Revista Colombiana de Matemáticas
Volumen 46(2012)2, páginas 97-111

On Conjugacy Classes of $\mathrm{SL}(2, q)$

Sobre las clases conjugadas de $\mathrm{SL}(2, q)$

Edith Adan-Bante[1,✉], John M. Harris[2]

[1]University of Saint Thomas, Minnesota, USA

[2]University of Southern Mississippi, Mississippi, USA

Abstract. Let $\mathrm{SL}(2, q)$ be the group of 2×2 matrices with determinant one over a finite field $\mathcal{F}$ of size q. We prove that if q is even, then the product of any two noncentral conjugacy classes of $\mathrm{SL}(2, q)$ is the union of at least $q - 1$ distinct conjugacy classes of $\mathrm{SL}(2, q)$. On the other hand, if $q > 3$ is odd, then the product of any two noncentral conjugacy classes of $\mathrm{SL}(2, q)$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes of $\mathrm{SL}(2, q)$.

Key words and phrases. Conjugacy classes, Matrices over a finite field, Products of conjugacy classes, Special linear group.

2010 Mathematics Subject Classification. 15A33, 20E45, 20G40.

Resumen. Sea $\mathrm{SL}(2, q)$ el grupo de las matrices 2×2 con determinante uno sobre un campo finito $\mathcal{F}$ de tamaño q. Se prueba que si q es par, entonces el producto de cualesquiera dos clases conjugadas no centrales de $\mathrm{SL}(2, q)$ es la unión de al menos $q - 1$ distintas clases conjugadas de $\mathrm{SL}(2, q)$. Por otro lado, si $q > 3$ es impar, entonces el producto de cualesquiera dos clases conjugadas no centrales de $\mathrm{SL}(2, q)$ es la unión de al menos $\frac{q+3}{2}$ distintas clases conjugadas de $\mathrm{SL}(2, q)$.

Palabras y frases clave. Clases conjugadas, matrices sobre un campo finito, producto de clases conjugadas, grupo especial lineal.

1. Introduction

Let $\mathcal{G}$ be a finite group, $A \in \mathcal{G}$ and $A^{\mathcal{G}} = \{A^B : B \in \mathcal{G}\}$ be the conjugacy class of A in $\mathcal{G}$. Let $\mathcal{X}$ be a $\mathcal{G}$-invariant subset of $\mathcal{G}$, i.e. $\mathcal{X}^A = \{B^A : B \in \mathcal{X}\} = \mathcal{X}$ for all $A \in \mathcal{G}$. Then $\mathcal{X}$ can be expressed as a union of n distinct conjugacy classes of $\mathcal{G}$, for some integer $n > 0$. Set $\eta(\mathcal{X}) = n$.

Given any conjugacy classes $A^{\mathcal{G}}$, $B^{\mathcal{G}}$ in $\mathcal{G}$, we can check that the product $A^{\mathcal{G}}B^{\mathcal{G}} = \{XY : X \in A^{\mathcal{G}}, Y \in B^{\mathcal{G}}\}$ is a $\mathcal{G}$-invariant subset and thus $A^{\mathcal{G}}B^{\mathcal{G}}$ is the union of $\eta(A^{\mathcal{G}}B^{\mathcal{G}})$ distinct conjugacy classes of $\mathcal{G}$.

It is proved in [2] that for any integer $n > 5$, given any nontrivial conjugacy classes α^{S_n} and β^{S_n} of the symmetric group S_n of n letters, that is $\alpha, \beta \in S_n \setminus \{e\}$, if n is a multiple of two or of three, the product $\alpha^{S_n}\beta^{S_n}$ is the union of at least two distinct conjugacy classes, i.e. $\eta(\alpha^{S_n}\beta^{S_n}) \geq 2$, otherwise the product $\alpha^{S_n}\beta^{S_n}$ is the union of at least three distinct conjugacy classes, i.e. $\eta(\alpha^{S_n}\beta^{S_n}) \geq 3$. A similar result is proved for the alternating group A_n in [1].

Fix a prime p and an integer $m > 0$. Let $\mathcal{F} = \mathcal{F}(q)$ be a field with $q = p^m$ elements and $\mathcal{S} = \mathrm{SL}(2, q) = \mathrm{SL}(2, \mathcal{F})$ be the special linear group, i.e. the group of 2×2 invertible matrices over $\mathcal{F}$ with determinant 1. Given any non-central conjugacy classes $A^{\mathcal{S}}$, $B^{\mathcal{S}}$ in $\mathcal{S}$, is there any relationship between $\eta(A^{\mathcal{S}}B^{\mathcal{S}})$ and q?

Arad and Herzog conjectured in [3] that the product of two nontrivial conjugacy classes is never a conjugacy class in a finite nonabelian simple group. Thus, when $q \geq 4$ is even we have that $\mathcal{S} = \mathrm{SL}(2, q) = \mathrm{PSL}(2, q)$ is simple and so we must have that $\eta(A^{\mathcal{S}}B^{\mathcal{S}}) > 1$ unless $A = I$ or $B = I$. In what follows, we expand and refine this statement.

