2} + 1\} & n \text{ is even} \\ \{1, 2, \frac{n+1}{2}\} & n \text{ is odd} \end{cases}.$$

Proof. By [10, p. 420], the conjugacy classes of T_{4n} are $\{e\}$, $\{a^n\}$, $\{a^r, a^{-r}\}$, $1 \leq r \leq n-1$, $\{a^{2j}b, 0 \leq j \leq n-1\}$, $\{a^{2j+1}b, 0 \leq j \leq n-1\}$. On the other hand, the product of conjugacy classes can be computed, as follows:

- $\{a^r, a^{-r}\} \cdot \{a^s, a^{-s}\} = \{a^{r+s}, a^{-(r+s)}\} \cup \{a^{r-s}, a^{-(r-s)}\}$.
- Since $(a^r)^{T_{4n}} \cdot (b)^{T_{4n}} = \{a^{r+2j}b, a^{-r+2j}b \ ; \ 0 \leq j \leq n-1\}$, the product is $(b)^{T_{4n}}$, when r is even. If r is odd, then the product will be $(ab)^{T_{4n}}$.
- We know that $(a^r)^{T_{4n}} \cdot (ab)^{T_{4n}} = \{a^{r+2j+1}b, a^{-r+2j+1}b \ ; \ 0 \leq j \leq n-1\}$. If r is even, then the product is $(ab)^{T_{4n}}$, and if r is odd, then the product will be $(b)^{T_{4n}}$.
- $$(b)^{T_{4n}} \cdot (b)^{T_{4n}} = \begin{cases} \bigcup_{r=0,2|r}^{n}\{a^r, a^{-r}\} & 2 \mid n \\ \bigcup_{r=1,2\nmid r}^{n}\{a^r, a^{-r}\} & 2 \nmid n \end{cases}.$$
- $$(b)^{T_{4n}} \cdot (ab)^{T_{4n}} = \begin{cases} \bigcup_{r=1,2\nmid r}^{n-1}\{a^r, a^{-r}\} & 2 \mid n \\ \bigcup_{r=0,2\nmid r}^{n-1}\{a^r, a^{-r}\} & 2 \nmid n \end{cases}.$$
- $$(ab)^{T_{4n}} \cdot (ab)^{T_{4n}} = \begin{cases} \bigcup_{r=0,2|r}^{n}\{a^r, a^{-r}\} & 2 \mid n \\ \bigcup_{r=1,2\nmid r}^{n}\{a^r, a^{-r}\} & 2 \nmid n \end{cases}.$$

This completes the proof. □

Example 2.5. Suppose G is a non-abelian group of order $4p$; p is prime. By an easy calculation, one can see that $\eta(D_8) = \eta(Q_8) = \eta(D_{12}) = \eta(Z_3 : Z_4) = \eta(A_4) = \{1, 2\}$, where $Z_3 : Z_4$ is a non-abelian group of order 12 different from A_4 and D_{12}. Thus, it is enough to consider that case that $p > 3$. Our proof considers two cases Thus $4|p-1$ or $4 \not| p-1$.

Case 1. $4|p-1$. If $4|p-1$, then up to isomorphism, there are three groups of order $4p$. These are D_{4p}, T_{4p}, and F_{4p}, where F_{4p} can be presented by $F_{4p} = \langle a, b | a^p = b^4 = 1, b^{-1}ab = a^{\lambda} \rangle$, and $\lambda^2 \equiv -1 \pmod p$. By Propositions 2 and 4, $\eta(D_{4p}) = \eta(T_{4p}) = \{1, 2, \frac{p+1}{2}\}$, and $\eta(F_{4p}) = \{1, 3, 4, \frac{p+3}{4}\}$.

Case 2. $4 \nmid p-1$. In this case, there are up to isomorphism two groups of order $4p$. These are D_{4p} and T_{4p}. As in Case 1, $\eta(D_{4p}) = \eta(T_{4p}) = \{1, 2, \frac{p+1}{2}\}$, as desired.

