BULL. AUSTRAL. MATH. SOC. 05E15, 11L05, 11T23, 20G40
VOL. 63 (2001) [15–20]

A COUNTING FORMULA ABOUT THE SYMPLECTIC SIMILITUDE GROUP

KWANKYU LEE

We derive an explicit formula for the number of elements in the symplectic similitude group $\mathrm{GSp}(2n,q)$ with given trace and determinant.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with q elements. Recall that the symplectic similitude group $\mathrm{GSp}(2n,q)$ over $\mathbb{F}_q$ is defined by

$$\mathrm{GSp}(2n,q) = \left\{ g \in \mathrm{GL}(2n,q) \mid {}^t g J g = \alpha(g) J \text{ for some } \alpha(g) \in \mathbb{F}_q^\times \right\},$$

where J denotes $\begin{bmatrix} 0 & 1_n \\ -1_n & 0 \end{bmatrix}$. This paper addresses the problem of counting the number of elements in $\mathrm{GSp}(2n,q)$ with given trace and determinant. More formally, we want to find the value of

$$C(\zeta,\eta) = \left|\left\{ g \in \mathrm{GSp}(2n,q) \mid \det g = \zeta,\ \mathrm{tr}\, g = \eta \right\}\right|,$$

when $\zeta \in \mathbb{F}_q^\times$, $\eta \in \mathbb{F}_q$ are given. In [1], Kim gave a related result: an explicit formula for the number of elements in $\mathrm{GSp}(2n,q)$ with given trace. In this paper, we derive an explicit formula for $C(\zeta,\eta)$.

THEOREM 1. *Let $\zeta \in \mathbb{F}_q^\times$, $\eta \in \mathbb{F}_q$. Let S denote the number of n-th roots of ζ in $\mathbb{F}_q$, and let*

$$T_m = q \sum_{\alpha \in \mathbb{F}_q^\times} \sum_{\alpha_1,\dots,\alpha_m \in \mathbb{F}_q^\times} t(\alpha^n, \alpha_1 + \alpha\alpha_1^{-1} + \cdots + \alpha_m + \alpha\alpha_m^{-1}) - (q-1)^m S,$$

where $t(x,y) = 1$ if $(x,y) = (\zeta,\eta)$, 0 otherwise; and the inner sum is regarded as $t(\alpha^n, 0)$ for $m = 0$. Then we have

$$C(\zeta,\eta) = q^{n^2-1} \sum_{b=0}^{[n/2]} \left(q^{b^2+b} \begin{bmatrix} n \\ 2b \end{bmatrix}_q \prod_{j=1}^{b} (q^{2j-1}-1) \sum_{l=0}^{[(n/2)-b]} q^l R(n-2b+1, l) T_{n-2b-2l} \right) + q^{n^2-1} \prod_{j=1}^{n} (q^{2j}-1) S,$$

Received 11th January, 2000
This work was supported by the Brain Korea 21 Project.

https://doi.org/10.1017/S0004972700019079 Published online by Cambridge University Press

where $R(m,l)$ *denotes* $\sum_{0<j_1<\cdots<j_l<m-l} \prod_{\nu=1}^{l} (q^{m-\nu-j_\nu}-1)$ *with* $R(m,0)=1$.

The definition of the q-binomial coefficient $\begin{bmatrix} n \\ b \end{bmatrix}_q$ is given in the next section.

2. Preparation

Recall that the symplectic group over $\mathbb{F}_q$ is defined by

$$\mathrm{Sp}(2n,q) = \{\, g \in \mathrm{GL}(2n,q) \mid {}^t gJg = J \,\}.$$

Observe that

$$\mathrm{GSp}(2n,q) = \coprod_{\alpha \in \mathbb{F}_q^\times} d_\alpha \mathrm{Sp}(2n,q)$$

with $d_\alpha = \begin{bmatrix} 1_n & 0 \\ 0 & \alpha 1_n \end{bmatrix}$. A maximal parabolic subgroup P of $\mathrm{Sp}(2n,q)$ is given by

$$P = P(2n,q) = \left\{ \begin{bmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{bmatrix} \begin{bmatrix} 1_n & B \\ 0 & 1_n \end{bmatrix} \;\middle|\; A \in \mathrm{GL}(n,q), {}^tB = B \right\}.$$

We let, for $0 \leqslant b \leqslant n$,

$$A_b = A_b(2n,q) = \{\, g \in P(2n,q) \mid \sigma_b g \sigma_b^{-1} \in P(2n,q) \,\},$$

where

$$\sigma_b = \begin{bmatrix} 0 & 0 & 1_b & 0 \\ 0 & 1_{n-b} & 0 & 0 \\ -1_b & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-b} \end{bmatrix}.$$

Now the Bruhat decomposition of $\mathrm{Sp}(2n,q)$ with respect to P says

$$\mathrm{Sp}(2n,q) = \coprod_{b=0}^{n} P\sigma_b P = \coprod_{b=0}^{n} P\sigma_b (A_b \backslash P).$$

This decomposition will play a crucial role in our proof of the theorem.