Theorem 1. *Fix a positive integer m. Let A and B be matrices in $\mathcal{S} = \mathrm{SL}(2, 2^m)$. Then exactly one of the following holds:*

(i) *$A^{\mathcal{S}}B^{\mathcal{S}} = (AB)^{\mathcal{S}}$ and at least one of A, B is a scalar matrix.*

(ii) *$A^{\mathcal{S}}B^{\mathcal{S}}$ is the union of at least $2^m - 1$ distinct conjugacy classes, i.e. $\eta(A^{\mathcal{S}}B^{\mathcal{S}}) \geq 2^m - 1$.*

Theorem 2. *Fix an odd prime p and an integer $m > 0$ such that $q = p^m > 3$. Let A and B be matrices in $\mathcal{S} = \mathrm{SL}(2, q)$. Then exactly one of the following holds:*

(i) *$A^{\mathcal{S}}B^{\mathcal{S}} = (AB)^{\mathcal{S}}$ and at least one of A, B is a scalar matrix.*

(ii) *$A^{\mathcal{S}}B^{\mathcal{S}}$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes, i.e. $\eta(A^{\mathcal{S}}B^{\mathcal{S}}) \geq \frac{q+3}{2}$.*

Given any group G, denote by $\min(G)$ the smallest integer in the set $\{\eta(a^G b^G) : a, b \in G \setminus \mathbf{Z}(G)\}$. In Proposition 12, given any integer $m > 0$, we present matrices A, B in $\mathrm{SL}(2, 2^m)$ such that $\eta(A^{\mathrm{SL}(2,2^m)}B^{\mathrm{SL}(2,2^m)}) = 2^m - 1$ and thus Theorem 1 is optimal. Also, given any $q = p^m > 3$, where p is an odd prime and m is a positive integer, in Proposition 18 we prove that Theorem 1 is optimal by presenting matrices where $\min(\mathrm{SL}(2, q))$ is attained. Also, using GAP [5], we can check that $\min(\mathrm{SL}(2, 3)) = 2$ and thus Theorem 2 cannot apply when $q = 3$.

When q is even, $\mathrm{SL}(2,q)=\mathrm{PSL}(2,q)$ is a simple group of Lie type of characteristic two. Hence, if we require that both A and B are not involutions in Theorem 1, the conclusion of Theorem 1 follows from Theorem 2 of [4]. We thank Rod Gow for pointing this out to us.

2. Proofs

Notation. We will denote with uppercase letters the matrices and with lowercase letters the elements in $\mathcal{F}$.

***Remark* 3.** We can describe matrix representatives of conjugacy classes in $\mathcal{S}=\mathrm{SL}(2,\mathcal{F})$ by four families or types ([6]):

(i) $\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$, where $r\in\mathcal{F}$ and $r^2=1$.

(ii) $\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}$, where $r,s\in\mathcal{F}$ and $rs=1$.

(iii) $\begin{bmatrix} s & u \\ 0 & s \end{bmatrix}$, where $s\in\mathcal{F}$, $s^2=1$ and u is either 1 or a non-square element of $\mathcal{F}$, i.e. $u\in\mathcal{F}\setminus\left\{x^2 : x\in\mathcal{F}\right\}$.

(iv) $\begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}$, where $w=r+r^q$ and $1=r^{1+q}$ for some $r\in\mathcal{E}\setminus\mathcal{F}$, where $\mathcal{E}$ is a quadratic extension of $\mathcal{F}$.

That is, any conjugacy class $A^{\mathcal{S}}$ of $\mathcal{S}$ must contain one of the above matrices.

***Remark* 4.** By Lemma 3 of [2], we have that $A^{\mathcal{S}}B^{\mathcal{S}}=B^{\mathcal{S}}A^{\mathcal{S}}$. Thus if we want to prove that given any non-central conjugacy classes $A^{\mathcal{S}}$ and $B^{\mathcal{S}}$ of $\mathcal{S}$, $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big)\geq n$ for some integer n, it suffices to prove that the statement holds for each of the six combinations of conjugacy classes containing matrices of type (ii), (iii) and (iv).

***Remark* 5.** Two matrices in the same conjugacy class have the same trace. Thus, if the matrices do not have the same trace, then they belong to distinct conjugacy classes.

Lemma 6. *Let* $C=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in\mathcal{S}$ *and* $A=\begin{bmatrix} e & f \\ g & h \end{bmatrix}\in\mathcal{S}$. *Then*

$$A^C=C^{-1}AC=\begin{bmatrix} a(de-bg)+c(df-bh) & b(de-bg)+d(df-bh) \\ a(-ce+ag)+c(-cf+ah) & b(-ce+ag)+d(-cf+ah) \end{bmatrix},$$

and therefore

(i)

$$\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}^C = \begin{bmatrix} adr - bcs & bd(r-s) \\ -ac(r-s) & ads - bcr \end{bmatrix},$$

(ii)

$$\begin{bmatrix} s & u \\ 0 & s \end{bmatrix}^C = \begin{bmatrix} s + ucd & ud^2 \\ -uc^2 & s - ucd \end{bmatrix},$$

(iii)

$$\begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}^C = \begin{bmatrix} ab + c(d - bw) & b^2 + d^2 - bdw \\ -a^2 - c^2 + acw & -ab + d(-c + aw) \end{bmatrix}.$$

Proof. Observe that $C^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ Hence

$$\begin{aligned} C^{-1}AC &= \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} de - bg & df - bh \\ -ce + ag & -cf + ah \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} a(de - bg) + c(df - bh) & b(de - bg) + d(df - bh) \\ a(-ce + ag) + c(-cf + ah) & b(-ce + ag) + d(-cf + ah) \end{bmatrix}. \end{aligned}$$ ☑

Lemma 7. *Let* $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{S}$. *Then*

(i) $\text{Trace}\left(\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}^C \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix} \right) = ad(r-s)(u-v) + (us + vr).$

(ii) $\text{Trace}\left(\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}^C \begin{bmatrix} t & u \\ 0 & t \end{bmatrix} \right) = t(r+s) - ac(r-s)u.$

(iii) $\text{Trace}\left(\begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}^C \begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix} \right) = (ac + bd)(s - r) + w(ads - bcr).$

(iv) $\text{Trace}\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^C \begin{bmatrix} t & w \\ 0 & t \end{bmatrix} \right) = 2rt - uwc^2.$

(v) $\text{Trace}\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^C \begin{bmatrix} 0 & 1 \\ -1 & s \end{bmatrix} \right) = -ud^2 - uc^2 + s(r - ucd).$