Therefore,

$$\eta(G) \in \begin{cases} \{\{1, 2, \frac{p+1}{2}\}\} & p > 3, 4 \nmid p-1 \\ \{\{1, 2, \frac{p+1}{2}\}, \{1, 3, 4, \frac{p+3}{4}\}\} & p > 3, 4 \mid p-1 \\ \{\{1, 2\}\} & p = 3 \end{cases}.$$

Proposition 2.6. $\eta(U_{6n}) = \{1, 2\}$.

Proof. By [10], the conjugacy classes of U_{6n} are $\{e\}$, $\{a^{2r}\}$, $\{a^{2r}b, a^{2r}b^2\}$, $\{a^{2r+1}, a^{2r+1}b, a^{2r+1}b^2\}$, $0 \leq r \leq n-1$. On the other hand, by Lemma 2.1 (4), $\eta((a^{2r}b)^{U_{6n}} \cdot (a^{2s+1})^{U_{6n}}) \leq 2$. But, $(a^{2r+1})^{U_{6n}} \cdot (a^{2s+1})^{U_{6n}} = \{a^{2(r+s+1)}\} \cup \{a^{2(r+s+1)}b, a^{2(r+s+1)}b^2\}$. Thus, $\eta(U_{6n}) = \{1, 2\}$, as desired. □

Hormozi and Rodtes [8, Definition 2.1], defined $C^{even} = C_1 \cup C_2^{even} \cup C_3^{even}$ and $C^{odd} = C_1 \cup C_2^{odd} \cup C_3^{odd}$, where $C_1 = \{0, 2, 4, \cdots, 2n\}$, $C_2^{even} = \{1, 3, 5, \cdots, n-1\}$, $C_3^{even} = \{2n+1, 2n+3, 2n+5, \cdots, 3n-1\}$, $C_2^{odd} = \{1, 3, 5, \cdots, n\}$, $C_3^{odd} = \{2n+1, 2n+3, 2n+5, \cdots, 3n\}$, $C_{even}^{\dagger} = C_1 \setminus \{0, 2n\}$ and $C_{odd}^{\dagger} = C_2^{even} \cup C_3^{even}$. Moreover, $C_{\star}^{even} = C^{even} \setminus \{0, 2n\}$ and $C_{\star}^{odd} = C^{odd} \setminus \{0, n, 2n, 3n\}$.

Proposition 2.7.

$$\eta(SD_{8n}) = \begin{cases} \{1, 2, n, n+1\} & n \text{ is even} \\ \{1, 2, \frac{n+1}{2}\} & n \text{ is odd} \end{cases}.$$

Proof. By [8, Proposition 2.2], the conjugacy classes of SD_{8n}; $n \geq 2$, can be computed in two separate cases, where n is odd or even. If n is even, then there are $2n+3$ conjugacy classes as: $\{e\}$, $\{a^{2n}\}$, $\{a^r, a^{(2n-1)r}\}; r \in C_*^{even}$, $\{ba^{2t} \mid t = 0, 1, 2, \cdots, 2n-1\}$ and $\{ba^{2t+1} \mid t = 0, 1, 2, \cdots, 2n-1\}$. If n is odd, then there are $2n+6$ conjugacy classes as $\{e\}$, $\{a^n\}$, $\{a^{2n}\}$, $\{a^{3n}\}$, $\{a^r, a^{(2n-1)r}\}; r \in C_*^{odd}$, $\{ba^{4t} \mid t = 0, 1, 2, \cdots, n-1\}$, $\{ba^{4t+1} \mid t = 0, 1, 2, \cdots, n-1\}$, $\{ba^{4t+2} \mid t = 0, 1, 2, \cdots, n-1\}$ and $\{ba^{4t+3} \mid t = 0, 1, 2, \cdots, n-1\}$. On the other hand by [8], we have:

(1) $(2n-1)r \equiv (4n-r) \pmod{4n}$, if r is even,

(2) $(2n-1)r \equiv (2nr) \pmod{4n}$, if r is odd,

(3) $(2n-1)(2n+k) \equiv (4n-k) \pmod{4n}$, if k is odd.