Let g_n be the number of $n \times n$ nonsingular matrices over $\mathbb{F}_q$, and a_n the number of $n \times n$ nonsingular alternating matrices over $\mathbb{F}_q$. We define $g_0 = a_0 = 1$ for convenience.

Then

$$g_n = \prod_{j=0}^{n-1}(q^n - q^j) = q^{(n^2-n)/2}\prod_{j=1}^{n}(q^j - 1),$$

$$a_n = \begin{cases} q^{(n/2)((n/2)-1)}\prod_{j=1}^{n/2}(q^{2j-1}-1) & \text{for } n \text{ even},\\ 0 & \text{for } n \text{ odd},\end{cases}$$

$$|A_b\backslash P| = q^{(b^2+b)/2}\begin{bmatrix} n \\ b \end{bmatrix}_q.$$

The q-binomial coefficient $\begin{bmatrix} n \\ r \end{bmatrix}_q$ is defined by

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{j=0}^{r-1}\frac{q^{n-j}-1}{q^{r-j}-1}.$$

See [**1**] and [**2**] for more details of these facts.

3. Proof of the theorem

For any complex-valued function f defined on $\mathbb{F}_q$ and $\sigma, \tau \in \mathbb{F}_q$, let $M_m(f;\sigma,\tau)$ denote

$$\sum_{\alpha_1,\ldots,\alpha_m\in\mathbb{F}_q^\times} f(\sigma\alpha_1 + \tau\alpha_1^{-1} + \cdots + \sigma\alpha_m + \tau\alpha_m^{-1})$$

with $M_0(f;\sigma,\tau) = f(0)$. Remember that $R(m,l)$ was defined in Theorem 1.

Lemma 1. *Let f be an arbitrary complex-valued function defined on $\mathbb{F}_q$, and $\sigma, \tau \in \mathbb{F}_q^\times$. Then*

$$\sum_{g\in \mathrm{GL}(n,q)} f(\sigma \operatorname{tr} g + \tau \operatorname{tr} g^{-1})$$
$$= q^{(n^2-n)/2-1}\sum_{l=0}^{[n/2]} q^l R(n+1,l)\Big(qM_{n-2l}(f;\sigma,\tau) - (q-1)^{n-2l}\sum_{\gamma\in\mathbb{F}_q} f(\gamma)\Big)$$
$$+ q^{(n^2-n)/2-1}\prod_{j=1}^{n}(q^j-1)\sum_{\gamma\in\mathbb{F}_q} f(\gamma).$$

Proof: Recall that for a nontrivial additive character λ of $\mathbb{F}_q$ and $\sigma,\tau \in \mathbb{F}_q$, the ordinary Kloosterman sum $K(\lambda;\sigma,\tau)$ is defined by $K(\lambda;\sigma,\tau) = \sum_{\alpha\in\mathbb{F}_q^\times}\lambda(\sigma\alpha+\tau\alpha^{-1})$. First we state a slightly modified version of Theorem 4.3 in [**2**].

https://doi.org/10.1017/S0004972700019079 Published online by Cambridge University Press

SUBLEMMA. *Let us define* $K_{\mathrm{GL}(n,q)}(\lambda;\sigma,\tau) = \sum_{g\in\mathrm{GL}(n,q)} \lambda(\sigma \operatorname{tr} g + \tau \operatorname{tr} g^{-1})$ *for a nontrivial additive character* λ *of* $\mathbb{F}_q$ *and* $\sigma,\tau \in \mathbb{F}_q^\times$. *Then*

$$K_{\mathrm{GL}(n,q)}(\lambda;\sigma,\tau) = q^{(n^2-n)/2}\sum_{l=0}^{[n/2]} q^l R(n+1,l)K(\lambda;\sigma,\tau)^{n-2l}.$$