(vi) $$\operatorname{Trace}\left(\begin{bmatrix}0 & 1\\ -1 & w\end{bmatrix}^C \begin{bmatrix}0 & 1\\ -1 & v\end{bmatrix}\right) = -a^2 - b^2 - c^2 - d^2 + bdw + acw + v\big(-ab + d(-c + aw)\big).$$

Proof. The result follows by Lemma 6 and 6(i)

(i) $$\begin{aligned}\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^C \begin{bmatrix}u & 0\\ 0 & v\end{bmatrix}\right) &= \operatorname{Trace}\left(\begin{bmatrix}adr - bcs & bd(r-s)\\ -ac(r-s) & ads - bcr\end{bmatrix}\begin{bmatrix}u & 0\\ 0 & v\end{bmatrix}\right)\\ &= u(adr - bcs) + v(ads - bcr)\\ &= ad(ur + vs) - bc(us + vr)\\ &= ad(ur + vs) + (1 - ad)(us + vr)\\ &= ad(ur + vs - us - vr) + (us + vr)\\ &= ad\big(u(r-s) - v(r-s)\big) + (us + vr)\\ &= ad(u - v)(r - s) + (us + vr).\end{aligned}$$

(ii) $$\begin{aligned}\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^C \begin{bmatrix}t & u\\ 0 & t\end{bmatrix}\right) &= \operatorname{Trace}\left(\begin{bmatrix}adr - bcs & bd(r-s)\\ -ac(r-s) & ads - bcr\end{bmatrix}\begin{bmatrix}t & u\\ 0 & t\end{bmatrix}\right)\\ &= t(adr - bcs) - ac(r-s)u + t(ads - bcr)\\ &= ad(rt + st) - bc(st + rt) - ac(r-s)u\\ &= (ad - bc)t(r + s) - ac(r - s)\\ &= t(r - s) - ac(r - s)u.\end{aligned}$$

(iii) $$\begin{aligned}&\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^C \begin{bmatrix}0 & 1\\ -1 & w\end{bmatrix}\right)\\ &= \operatorname{Trace}\left(\begin{bmatrix}adr - bcs & bd(r-s)\\ -ac(r-s) & ads - bcr\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & w\end{bmatrix}\right)\\ &= -bd(r-s) - ac(r-s) + w(ads - bcr)\\ &= (ac + bd)(s - r) + w(ads - bcr).\end{aligned}$$

(iv) $$\begin{aligned}\operatorname{Trace}\left(\begin{bmatrix}r & u\\ 0 & r\end{bmatrix}^C \begin{bmatrix}t & w\\ 0 & t\end{bmatrix}\right) &= \operatorname{Trace}\left(\begin{bmatrix}r + ucd & ud^2\\ -uc^2 & r - ucd\end{bmatrix}\begin{bmatrix}t & w\\ 0 & t\end{bmatrix}\right)\\ &= t(r + ucd) + w\big(-uc^2\big) + t(r - ucd)\\ &= 2rt - uwc^2.\end{aligned}$$

(v) $$\begin{aligned}\operatorname{Trace}\left(\begin{bmatrix}r & u\\ 0 & r\end{bmatrix}^C \begin{bmatrix}0 & 1\\ -1 & s\end{bmatrix}\right) &= \operatorname{Trace}\left(\begin{bmatrix}r + ucd & ud^2\\ -uc^2 & r - ucd\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & s\end{bmatrix}\right)\\ &= -ud^2 - uc^2 + s(r - ucd).\end{aligned}$$

(vi)
$$\begin{aligned}
&\operatorname{Trace}\left(\begin{bmatrix}0 & 1\\ -1 & w\end{bmatrix}^{C}\begin{bmatrix}0 & 1\\ -1 & v\end{bmatrix}\right)\\
&\quad= \operatorname{Trace}\left(\begin{bmatrix}ab+c(d-bw) & b^2+d^2-bdw\\ -a^2-c^2+acw & -ab+d(-c+aw)\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & v\end{bmatrix}\right)\\
&\quad= -b^2-d^2+bdw-a^2-c^2+acw+v\big(-ab+d(-c+aw)\big)
\end{aligned}$$ ☑

***Remark* 8.** For any $a, b \in \mathcal{F}$ such that $a \neq 0$, we have that $\{ax+b : x \in \mathcal{F}\} = \mathcal{F}$.

Lemma 9. *Let $A = \begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}$ where $r \neq s$, and B be any non-central matrix in $\mathcal{S}$, i.e. of type (ii), (iii) or (iv) in Remark 3. Given any $f \in \mathcal{F}$, there exists a matrix D in the product $A^{\mathcal{S}}B^{\mathcal{S}}$ such that* $\operatorname{Trace}(D) = f$. *In particular, $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) \geq q$ for any non-central matrix B.*

***Proof*.** Given $i \in \mathcal{F}$, set $C(i) = \begin{bmatrix}i & i-1\\ 1 & 1\end{bmatrix}$. Observe that $C(i) \in \mathcal{S}$ for all $i \in \mathcal{F}$. Fix u, v in $\mathcal{F}$ such that $uv = 1$. By Lemma 7(i), we have that

$$\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^{C(i)}\begin{bmatrix}u & 0\\ 0 & v\end{bmatrix}\right) = (r-s)(u-v)i + (us+vr). \tag{1}$$

By Lemma 7(ii) we have that

$$\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^{C(i)}\begin{bmatrix}t & u\\ 0 & t\end{bmatrix}\right) = -(r-s)ui + t(r+s). \tag{2}$$

Now let $E(i) = \begin{bmatrix}1 & i\\ 0 & 1\end{bmatrix}$ for $i \in \mathcal{F}$. As before, observe that $E(i) \in \mathcal{S}$ for any $i \in \mathcal{F}$. Then by Lemma 7(iii), we have that

$$\operatorname{Trace}\left(\begin{bmatrix}r & 0\\ 0 & s\end{bmatrix}^{E(i)}\begin{bmatrix}0 & 1\\ -1 & w\end{bmatrix}\right) = (s-r)i + ws. \tag{3}$$