If n is even, then the product of conjugacy classes, of SD_{8n} are as follows:

- $\{a^r, a^{(2n-1)r} \ \& \ 2|r\} \cdot \{a^s, a^{(2n-1)s} \ \& \ 2|s\} = \{a^r, a^{(2n-1)r} \ \& \ 2 \nmid r\} \cdot \{a^s, a^{(2n-1)s} \ \& \ 2 \nmid s\} = (a^{r+s})^{SD_{8n}} \cup (a^{r+(2n-1)s})^{SD_{8n}}$,
- $\{a^r, a^{(2n-1)r} \ \& \ 2|r\} \cdot (b)^{SD_{8n}} = \{a^r, a^{(2n-1)r} \ \& \ 2 \nmid r\} \cdot (ba)^{SD_{8n}} = (b)^{SD_{8n}}$,
- $\{a^r, a^{(2n-1)r} \ \& \ 2|r\} \cdot (ba)^{SD_{8n}} = \{a^r, a^{(2n-1)r} \ \& \ 2 \nmid r\} \cdot (b)^{SD_{8n}} = (ba)^{SD_{8n}}$,
- $(b)^{SD_{8n}} \cdot (b)^{SD_{8n}} = (ba)^{SD_{8n}} \cdot (ba)^{SD_{8n}} = \bigcup_{r \in C_1} \{a^r, a^{(2n-1)r}\}$,
- $(b)^{SD_{8n}} \cdot (ba)^{SD_{8n}} = \bigcup_{r \in C_2^{even} \cup C_3^{even}} \{a^r, a^{(2n-1)r}\}$.

If n is odd, then the products of conjugacy classes of SD_{8n} are as follows:

- $(a^r)^{SD_{8n}} \cdot (a^s)^{SD_{8n}} = \{a^{r+s}, a^{(2n-1)(r+s)}\} \cup \{a^{r+(2n-1)s}, a^{s+(2n-1)r}\}$,
- $(a^r)^{SD_{8n}} \cdot (ba^i)^{SD_{8n}} = (ba^j)^{SD_{8n}}$, where $j = i-r,\ i+2n-r$, when r is even or odd, respectively.
- $(b)^{SD_{8n}} \cdot (b)^{SD_{8n}} = (ba^2)^{SD_{8n}} \cdot (ba^2)^{SD_{8n}} = (ba)^{SD_{8n}} \cdot (ba^3)^{SD_{8n}} = \bigcup_{r \in C_1, r \equiv 0 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(b)^{SD_{8n}} \cdot (ba)^{SD_{8n}} = \bigcup_{r \in C_2^{odd} \cup C_3^{odd}, r \equiv 1 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(ba^2)^{SD_{8n}} \cdot (ba^3)^{SD_{8n}} = \bigcup_{r \in C_2^{odd} \cup C_3^{odd}, r \equiv 1 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(b)^{SD_{8n}} \cdot (ba^2)^{SD_{8n}} = \bigcup_{r \in C_1, r \equiv 2 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(ba)^{SD_{8n}} \cdot (ba)^{SD_{8n}} = \bigcup_{r \in C_1, r \equiv 2 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(b)^{SD_{8n}} \cdot (ba^3)^{SD_{8n}} = \bigcup_{r \in C_2^{odd} \cup C_3^{odd}, r \equiv 3 \pmod 4} \{a^r, a^{(2n-1)r}\}$,
- $(ba)^{SD_{8n}} \cdot (ba^2)^{SD_{8n}} = \bigcup_{r \in C_2^{odd} \cup C_3^{odd}, r \equiv 3 \pmod 4} \{a^r, a^{(2n-1)r}\}$,