Now pick a nontrivial additive character λ of $\mathbb{F}_q$. We then have

$$\begin{aligned}\sum_{g\in\mathrm{GL}(n,q)} & f(\sigma\operatorname{tr} g+\tau\operatorname{tr} g^{-1})\\ &= \sum_{\gamma\in\mathbb{F}_q} \left|\{\, g\in\mathrm{GL}(n,q) \mid \sigma\operatorname{tr} g+\tau\operatorname{tr} g^{-1}=\gamma\,\}\right| f(\gamma)\\ &= \frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q}\sum_{g\in\mathrm{GL}(n,q)} \lambda\big(\delta(\sigma\operatorname{tr} g+\tau\operatorname{tr} g^{-1}-\gamma)\big)f(\gamma)\\ &= \frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q^\times} K_{\mathrm{GL}(n,q)}(\lambda;\delta\sigma,\delta\tau)\lambda(-\delta\gamma)f(\gamma) + \frac{1}{q}g_n\sum_{\gamma\in\mathbb{F}_q} f(\gamma).\end{aligned}$$

By the sublemma,

$$\begin{aligned}\sum_{g\in\mathrm{GL}(n,q)} & f(\sigma\operatorname{tr} g+\tau\operatorname{tr} g^{-1})\\ &= q^{(n^2-n)/2}\sum_{l=0}^{[n/2]} q^l R(n+1,l)\frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q^\times} K(\lambda;\delta\sigma,\delta\tau)^{n-2l}\lambda(-\delta\gamma)f(\gamma)\\ &\qquad + q^{(n^2-n)/2-1}\prod_{j=1}^{n}(q^j-1)\sum_{\gamma\in\mathbb{F}_q} f(\gamma).\end{aligned}$$

But we have

$$\begin{aligned}\frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q^\times} & K(\lambda;\delta\sigma,\delta\tau)^{n-2l}\lambda(-\delta\gamma)f(\gamma)\\ &= \frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q^\times}\Big(\sum_{\alpha\in\mathbb{F}_q^\times}\lambda(\delta\sigma\alpha+\delta\tau\alpha^{-1})\Big)^{n-2l}\lambda(-\delta\gamma)f(\gamma)\\ &= \frac{1}{q}\sum_{\gamma\in\mathbb{F}_q}\sum_{\delta\in\mathbb{F}_q}\sum \lambda\big(\delta(\sigma\alpha_1+\tau\alpha_1^{-1}+\cdots+\sigma\alpha_{n-2l}+\tau\alpha_{n-2l}^{-1}-\gamma)\big)f(\gamma)\\ &\qquad - \frac{1}{q}(q-1)^{n-2l}\sum_{\gamma\in\mathbb{F}_q} f(\gamma)\\ &= \sum f(\sigma\alpha_1+\tau\alpha_1^{-1}+\cdots+\sigma\alpha_{n-2l}+\tau\alpha_{n-2l}^{-1}) - \frac{1}{q}(q-1)^{n-2l}\sum_{\gamma\in\mathbb{F}_q} f(\gamma),\end{aligned}$$

where the unspecified sums are taken over $\alpha_1,\ldots,\alpha_{n-2l}\in\mathbb{F}_q^\times$. Thus we get the lemma. ∎

Lemma 2. *Let e, f be arbitrary complex-valued functions defined on $\mathbf{F}_q$. Then*

$$\sum_{g\in \mathrm{GSp}(2n,q)} e(\det g)f(\operatorname{tr} g)$$
$$= q^{n^2-1}\sum_{b=0}^{[n/2]}\Bigg(q^{b^2+b}\begin{bmatrix} n \\ 2b\end{bmatrix}_q \prod_{j=1}^{b}(q^{2j-1}-1)\sum_{l=0}^{[(n/2)-b]} q^l R(n-2b+1,l)$$
$$\times \sum_{\alpha\in\mathbf{F}_q^\times} e(\alpha^n)\Big(qM_{n-2b-2l}(f;1,\alpha)-(q-1)^{n-2b-2l}\sum_{\gamma\in\mathbf{F}_q} f(\gamma)\Big)\Bigg)$$
$$+ q^{n^2-1}\prod_{j=1}^{n}(q^{2j}-1)\sum_{\alpha\in\mathbf{F}_q^\times} e(\alpha^n)\sum_{\gamma\in\mathbf{F}_q} f(\gamma).$$