Since $(r-s)(u-v) \neq 0$, $(r-s)u \neq 0$, and $s-r \neq 0$, the result follows from (1), (2),(3), Remark 3, Remark 5 and Remark 8. ☑

Lemma 10. *Let $\mathcal{F}$ be a field with 2^m elements for some integer m and $a \in \mathcal{F}$ with $a \neq 0$. Given any $\mathcal{H} \subseteq \mathcal{F}$, the set $\{ai^2 + c : i \in \mathcal{H}\}$ has $|H|$ elements. In particular, if $\mathcal{H} = \mathcal{F}$, then the set $\{ai^2 + c : i \in \mathcal{H}\}$ has q elements.*

Proof. Observe that

$$\left|\{ai^2+c : i\in\mathcal{H}\}\right| = \left|\{ai^2 : i\in\mathcal{H}\}\right| = \left|\{i^2 : i\in\mathcal{H}\}\right|.$$

Since $\mathcal{F}$ is a field of characteristic two, the map $x\mapsto x^2$ is an automorphism of $\mathcal{F}$ and thus $\left|\{i^2 : i\in\mathcal{H}\}\right| = \left|\mathcal{H}\right|$. ☑

Lemma 11. *Let $\mathcal{F}$ be a field with $q=2^m$ elements for some integer m.*

(i) For any f in $\mathcal{F}$, there exists a matrix D in the product $\begin{bmatrix}1&1\\0&1\end{bmatrix}^{\mathcal{S}}\begin{bmatrix}1&1\\0&1\end{bmatrix}^{\mathcal{S}}$ such that $\operatorname{Trace}(D)=f$.

(ii) For any f in $\{i^2+w : i\in\mathcal{F}\smallsetminus\{0\}\}$, there exists a matrix D in the product $\begin{bmatrix}1&1\\0&1\end{bmatrix}^{\mathcal{S}}\begin{bmatrix}0&1\\-1&w\end{bmatrix}^{\mathcal{S}}$ such that $\operatorname{Trace}(D)=f$.

(iii) Given any $f\in\mathcal{F}$, there exists a matrix D in the product $\begin{bmatrix}0&1\\-1&w\end{bmatrix}^{\mathcal{S}}\begin{bmatrix}0&1\\-1&v\end{bmatrix}^{\mathcal{S}}$, where $vw\neq 0$, such that $\operatorname{Trace}(D)=f$.

Thus given any conjugacy classes $A^{\mathcal{S}}, B^{\mathcal{S}}$ in $\mathcal{S}$, where A, B is either of type (iii) or (iv) in Remark 3, the product $A^{\mathcal{S}}B^{\mathcal{S}}$ is the union of at least $q-1$ distinct conjugacy classes.

Proof.

(i) Given any $i\in\mathcal{F}$, set $C(i)=\begin{bmatrix}1&0\\i&1\end{bmatrix}$. Observe that $C(i)$ is in $\mathcal{S}$. By Lemma 7(iv)

$$\operatorname{Trace}\left(\begin{bmatrix}1&1\\0&1\end{bmatrix}^{C(i)}\begin{bmatrix}1&1\\0&1\end{bmatrix}\right)=i^2.$$

By Lemma 10 we have that $\{i^2 : i\in\mathcal{F}\}=\mathcal{F}$ and thus (i) follows.

(ii) Given any $i\in\mathcal{F}\smallsetminus\{0\}$, set $E(i)=\begin{bmatrix}i^{-1}&0\\0&i\end{bmatrix}$. By Lemma 7(v), we have

$$\operatorname{Trace}\left(\begin{bmatrix}1&1\\0&1\end{bmatrix}^{E(i)}\begin{bmatrix}0&1\\-1&w\end{bmatrix}\right)=i^2+w.$$

(iii) For $i \in \mathcal{F}$, set $F(i) = \begin{bmatrix} i+1 & i \\ i & i+1 \end{bmatrix}$. Observe that since $\mathcal{F}$ is of characteristic two, we have $\det\big(F(i)\big) = (i+1)^2 - i^2 = i^2 + 1 - i^2 = 1$ and thus $F(i) \in \mathcal{S}$. By Lemma 7(vi) we have

$$\operatorname{Trace}\left(\begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}^{F(i)} \begin{bmatrix} 0 & 1 \\ -1 & v \end{bmatrix} \right) = vw(i^2+1).$$

If $vw \neq 0$, then the set $\big\{vw(i^2+1) : i \in \mathcal{F}\big\} = \mathcal{F}$ by Lemma 10.

Since $\mathcal{F}$ is of characteristic two, the only matrix representative of type (iii) is $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Also, since $\mathcal{F}$ is of characteristic two, we can check that the matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ are in the same conjugacy class. If we take w in (ii) and v in (iii) as in Remark 5(iv), with cases (i), (ii), and (iii), we cover all possible combinations of representatives of type (iii) and (iv), and by Remark 3, the proof of the result is complete. ☑

Proof of Theorem 1. If at least one of A or B is in the center, i.e. A or B are of type (i) in Remark 3, then $A^{\mathcal{S}}B^{\mathcal{S}} = (AB)^{\mathcal{S}}$. Theorem 1 then follows from Remark 4, Lemma 9 and Lemma 11. ☑

Proposition 12. *Fix $q = 2^m$ for some integer $m > 0$ and let $\mathcal{F}$ be a field with q elements. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}$ in $\mathcal{S}$, where $x^2 - wx + 1$ is an irreducible polynomial over $\mathcal{F}$. Then $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) = q - 1$.*

Hence, Theorem 1 is optimal.