which completes the proof. □

The Frobenius group $F_{p,q}$ can be presented by

$$F_{p,q} = \langle a, b \mid a^p = b^q = e, b^{-1}ab = a^u \rangle,$$

where $u^q \equiv 1\ (mod\ p)$ [10, Definition 25.6]. Let L be the subgroup of $\mathbb{Z}_p^*$ consisting of the powers of u and $r = (p-1)/q$. Choose coset representatives $v_1, \cdots, v_r$ for L in $\mathbb{Z}_p^*$. By [10, Proposition 25.9], the conjugacy classes of $F_{p,q}$ are as follows:

$$\{e\},$$
$$(a^{v_i})^{F_{p,q}} = \{a^{v_i l} : l \in L\}\ (1 \le i \le r),$$
$$(b^n)^{F_{p,q}} = \{a^m b^n :\ 0 \le m \le p-1\}(1 \le n \le q-1).$$

Then $(b^i)^{F_{p,q}} \cdot (b^j)^{F_{p,q}} = (b^{i+j})^{F_{p,q}}$, when $i+j \ne q$. If $i+j=q$, then $(b^i)^{F_{p,q}} \cdot (b^j)^{F_{p,q}} = \bigcup_{i=1}^{r}(a^{v_i})^{F_{p,q}} \cup (b^{i+j})^{F_{p,q}}$. On the other hand, $(a^{v_i})^{F_{p,q}} \cdot (b^j)^{F_{p,q}} = (b^j)^{F_{p,q}}$, and $(a^{v_i})^{F_{p,q}} \cdot (a^{v_j})^{F_{p,q}} = \cup(a^{v_k})^{F_{p,q}}$ such that $v_k \equiv v_i u^m + v_j u^t\ (mod\ p)$, where $0 \le m, t \le q-1$. We have explicitly computed the set $\eta(F_{p,q})$ for several pairs of distinct primes p and q, such that $q \nmid p-1$. However, we were unable to find a general formula for $\eta(F_{p,q})$.

Question 2.8. Is it possible to find a closed formula for $\eta(F_{p,q})$?

Suppose p and q are primes, and $q|p-1$. Define:

$$S_{p,q} = \langle a, b, c \mid a^p = b^q = c^2 = e, cac = a^{-1}, bc = cb, b^{-1}ab = a^r, r^q \equiv 1\ (mod\ p)\rangle.$$

Proposition 2.9. *Suppose G is a group of order $2pq$, p and q, $p > q$, are odd primes, and $G \ncong S_{p,q}$. Then*

$$\eta(G) \in \{\{1\}, \{1, 2, \frac{p+1}{2}\}, \{1, 2, \frac{q+1}{2}\}, \{1, 2, \frac{pq+1}{2}\}, \eta(F_{p,q})\}.$$

Proof. Suppose p and q are distinct odd primes, and $p > q$. Following Zhang et al. [12], if $q \nmid p-1$, then there are four non-abelian groups of order $2pq$, and if $q|p-1$, the number of such groups is six. These groups are: $R_1 = Z_{2pq}$, $R_2 = D_{2pq}$, $R_3 = Z_q \times D_{2p}$, $R_4 = Z_p \times D_{2q}$, $R_5 = Z_2 \times F_{p,q}$, and $S_{p,q}$. The last two groups are for the case when $q|p-1$. We first notice that by Proposition 2, $\eta(R_2) = \eta(D_{2pq}) = \{1, 2, \frac{pq+1}{2}\}$. Since R_1 is abelian, $\eta(R_1) = \{1\}$. On the other hand, if G is abelian and H is an arbitrary group, then it is easy to see that $\eta(G \times H) = \eta(H)$. This implies that $\eta(R_4) = \eta(Z_p \times D_{2q}) = \eta(D_{2q}) = \{1, 2, \frac{q+1}{2}\}$, $\eta(R_3) = \eta(Z_q \times D_{2p}) = \eta(D_{2p}) = \{1, 2, \frac{p+1}{2}\}$, and $\eta(R_5) = \eta(Z_2 \times F_{p,q}) = \eta(F_{p,q})$. □

At the end of this section, we apply [6, Theorem B] for computing $\eta(G)$, where G is a non-abelian groups of order p^3; p is odd. These groups can be represented by

i. $G_1 = < a, b; a^{p^2} = b^p = e; b^{-1}ab = a^{1+p} >$,
ii. $G_2 = < a, b, z; a^p = b^p = z^p = e, az = za, bz = zb, b^{-1}ab = az >$.