Proof: We have

$$\sum_{g\in \mathrm{GSp}(2n,q)} e(\det g)f(\operatorname{tr} g) = \sum_{\alpha\in\mathbf{F}_q^\times}\sum_{g\in \mathrm{Sp}(2n,q)} e\big(\det(d_\alpha g)\big)f\big(\operatorname{tr}(d_\alpha g)\big)$$
$$= \sum_{\alpha\in\mathbf{F}_q^\times} e(\alpha^n)\sum_{g\in \mathrm{Sp}(2n,q)} f\big(\operatorname{tr}(d_\alpha g)\big).$$

By the Bruhat decomposition,

$$\sum_{g\in \mathrm{GSp}(2n,q)} e(\det g)f(\operatorname{tr} g) = \sum_{\alpha\in\mathbf{F}_q^\times} e(\alpha^n)\sum_{b=0}^{n}|A_b\backslash P|\sum_{g\in P} f\big(\operatorname{tr}(d_\alpha g\sigma_b)\big).$$

Observe that the structure of P allows us to compute explicitly $\operatorname{tr}(d_\alpha g\sigma_b)$ for $g\in P$. Thus we get

$$\sum_{g\in \mathrm{GSp}(2n,q)} e(\det g)f(\operatorname{tr} g)$$
$$= \sum_{\alpha\in\mathbf{F}_q^\times} e(\alpha^n)\sum_{b=0}^{n}|A_b\backslash P|\Big(q^{(n^2+n)/2-1}\big(g_n - a_b g_{n-b}q^{b(n-b)}\big)\sum_{\gamma\in\mathbf{F}_q} f(\gamma)$$
$$+ a_b q^{(n^2+n)/2+b(n-b)}\sum_{g\in \mathrm{GL}(n-b,q)} f(\operatorname{tr} g+\alpha\operatorname{tr} g^{-1})\Big).$$

Now use Lemma 1 to resolve the last expression. This completes the proof. ∎

Proof of Theorem 1: We obtain Theorem 1 from Lemma 2 simply by setting e and f to be the functions defined by

$$e(\alpha)=\begin{cases}1 & \text{if } \alpha=\zeta,\\ 0 & \text{otherwise,}\end{cases}\quad \text{and}\quad f(\alpha)=\begin{cases}1 & \text{if } \alpha=\eta,\\ 0 & \text{otherwise,}\end{cases}$$

for $\alpha\in\mathbf{F}_q$. ∎

https://doi.org/10.1017/S0004972700019079 Published online by Cambridge University Press

REMARK. Tables of $C(\zeta,\eta)$ for $GSp(2n,q)$ with different n and q are included below. These were produced by a `Mathematica` program into which the formula for $C(\zeta,\eta)$ was coded. The referee explained the apparent symmetries in the tables by observing that $C(\zeta,\eta) = C(\alpha^{2n}\zeta, \alpha\eta)$ for $\alpha \in \mathbf{F}_q^\times$.

TABLES OF $C(\zeta,\eta)$

$GSp(6,3)$

$C(\zeta,\eta)$	$\eta=0$	$\eta=1$	$\eta=2$
$\zeta=1$	3053423790	3058639785	3058639785
$\zeta=2$	3063934512	3053384424	3053384424

$GSp(4,5)$

$C(\zeta,\eta)$	$\eta=0$	$\eta=1$	$\eta=2$	$\eta=3$	$\eta=4$
$\zeta=1$	3867500	3713125	3713125	3713125	3713125
$\zeta=2$	0	0	0	0	0
$\zeta=3$	0	0	0	0	0
$\zeta=4$	3870000	3712500	3712500	3712500	3712500

$GSp(6,5)$

$C(\zeta,\eta)$	$\eta=0$	$\eta=1$	$\eta=2$	$\eta=3$	$\eta=4$
$\zeta=1$	91408007812500	91395326171875	91401669921875	91401669921875	91395326171875
$\zeta=2$	91395312500000	91408015625000	91395328125000	91395328125000	91408015625000
$\zeta=3$	91395312500000	91395328125000	91408015625000	91408015625000	91395328125000
$\zeta=4$	91408007812500	91401669921875	91395326171875	91395326171875	91401669921875

REFERENCES

[1] D.S. Kim, 'Exponential sums for symplectic groups and their applications', *Acta Arith.* **88** (1999), 155–171.

[2] D.S. Kim, 'Gauss sums for symplectic groups over a finite field', *Monatsh. Math.* **126** (1998), 55–71.

Department of Mathematics
Sogang University
Seoul 121-742
Korea
e-mail: leekk@math.sogang.ac.kr

https://doi.org/10.1017/S0004972700019079 Published online by Cambridge University Press