Proof. Set $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\mathcal{S}$. By Lemma 7(iv), we have that $\operatorname{Trace}\big(A^C B\big) = -d^2 - c^2 + w(1 - cd)$. Suppose that $-d^2 - c^2 + w(1-cd) = w$, that is, $d^2 + c^2 + wcd = 0$. Since C is invertible, at least one of c and d are nonzero, and so both must be nonzero. Thus,

$$x^2 - wx + 1 = x^2 + \frac{c^2+d^2}{cd}x + 1 = \Big(x + \frac{c}{d}\Big)\Big(x + \frac{d}{c}\Big),$$

a contradiction. Hence, the matrices in $A^{\mathcal{S}}B^{\mathcal{S}}$ do not have trace w. Also, since the eigenvalues of B are not in $\mathcal{F}$ and the eigenvalues of A is 1, then $A^{\mathcal{S}} \neq \big(B^{-1}\big)^{\mathcal{S}}$ and so the identity I is not in $A^{\mathcal{S}}B^{\mathcal{S}}$.

Since $\mathcal{F}$ has even characteristic and I is not in $A^{\mathcal{S}}B^{\mathcal{S}}$, we conclude that there is a one-to-one correspondence of the conjugacy classes in $A^{\mathcal{S}}B^{\mathcal{S}}$ with the traces of the matrices: if the trace is 0, then the matrix is similar to a matrix of type (iii), and otherwise, the matrix is similar to a matrix of type (ii) or type (iv), depending on whether or not its characteristic equation is reducible. Thus $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) = q - 1$. ☑

Lemma 13. *Let u, v in $\mathcal{F}$. Then the matrices $\begin{bmatrix} s & v \\ 0 & s \end{bmatrix}$ and $\begin{bmatrix} s & u \\ 0 & s \end{bmatrix}$ are similar if and only if $v = ud^2$ for some d in $\mathcal{F} \setminus \{0\}$. In particular, if u is a non-square, then the matrices $\begin{bmatrix} s & 1 \\ 0 & s \end{bmatrix}$ and $\begin{bmatrix} s & u \\ 0 & s \end{bmatrix}$ are not similar, i.e. they belong to distinct conjugacy classes.*

Proof. Let $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{S}$. By Lemma 6(ii), we have that $\begin{bmatrix} s & u \\ 0 & s \end{bmatrix}^C = \begin{bmatrix} s + ucd & ud^2 \\ -uc^2 & s - ucd \end{bmatrix}$. Thus, if $\begin{bmatrix} s + ucd & ud^2 \\ -uc^2 & s - ucd \end{bmatrix} = \begin{bmatrix} t & v \\ 0 & t \end{bmatrix}$, then either $c = 0$ and $v = ud^2$, so the result follows, or $u = v = 0$, and in this case the result is trivially true. ☑

Lemma 14. *Let $\mathcal{F}$ be a finite field with q elements and $a, b, c \in \mathcal{F}$ with $a \neq 0$. If q is an odd number, then the set $\big\{ai^2 + bi + c : i \in \mathcal{F}\big\}$ has exactly $\frac{q+1}{2}$ elements.*

Proof. Since the field $\mathcal{F}$ is of odd characteristic, we have that $2 \neq 0$ and thus

$$\begin{aligned} \big|\big\{ai^2 + bi + c : i \in \mathcal{F}\big\}\big| &= \left|\left\{i^2 + \frac{b}{a}i + \frac{c^2}{a} : \mathcal{F}\right\}\right| \\ &= \left|\left\{i^2 + \frac{b}{a}i + \left(\frac{b}{2a}\right)^2 : \mathcal{F}\right\}\right| \\ &= \left|\left\{\left(i + \frac{b}{2a}\right)^2 : i \in \mathcal{F}\right\}\right| = \big|\big\{i^2 : i \in \mathcal{F}\big\}\big|. \end{aligned}$$

Since q is odd, then 2 divides $q - 1$ and so the square of the set of units forms a subgroup of order $\frac{q-1}{2}$. Since $0^2 = 0$, we have that the set $\big\{ai^2 + bi + c : i \in \mathcal{F}\big\}$ has exactly $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ elements. ☑

Lemma 15. *Let $\mathcal{F}$ be a finite field of size q, where q is odd.*

(i) Fix $a, b \in \mathcal{F} \setminus \{0\}$, and suppose that $q > 3$. Then the set

$$\big\{ax^2 + by^2 : x, y \in \mathcal{F} \setminus \{0\}\big\}$$

has a square and a non-square element.

(ii) Fix r, s and u in $\mathcal{F}$ with $s^2-4\neq 0$. Then the set

$$\big\{-ux^2-uy^2+s(r-uxy) : x,y\in\mathcal{F}, (x,y)\neq(0,0)\big\}$$

has at least $q-1$ elements.

(iii) Let $w\in\mathcal{F}$ be such that w^2-4 is not a square. Then

$$\big\{a^2-c^2+acw : a,c\in\mathcal{F}, a\neq 0\big\}=\mathcal{F}\setminus\{0\}.$$

Proof.

(i) Observe that if $c\in\mathcal{F}$ is a non-square element, i.e. $c\notin\big\{i^2 : i\in\mathcal{F}\big\}$, then $\mathcal{F}=\big\{i^2 : i\in\mathcal{F}\big\}\cup\big\{ci^2 : i\in\mathcal{F}\big\}$. Thus, if x is a square and y is a non-square element, then ax is a square and ay is a non-square element when a is a square, and otherwise, ax is a non-square element and ay is a square. Thus the set $\big\{ax^2+by^2 : x,y\in\mathcal{F}\setminus\{0\}\big\}$ has a square and a non-square element if and only if $\big\{x^2+\frac{b}{a}y^2 : x,y\in\mathcal{F}\setminus\{0\}\big\}$ has a square and a non-square element. Hence, without loss of generality, we may assume that $a=1$.