It is well-known that $G_1' = Z(G_1) = \langle a^p \rangle$, and $G_2' = Z(G_2) = \langle z \rangle$. To apply [6, Theorem B], we first compute $[x, G_1]$ and $[y, G_2]$, where $x \in G_1$ and $y \in G_2$. We have:

$$\begin{aligned}
[a^ib^j, G_1] &= \{[a^ib^j, a^rb^s]; 0 \le r \le p^2-1, 0 \le s \le p-1\}, \\
&= \{a^i(b^ja^rb^{-j})(b^sa^{-i}b^{-s})a^{-r}; 0 \le r \le p^2-1, 0 \le s \le p-1\}, \\
&= \{a^ia^{r(1+p)^j}a^{-i(1+p)^s}a^{-r}; 0 \le r \le p^2-1, 0 \le s \le p-1\}, \\
&= \{a^{p(rj-is)}; 0 \le r \le p^2-1, 0 \le s \le p-1\}
\end{aligned}$$

and

$$\begin{aligned}
[a^ib^jz^k, G_2] &= \{[a^ib^jz^k, a^rb^sz^t]; 0 \le r, s \le p-1\}, \\
&= \{(a^ib^jz^k)(a^rb^sz^t)(a^ib^jz^k)^{-1}(a^rb^sz^t)^{-1}; 0 \le r, s \le p-1\}, \\
&= \{a^ib^ja^r(b^{s-j}a^{-i}b^{-s})a^{-r}; 0 \le r, s \le p-1\}, \\
&= \{a^ib^ja^r(a^{-i}b^{-j}z^{(s-j)i})a^{-r}; 0 \le r, s \le p-1\}, \\
&= \{z^{(p-j)(r-i)}; 0 \le r, s \le p-1\}.
\end{aligned}$$

Therefore, $[x, G_1] = Z(G_1)$, and $[y, G_2] = Z(G_2)$ and, by [6, Theorem A(ii)], $x^{G_1}(x^{-1})^{G_1} = [x, G_1]$ and $y^{G_2}(y^{-1})^{G_2} = [y, G_2]$. This implies that for each $u, v \in G_1$ and $u', v' \in G_2$, $|[u, G_1] \cap v^{G_1}(v^{-1})^{G_1}| = |[u, G_1] \cap [v, G_1]| = p$, and $|[u', G_2] \cap v'^{G_2}(v'^{-1})^{G_2}| = |[u', G_2] \cap [v', G_2]| = p$. If $u, v \in G_1$ and $u', v' \in G_2$ are non-identity, then by [6, Theorem B(i)], $\eta(G_1) = \eta(G_2) = \{1, p\}$.

3. Concluding Remarks

In this paper, the set $\eta(G)$ was computed for some classes of finite groups. It seems that computing $\eta(G)$ for some known group G returns to some open questions in the number theory. For example, the group $G = S_{p,q}$ in Proposition 9 has exactly $\frac{4q^2+p-1}{2q}$ conjugacy classes. These are:

$$\begin{aligned}
e^G &= \{e\}, c^G = \{c, ca, ca^2, \cdots, ca^{p-1}\}, \\
(b^i)^G &= \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\}; 1 \le i \le q-1, \\
(cb^i)^G &= \{cb^i, cb^ia, cb^ia^2, \cdots, cb^ia^{p-1}\}; 1 \le i \le q-1, \\
(a^i)^G &= \{a^i, a^{ir}, \cdots, a^{ir^{q-1}}, a^{-i}, a^{-ir}, \cdots, a^{-ir^{q-1}}\}; 1 \le i \le \frac{p-1}{2q}.
\end{aligned}$$