Note that there are $\frac{q+1}{2}$ square elements in $\mathcal{F}$ and $\frac{q-1}{2}$ non-square elements in $\mathcal{F}$. Also, since $|\mathcal{F}|>3$, if $\mathcal{F}$ has characteristic $p\neq 3$ then $3^2+4^2=5^2$, otherwise there exists an element $w\in\mathcal{F}$ such that $w^2+1=0$. Thus the set $\big\{x^2+y^2 : x,y\in\mathcal{F}\big\}$ always contains a square element. If b is a square element, the set $\big\{x^2+by^2 : x,y\in\mathcal{F}\setminus\{0\}\big\}=\big\{x^2+y^2 : x,y\in\mathcal{F}\big\}$ has a square and a non-square element; otherwise the set of square elements would be a subfield of size $\frac{q+1}{2}$ of the field of size q, but $\frac{q+1}{2}$ does not divide q.

Suppose that b is a non-square element. If -1 is a non-square element, then $\big\{x^2+by^2 : x,y\in F\setminus\{0\}\big\}=\big\{x^2-y^2 : x,y\in F\setminus\{0\}\big\}$, and hence we may assume that $b=-1$. Let ϵ be a generator of $\mathcal{F}$. Observe that ϵ is not a square and if $x=\frac{\epsilon+1}{2}=1+y$, then $x^2-y^2=(x-y)(x+y)=\epsilon$ and $x,y\in\mathcal{F}\setminus\{0\}$ since $|\mathcal{F}|>3$. Also for any $x=y\neq 0$, we have that $x^2-y^2=0$ and thus the set $\big\{x^2-y^2 : x,y\in\mathcal{F}\setminus\{0\}\big\}$ contains a square, namely zero, and a non-square element, namely ϵ. We may assume then that -1 is a square element.

Given $z\in\mathcal{F}\setminus\{0\}$, set $y=xz$. Then $x^2+by^2=x^2(1+bz^2)$. Observe that $1+bz^2=0$ does not have a solution since -1 is square and so $-1/z^2$ is a square. Since the set $Z=\big\{1+bz^2 : z\in\mathcal{F}\setminus 0\big\}$ has $\frac{q-1}{2}$ elements and $0,1\notin Z$, either Z has a square and a non-square element, or it has only non-square elements. In the first case, since $\big\{x^2(1+bz^2) : x,z\in\mathcal{F}\setminus\{0\}\big\}\subset\big\{x^2+by^2 : x,y\in\mathcal{F}\big\}$, the result follows. We may assume now that Z is the set of non-square elements. Given $w\in\mathcal{F}\setminus\{0\}$, set $x=wy$. Then $x^2+by^2=y^2(w^2+b)$. Hence $W=\big\{w^2+b : w\in\mathcal{F}\setminus 0\big\}$

has $\frac{q-1}{2}$ elements and $b, -b \notin W$. Since both b and $-b$ are non-squares, it follows that either W contains both square and non-square elements, or W contains only square elements. In the first case, the result follows as before. In the second case, since $\{x^2(1+bz^2) : x, z \in \mathcal{F} \setminus \{0\}\}$ is the set of all non-square elements and $\{y^2(w^2+b) : y, w \in \mathcal{F} \setminus \{0\}\}$ is the set of all nonzero square elements, (i) follows.

(ii) Observe that $-ux^2 - uy^2 + s(r - uxy) = f$ if and only if

$$x^2 + y^2 - sxy + \frac{f - sr}{u} = 0 \tag{4}$$

for some (x, y). Observe that (4) has a solution if there is some $y \in \mathcal{F}$ such that the discriminant $\Delta(y) = (sy)^2 - 4\big(y^2 + \frac{f-sr}{u}\big) = (s^2-4)y^2 + \frac{4(f-sr)}{u}$ is a square. Since $s^2 - 4 \neq 0$, by Lemma 14 we have that the set $\big\{(s^2-4)y^2 + \frac{4(f-sr)}{u} : y \in \mathcal{F}\big\}$ has at least $\frac{q+1}{2}$ elements. Since there are $\frac{q+1}{2}$ squares, for some y we must have that $\Delta(y)$ is a square. It follows then that $x = \frac{sy \pm \sqrt{\Delta(y)}}{2}$ is a solution for (4). Observe that $(x, y) = (0, 0)$ is a solution for the Equation 4 if and only if $f - sr = 0$. We conclude that for at least $q - 1$ elements of $\mathcal{F}$, (4) has a solution (x, y) with $(x, y) \neq (0, 0)$.

(iii) Observe that the equation $x^2 + y^2 - xyw = 0$ has the unique solution $(x, y) = (0, 0)$ since $w^2 - 4$ is not a square and so the discriminant $\delta(y) = y^2w^2 - 4y^2 = y^2(w^2 - 4)$ is a square if and only if $y = 0$. As before, we can check that for any $f \in \mathcal{F} \setminus \{0\}$, the equation $x^2 + y^2 - xyw = f$ has a solution with $x \neq 0$. ☑

Lemma 16. *Let $q > 3$ be odd, and let $\mathcal{F}$ be a finite field with q elements.*

(i) Given any f in $\{2rt - uwi^2 : i \in \mathcal{F}\}$, there exists a matrix B in the product $\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} t & w \\ 0 & t \end{bmatrix}^{\mathcal{S}}$ such that Trace$(B) = f$. *Also for some $a, b \in \mathcal{F}$, where a is a square and b is a non-square, the matrices $\begin{bmatrix} rt & a \\ 0 & rt \end{bmatrix}$ and $\begin{bmatrix} rt & b \\ 0 & rt \end{bmatrix}$ are in the product $\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} t & w \\ 0 & t \end{bmatrix}^{\mathcal{S}}$. Thus $\eta\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} t & w \\ 0 & t \end{bmatrix}^{\mathcal{S}}\right) \geq \frac{q+3}{2}$.*

(ii) For any f in $\{-uc^2 - ud^2 + s(r - cd) : c, d \in \mathcal{F} \setminus \{0\}\}$, there exists a matrix D in the product $\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} 0 & 1 \\ -1 & s \end{bmatrix}^{\mathcal{S}}$ such that Trace$(D) = f$. *Therefore $\eta\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} 0 & 1 \\ -1 & s \end{bmatrix}^{\mathcal{S}}\right) \geq q - 1$.*

We conclude that given any conjugacy classes $A^{\mathcal{S}}, B^{\mathcal{S}}$ in $\mathcal{S}$, where at least one of A or B is of type (iii), the product $A^{\mathcal{S}}B^{\mathcal{S}}$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes.

Proof.

(i) By Lemma 6, given any $x, y \in \mathcal{F} \smallsetminus \{0\}$,

$$\begin{bmatrix} rt & rwy^2 + tux^2 \\ 0 & rt \end{bmatrix} = \begin{bmatrix} r & ux^2 \\ 0 & r \end{bmatrix} \begin{bmatrix} t & wy^2 \\ 0 & t \end{bmatrix} \in \begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{\mathcal{S}} \begin{bmatrix} t & w \\ 0 & t \end{bmatrix}^{\mathcal{S}}.$$

By Lemma 15(i), the set $\{rwy^2 + tux^2 : x, y \in \mathcal{F} \smallsetminus \{0\}\}$ has a square and a non-square element. It follows then by Lemma 13 that there are two matrices that are not similar in the product with the same trace.

Given any $i \in \mathcal{F}$, let $C(i) = \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}$. By Lemma 7(iv), we have that

$$\text{Trace}\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{C(i)} \begin{bmatrix} t & w \\ 0 & t \end{bmatrix} \right) = 2rt - uwi^2.$$

By Lemma 14, the set $\{2rt - uwi^2 : i \in \mathcal{F}\}$ has $\frac{q+1}{2}$ elements. Thus there are at least $\frac{q+1}{2}$ distinct values for the traces of the matrices in the product. Since there are at least two matrices that are not similar in the product with the same trace and $\frac{q+1}{2} + 1 = \frac{q+3}{2}$, (i) follows.

(ii) Let $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{S}$. By Lemma 7(v), we have

$$\text{Trace}\left(\begin{bmatrix} r & u \\ 0 & r \end{bmatrix}^{C} \begin{bmatrix} 0 & 1 \\ -1 & s \end{bmatrix} \right) = -ud^2 - uc^2 + s(r - ucd).$$

By Lemma 15(ii), we have the set $\{ -ud^2 - uc^2 + s(r - ucd) : c, d \in \mathcal{F}, (c, d) \neq (0, 0)\}$ has $q - 1$ elements and thus (ii) follows. ☑

Lemma 17. *Let $A = \begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & v \end{bmatrix}$, where $v, w \in \mathcal{F}$ are such that $v^2 - 4$ and $w^2 - 4$ are both non-square elements, i.e. A and B are of type (iv).*

Given any f in $\{ -i^2 + i(v - w) + w - 2 : i \in \mathcal{F}\}$, there exists a matrix E in the product $A^{\mathcal{S}}B^{\mathcal{S}}$ such that Trace$(E) = f$.

Let s be a non-square element of $\mathcal{F}$. If $v + w \neq 0$, the matrices $\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$ and $\begin{bmatrix} -1 & s \\ 0 & -1 \end{bmatrix}$ are in the product $A^{\mathcal{S}}B^{\mathcal{S}}$. Otherwise the matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}$ are in the product $A^{\mathcal{S}}B^{\mathcal{S}}$.

We conclude that given any conjugacy classes $A^{\mathcal{S}}, B^{\mathcal{S}}$ in $\mathcal{S}$, where both A and B are of type (iv), the product $A^{\mathcal{S}}B^{\mathcal{S}}$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes. $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) \geq \frac{q+3}{2}$.

Proof. Given any $i \in \mathcal{F}$, let $C(i) = \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix}$. Then by Lemma 7(vi), we have that

$$\text{Trace}\left(A^{C(i)}B\right) = -i^2 + i(v - w) + w - 2.$$

Fix a and c in $\mathcal{F}$, where $a \neq 0$. Set $t_1 = -a^2 - c^2 + acw$ and $C = \begin{bmatrix} a & \frac{c-aw}{t_1} \\ c & -\frac{a}{t_1} \end{bmatrix}$. We can check that $t_1 \neq 0$ since $w^2 - 4$ is a non-square and $C \in \mathcal{F}$. Also

$$A^C = \begin{bmatrix} 0 & 1 \\ -1 & w \end{bmatrix}^C = \begin{bmatrix} w & -\frac{1}{t_1} \\ t_1 & 0 \end{bmatrix}.$$

Fix e and g in $\mathcal{F}$, where $e \neq 0$. Set $t_2 = -e^2 - g^2 + egv$ and $D = \begin{bmatrix} e & \frac{g}{t_2} \\ g & \frac{-e+gv}{t_2} \end{bmatrix}$. By Lemma 15(iii), for any $e, g \in \mathcal{F}$ with $e \neq 0$, we have $t_2 \neq 0$ since $v^2 - 4$ is a non-square.

$$B^D = \begin{bmatrix} 0 & 1 \\ -1 & v \end{bmatrix}^D = \begin{bmatrix} 0 & -\frac{1}{t_2} \\ t_2 & v \end{bmatrix}.$$

Thus

$$A^C B^D = \begin{bmatrix} -\frac{t_2}{t_1} & -\frac{w}{t_2} - \frac{v}{t_1} \\ 0 & -\frac{t_1}{t_2} \end{bmatrix}.$$