Since $(a^{-i}ba^i) = a^{-i-1}(ab)a^i = a^{-i-1}(ba^r)a^i = a^{-i-1}ba^{i+r} = a^{-i-2}(ab)$ $a^{i+r} = a^{-i-2}(ba^r)a^{i+r} = a^{-i-2}ba^{i+2r} = \cdots = ba^{i(1-r)}$,

$$\begin{aligned}(c^kb^ja^i)^{-1}(b^l)(c^kb^ja^i) &= a^{-i}b^{-j}c^{-k}b^lc^kb^ja^i \\ &= a^{-i}b^{-j}b^lb^ja^i \\ &= a^{-i}b^la^i \\ &= (a^{-i}ba^i)^l \\ &= (ba^{i(1-r)})^l = (b^la^{i(1-r^l)}).\end{aligned}$$

On the other hand, since $(a^{-i}ba^i) = a^{-i-1}(ab)a^i = a^{-i-1}(ba^r)a^i = a^{-i-1}(b)a^{i+r} = a^{-i-2}(ab)a^{i+r} = a^{-i-2}(ba^r)a^{i+r} = a^{-i-2}ba^{i+2r} = \cdots = ba^{i(1-r)}$,

$$\begin{aligned}(a^ib^jc^k)^{-1}c(a^ib^jc^k) &= c^{-k}b^{-j}a^{-i}ca^ib^jc^k \\ &= c^{-k}b^{-j}ca^ia^ib^jc^k \\ &= c^{-k}b^{-j}ca^{2i}b^jc^k \\ &= c^{-k}cb^{-j}a^{2i}b^jc^k \\ &= c^{-k+1}(b^{-j}a^{2i}b^j)^k \\ &= c^{-k}(ca^mc)c^{k-1} \\ &= c^{-k}a^{-m}c^{k-1} \\ &= c^{-k+1}a^mc^{k-2} \\ &= \vdots \\ &= c^{-k+(k-1)}a^{(-1)^k2ir^j}c^{k-k} \\ &= ca^{(-1)^k2ir^j}.\end{aligned}$$

By a similar argument as above, we have:

$$\begin{aligned}(a^ib^jc^k)^{-1}a^l(a^ib^jc^k) &= c^{-k}b^{-j}a^{-i}a^la^ib^jc^k \\ &= c^{-k}b^{-j}a^lb^jc^k \\ &= c^{-k}a^{r^jl}c^k \\ &= c^{-k+1}(c^{-1}a^{r^jl}c)c^{k-1} \\ &= c^{-k+1}(c^{-1}ac)^{r^jl}c^{k-1} \\ &= c^{-k+2}a^{-r^jl}c^{k-2} \\ &= \vdots \\ &= a^{(-1)^kr^jl}.\end{aligned}$$

We are now ready to compute the product of conjugacy classes in G. We first noticed that $(ca^i)(cb^ja^l) = a^{-i}ccb^ja^l = a^{-i}c^2b^ja^l = a^{-i}b^ja^l$

$= b^ja^{-ir^j}a^l = b^ja^{-ir^j+l}$. Thus, $c^G \cdot (cb^i)^G = \{c, ca, ca^2, \cdots, ca^{p-1}\} \cdot \{cb^i, cb^ia, cb^ia^2, \cdots, cb^ia^{p-1}\} = \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\} = (b^i)^G$. But $(ca^i)(ca^j) = (a^{-i}c)ca^j = a^{-i+j}$ and so $c^G \cdot c^G = \{c, ca, ca^2, \cdots, ca^{p-1}\} \cdot \{c, ca, ca^2, \cdots, ca^{p-1}\} = \{e, a, \cdots, a^{p-1}, a^{-1}, \cdots, a^{-(p-1)}\} = \bigcup_{i=0}^{\frac{p-1}{2q}} (a^i)^G$. Again, $(ca^i)(b^ja) = c(a^ib^j)a = c(b^ja^{lr^i})a = cb^ja^{lr^i}$ and so $c^G \cdot (b^i)^G = \{c, ca, ca^2, \cdots, ca^{p-1}\} \cdot \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\} = (cb^i)^G$.

Next, since $(cb^ia^j)(ca^l) = cb^i(a^jc)a^l = cb^ica^{-j}a^l = c^2b^ia^{l-j} = b^ia^{l-j}$,

$$(cb^i)^G \cdot c^G = \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\} = (b^i)^G.$$

To compute $(cb^i)^G \cdot (cb^j)^G$, we noticed that $(cb^ia^l)(cb^ja^m) = cb^i(ca^{-l})b^ja^m = c^2b^ia^{-l}b^ja^m = b^ia^{-l}b^ja^m = b^{i+j}a^{-lr^j+m}$. Thus, if $i + j \neq q$, then $(cb^i)^G \cdot (cb^j)^G = (b^{i+j})^G$. Otherwise, $(cb^i)^G.(cb^j)^G = \left(\cup_{1 \leq i \leq \frac{p-1}{2q}} (a_i)^G\right) \cup (b^q)^G$. A similar argument shows that when $i + j \neq q$, we have $(b^i)^G \cdot (b^j)^G = (b^{i+j})^G$, otherwise $(b^i)^G.(b^j)^G = \left(\cup_{1 \leq i \leq \frac{p-1}{2q}} (a_i)^G\right) \cup (b^q)^G$.

On the other hand, the equalities $(b^ia^j)(ca^l) = b^i(a^jc)a^l = b^i(ca^{-j})a^l = b^i(ca^{-j})a^l = b^i(ca^{-j})a^l = cb^ia^{-j+l}$ imply that:

$$\begin{aligned}(b^i)^G \cdot c^G &= \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\} \cdot \{c, ca, ca^2, \cdots, ca^{p-1}\} \\ &= \{cb^i, cb^ia, cb^ia^2, \cdots, cb^ia^{p-1}\} = (cb^i)^G.\end{aligned}$$

Other calculations were similar and were recorded as follows:

i. $c^G \cdot (a^i)^G = \{c, ca, ca^2, \cdots, ca^{p-1}\} = c^G$,
ii. $(b^i)^G \cdot (cb^j)^G = \{cb^{i+j}, cb^{i+j}a, cb^{i+j}a^2, \cdots, cb^{i+j}a^{p-1}\} = (cb^{i+j})^G$,
iii. $(b^i)^G \cdot (a^j)^G = \{b^i, b^ia, b^ia^2, \cdots, b^ia^{p-1}\} = (b^i)^G$,
iv. $(a^i)^G \cdot (b^j)^G = \{b^j, b^ja, b^ja^2, \cdots, b^ja^{p-1}\} = (b^j)^G$,
v. $(a^i)^G \cdot (cb^j)^G = \{cb^i, cb^ia, cb^ia^2, \cdots, cb^ia^{p-1}\} = (cb^j)^G$.

Again, we were unable to compute $\eta((a_i)^G \cdot (a_i)^G)$, in general. Our calculations given above and computing by the small group library of GAP [11] show that $\{1, \frac{p+2q-1}{2q}\} \subset \eta(G)$.

Question 3.1. What is $\eta(S_{p,q})$?

Using a simple calculation, one can see that $\eta(U_{6n}) = \{1, 2\}$, $\eta(D_{10}) = \{1, 2, 3\}$, $\eta(V_{48}) = \{1, 2, 3, 4\}$, $\eta(SL(2, 3) \ltimes Z_4) = \{1, 2, 3, 4, 5\}$, and $\eta((Z_3 \times ((Z_4 \times Z_2) \ltimes Z_2)) \ltimes Z_2) = \{1, 2, 3, 4, 5, 6\}$. In the small group library notation of GAP [11], $SL(2, 3) \ltimes Z_4 = SmallGroup(96, 66)$ and $(Z_3 \times ((Z_4 \times Z_2) \ltimes Z_2) = SmallGroup(96, 13)$. Thus, it is natural to ask the following question:

Question 3.2. Is there a group G, such that $\eta(G) = \{1, 2, \cdots, n\}$, where $n \geq 7$. For which values of n, we can find a group G, such that $\eta(G) = \{1, 2, \cdots, n\}$?