Therefore, if $t_1 = t_2$ we get that $A^C B^D = \begin{bmatrix} -1 & -\frac{w+v}{t_1} \\ 0 & -1 \end{bmatrix}$. By Lemma 15(iii), we have that $\big\{a^2 + c^2 - acw : a, c \in \mathcal{F}, a \neq 0\big\} = \mathcal{F} \setminus \{0\}$. Thus the set $\big\{ -\frac{w+v}{t_1} : t_1 = -a^2 - c^2 + acw, a, c \in \mathcal{F}, a \neq 0\big\}$ has $q - 1$ elements as long as $w + v \neq 0$. If $w + v = 0$, then $w - v \neq 0$ since $w \neq 0$. In that case, let $t_1 = -t_2$ and thus the set $\big\{ -\frac{w-v}{t_1} : t_1 = -a^2 - c^2 + acw, a, c \in \mathcal{F}, a \neq 0\big\}$ has $q - 1$ elements. In particular, in both cases the sets contain 1 and a non-square element and the result follows. ☑

Proof of Theorem 2. If at least one of A and B is a scalar matrix, then $A^{\mathcal{S}}B^{\mathcal{S}}$ is a conjugacy class. We may assume then that A, B are similar to matrices of type (ii), (iii) or (iv). Theorem 2 then follows from Lemma 9, Lemma 16 and Lemma 17. ☑

Proposition 18. *Assume that $\mathcal{F}$ is a field of q elements, with $q > 3$ odd.*

(i) Assume that $q \equiv 1 \bmod 4$. Let w be a non-square element in $\mathcal{F}$. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & w \\ 0 & 1 \end{bmatrix}$. Then

$$\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) = \frac{q+3}{2}. \tag{5}$$

(ii) Assume that $q \not\equiv 1 \bmod 4$. Set $E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then

$$\eta(E^{\mathcal{S}}E^{\mathcal{S}}) = \frac{q+3}{2}. \tag{6}$$

Hence, Theorem 2 is optimal.

Proof.

(i) Let $C_i = \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \in \mathcal{S}$ for $i = 1, 2$. By Lemma 6(ii),

$$A^{C_i}B = \begin{bmatrix} 1 + c_i d_i & {d_i}^2 \\ -{c_i}^2 & 1 - c_i d_i \end{bmatrix} \begin{bmatrix} 1 & w \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 + c_i d_i & w + wc_i d_i + {d_i}^2 \\ -c_i^2 & 1 - c_i d_i - w{c_i}^2 \end{bmatrix}.$$

Hence, Trace $\big(A^{C_i}B\big) = 2 - w{c_i}^2$, which takes on $\frac{q+1}{2}$ values by Lemma 14. Note that if two matrices $A^{C_1}B$ and $A^{C_2}B$ have the same trace, then ${c_1}^2 = {c_2}^2$.

Suppose ${c_1}^2 = {c_2}^2 \neq 0$. Let $D = \begin{bmatrix} 1 & \frac{c_2 d_2 - c_1 d_1}{{c_1}^2} \\ 0 & 1 \end{bmatrix}$.

Then $\big(A^{C_1}B\big)^D = A^{C_2}B$, and so, excluding trace 2, each possible value of the trace is obtained by at most one conjugacy class.

Suppose $c_1 = c_2 = 0$. Then $A^{C_i}B = \begin{bmatrix} 1 & w + {d_i}^2 \\ 0 & 1 \end{bmatrix}$. Note that $w + {d_i}^2 \neq 0$ since $-w$ is non-square. Let z be a generator of the multiplicative group of units of $\mathcal{F}$, and suppose $w + {d_i}^2 = z^{n_i}$. By Lemma 13, $A^{C_1}B$ and $A^{C_2}B$ are conjugate if and only if there is an $e \in \mathcal{F} \smallsetminus \{0\}$ such that $z^{n_1}e^2 = z^{n_2}$, i.e. when n_1 and n_2 have the same parity. Hence there are at most two conjugacy classes represented by matrices with trace 2, and thus, $\eta\big(A^{\mathcal{S}}B^{\mathcal{S}}\big) \leq \big(\frac{q+1}{2} - 1\big) + 2 = \frac{q+3}{2}$.

(ii) Define C_i as in (i). Then we may proceed by replacing w with 1 in the argument for the previous case, since -1 is not a square in $\mathcal{F}$. Thus, $\eta\big(E^{\mathcal{S}}E^{\mathcal{S}}\big) \leq \frac{q+3}{2}$.

Hence, in each case, the result follows by Theorem 2. ☑

Acknowledgement. The first author thanks to Daniel M. Suarez for his encouragement.

References

[1] E. Adan-Bante, J. Harris, and H. Verril, *Products of Conjugacy Classes of the Alternating Group*, preprint.

[2] E. Adan-Bante and H. Verrill, *Symmetric Groups and Conjugacy Classes*, J. Group Theory **11** (2008), no. 3, 371–379.

[3] Z. Arad and M. Herzog, *Products of Conjugacy Classes in Groups*, Lecture notes in mathematics, vol. 1112, Springer-Verlag, 1985.

[4] R. Gow, *Commutators in Finite Simple Groups of Lie Type*, Bull. London Math. Soc. **32** (2000), 311–315.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007, http://www.gap-system.org.

[6] G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge mathematical textbooks, Cambridge University Press, 2001.

(Recibido en agosto de 2011. Aceptado en noviembre de 2012)

Department of Mathematics
University of Saint Thomas
Mail OSS 201, 2115 Summit Avenue
Saint Paul, MN 55105-1079
Minnesota, USA
e-mail: EdithAdan@illinoisalumni.org

Department of Mathematics
University of Southern Mississippi
730 East Beach Boulevard
Long Beach, MS 39560
Mississippi, USA
e-mail: john.m.harris@usm.edu