Acknowledgment

We are indebted to the referee for his/her suggestions and helpful remarks. The research works of the authors were partially supported by the University of Kashan, under the grant No of 364988/77.

References

1. E. Adan−Bante, Derived length and products of conjugacy classes, *Israel J. Math.* **168** (2008) 93–100.
2. E. Adan−Bante, On nilpotent groups and conjugacy classes, *Houston J. Math.* **36** (2) (2010) 345–356.
3. E. Adan−Bante and J. M. Harris, On conjugacy classes of $SL(2, q)$, *Rev. Colombiana Mat.* **46** (2012) (2) 97–111.
4. Z. Arad, D. Chillag and G. Moran, Groups with a small covering number, In: Products of Conjugacy Classes in Groups, Lecture Notes in Math. 1112, Berlin, Springer−Verlag, pp. 222–244, 1985.
5. Z. Arad and E. Fisman, An analogy between products of two conjugacy classes and products of two irreducible characters in finite groups, *Proc. Edin. Math. Soc.* **30** (1987) 7–22.
6. M. R. Darafsheh and S. Mahmood Robati, Products of conjugacy classes and products of irreducible characters in finite groups, *Turkish J. Math.* **37** (2013) (4) 607–616.
7. M. R. Darafsheh and N. S. Poursalavati, On the existence of the orthogonal basis of the symmetry classes of tensors associated with certain groups, *SUT J. Math.* **37** (1) (2001) 1–17.
8. M. Hormozi and K. Rodtes, Symmetry classes of tensors associated with the semi−dihedral groups SD_{8n}, *Colloq. Math.* **131** (2013) (1) 59–67.
9. I. M. Isaacs, Character Theory of Finite Groups, Academic Press, New York, 1976.
10. G. James and M. Liebeck, Representations and Characters of Groups, Cambridge Univ. Press, London−New York, 1993.
11. The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.7.5; 2014.
12. C. Zhang, J. -X. Zhou and Y. -Q. Feng, Automoprphisms of cubic Cayley graphs of order $2pq$, *Discrete Math.* **309** (2009) 2687–2695.

Maryam Jalali

Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, P.O.Box 87317-51167, Kashan, I. R. Iran

Ali Reza Ashrafi

Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, P.O.Box 87317-51167, Kashan, I. R. Iran

Email: ashrafi@kashanu.ac.ir

Journal of Algebraic Systems

COMPUTING THE PRODUCTS OF CONJUGACY CLASSES FOR SPECIFIC FINITE GROUPS

MARYAM JALALI-RAD AND ALI REZA ASHRAFI

محاسبه حاصل‌ضرب کلاس‌های تزویج برخی گروه‌های متناهی

مریم جلالی راد و علی‌رضا اشرفی
کاشان – دانشگاه کاشان – دانشکده علوم ریاضی–گروه ریاضی محض

فرض کنید G یک گروه متناهی و A و B دو کلاس تزویج از آن باشند. در این‌صورت تعداد کلاس‌های تزویج مشمول در AB را با $\eta(AB)$ و مجموعه $\eta(AB)$هایی که A و B روی کلاس‌های تزویج G تغییر می‌کنند را با $\eta(G)$ نشان می‌دهیم. هدف این مقاله محاسبه $\eta(G)$هایی است که در آن G گروهی غیر قابل تجزیه از مرتبه $۲pq$، p و q اعدادی اول هستند، گروهی از مرتبه $p^۳$، گروهی از مرتبه $۴p$ یا G یکی از گروه‌های زیر است:

$$D_{۲n}, T_{۴n}, U_{۶n}, V_{۸n}, SD_{۸n}.$$

کلمات کلیدی: کلاس تزویج، زیرمجموعه $G-$ پایا، $p-$گروه.